STid
Electronic Identification

SECARD

MANUEL UTILISATEUR

Designed in France
Made in France

www.stid.com

Remerciements

Bienvenue dans le monde de la haute sécurité !

Vous venez de faire l'acquisition du logiciel SECard vous permettant de programmer des badges de configurations et utilisateurs.

Nous vous remercions de votre confiance et espérons que cette solution développée par STid vous donnera entière satisfaction.

Nous restons à votre disposition pour toute question sur l'utilisation de ce logiciel ou sur notre gamme de produits.

Nous vous donnons rendez-vous pour plus d'informations sur notre site internet www.stid.com.

L'équipe STid

Introduction

Ce manuel se décompose en deux parties :

Partie 1 : Description détaillée de toutes les fonctionnalités

Partie 2 : Technique

MANUEL UTILISATEUR / PARTIE 1

MANUEL UTILISATEUR / PARTIE 2

STid
Electronic Identification

SECARD

MANUEL UTILISATEUR

Partie 1 : Description détaillée de toutes les fonctionnalités

Designed in France
Made in France

www.stid.com

I. Informations

I. 1 - Prérequis PC

- Un PC avec comme système d'exploitation : Windows 7, 8 ou 10 ou Windows serveur 2012r2
- Une connexion USB ou RS232.
- Espace disque disponible de 50 Mo minimum.

I. 2 - Contenu de la clé USB

- Driver USB FTDI pour Windows 7, 8.x et 10.
- SECard Version 3.x.x.
- MorphoSmart Driver 3.58.

I. 3 - Matériel nécessaire

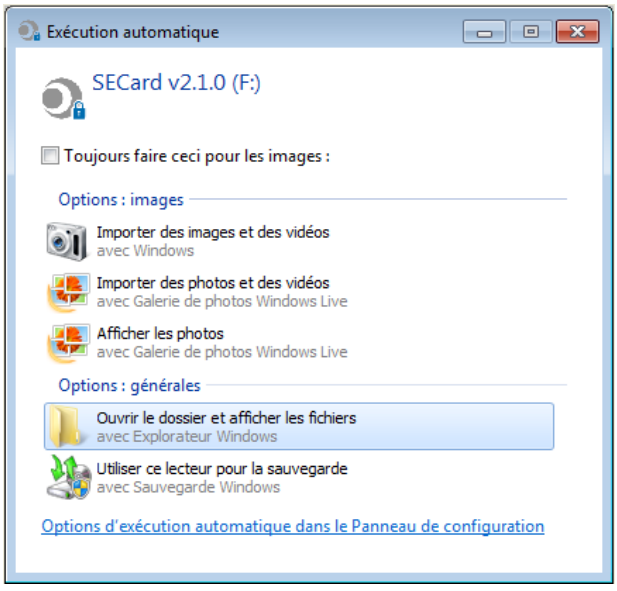
- Encodeur 13.56 MHz STid
  SECard :
  - USB (Réf. STR-W35-E-PH5-5AA-1) ou RS232 (Réf. STR-W32-E-PH5-5AA-1).
    Version de firmware U12 minimum (visible sur l'étiquette au dos de l'encodeur).
  - USB (Réf. ARC-W35-G-PH5-5AA-1).
    Version de firmware Z06 minimum (visible sur l'étiquette au dos de l'encodeur).

  SECard avec encodeur Bluetooth :
  - USB (Réf. ARCS-W35-G-BT1-5AA-1).
    Version de firmware Z06 minimum (visible sur l'étiquette au dos de l'encodeur).

- Un cordon USB ou RS232.

I. 4 - Installation sous Windows

- Insérer la clé USB SECard dans un port USB de votre PC.
- Attendre l'ouverture automatique de la fenêtre d'exploration.



- Lancer SECard V3x.x_setup.exe.
- Suivre les instructions affichées à l'écran.

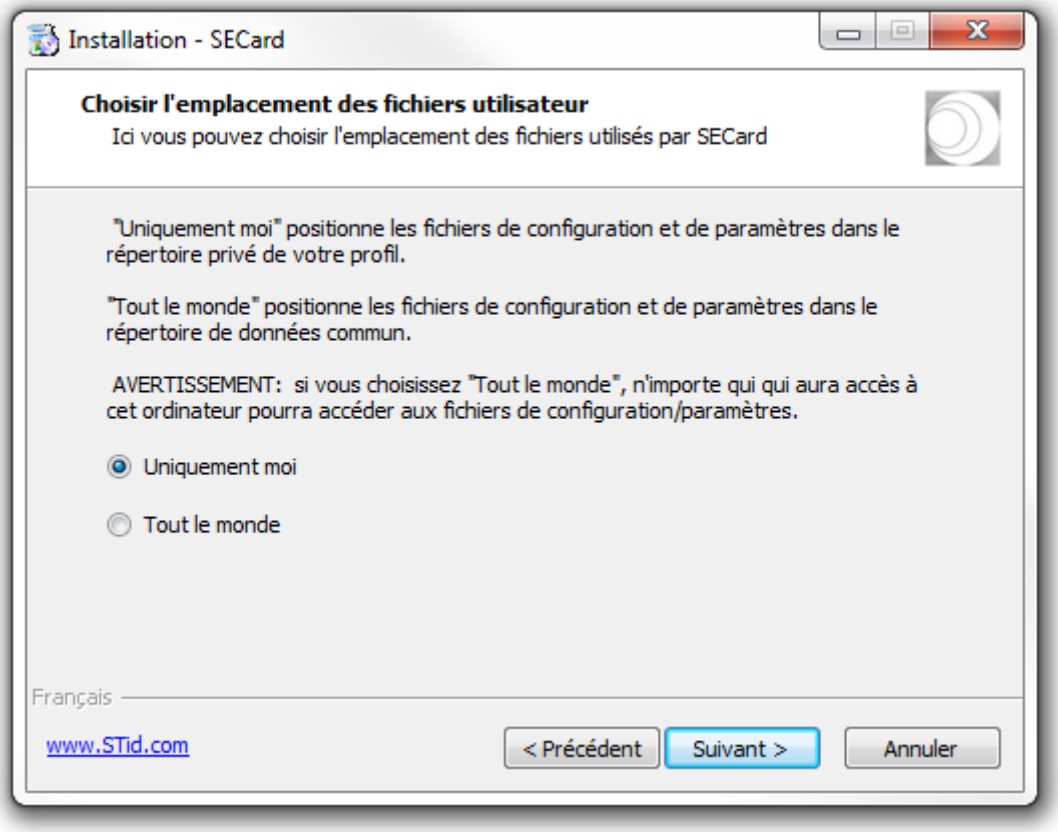
Remarque :

si la biométrie a déjà été installée sur le PC lors d'une précédente installation de SECard, décocher Biométrie dans l'assistant d'installation.

si le driver FTDI a déjà été installé sur le PC lors d'une précédente installation de SECard, décocher driver FTDI dans l'assistant d'installation.

- Localisation des fichiers utilisateurs.

  Les fichiers de paramètres seront installés dans le répertoire contenant l'exécutable mais aussi dans un des répertoires suivants selon le choix de l'utilisateur.



  - ✓ « Uniquement moi » : les fichiers utilisateurs sont placés dans : ../Utilisateurs/ UtilisateurXX/STid/SECard vX.Y.Z.B/ et ne sont donc accessibles qu'à l'utilisateur UtilisateurXX ou à l'Administrateur.

  - ✓ « Tout le monde » : les fichiers utilisateurs sont placés dans : ../ProgramData/STid/SECard v.X.Y.Z.B/ et sont accessibles à tout le monde.

Remarque : pour modifier la localisation des fichiers utilisateurs, ouvrir le fichier .gcf qui se situe dans le même répertoire que SECard.exe et changer la valeur de la section [File]

Location=X ;X=0 pour « Just me », X=1 pour « Everyone »

```
[File]
Settings=.\SECard.pse
Location=0
```

I. 5 - Compatibilité

- **Firmware / version de SECard**

Le logiciel SECard (V3.x.x) permet une gestion des compatibilités entre les versions de SECard et les versions de firmware des lecteurs.

Le but est de pouvoir configurer les lecteurs haute sécurité Standards, encastrables WAL et Architect® avec le même logiciel SECard.

Lecteurs Standards	Version de SECard	Version du SCB	Version du Firmware
	V1.1.x	V3	≥ U7
	V1.2.x	V4	≥ U8
	V1.3.x	V5	≥ U11
	V1.4.x	V6	≥ U13
	V1.4B	V7	≥ U20

Lecteurs WAL	Version de SECard	Version du SCB	Version du Firmware
	V1.4.x	V6	Z16
	V1.5.x	V8	≥ Z17
	V1.6.x	V9	≥ Z20

Lecteurs ARC	Version de SECard	Version du SCB	Version du Firmware
	V2.0.x	V7	Z01
	V2.1.x	V8	≥ Z02
	V2.2.x	V9	≥ Z04
	V3.0.x	V10	≥ Z05
	V3.1.x	V11	≥ Z07

Lecteurs ARCS	Version de SECard	Version du SCB	Version du Firmware
	V3.0.x	V10	≥ Z05
	V3.1.x	V11	≥ Z07
	V3.2.x	V12	≥ Z08

	Lecteurs Standards	Lecteurs WAL	Lecteurs ARC / ARC1	Lecteurs ARCS	Lecteurs ARCS Blue
SCB Standards	✓	✓	✓	✓	✓ (1)
SCB WAL	x	✓	✓	✓	✓ (1)
SCB ARC/ARC1	x	x	✓	✓	✓ (1)
SCB ARCS	x	x	✓	✓	✓ (1)
SCB ARCS Blue	x	x	x	✓	✓

Note importante pour les lecteurs Architect®

Avec SECard il est possible de configurer l'ensemble des fonctionnalités de l'Architect® (RFID, clavier, écran tactile, biométrie, Bluetooth) sur un même SCB. Le lecteur viendra récupérer dans le SCB uniquement les paramètres qui lui sont nécessaires. Pour désactiver une fonctionnalité, il faut déconnecter le sous-ensemble correspondant et représenter le SCB au lecteur.

(1): Sous certaines conditions si un SCB Standard, WAL, ARC, ARCS sans configuration Bluetooth est présenté à un lecteur ARCS Bluetooth une configuration Bluetooth, appelée “DESFireAuto”, est activée pour le Bluetooth.

- **Fichier de configuration / Version de SECard**

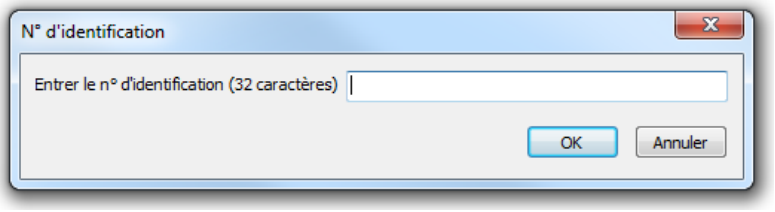
	SECard V1.x	SECard V2.x	SECard V3.x
.ese	✓	Convertisseur de fichier	Convertisseur de fichier
.pse générer avec une version < 3	x	✓	✓*
.pse générer avec une version ≥ 3	x	x	✓

Attention*

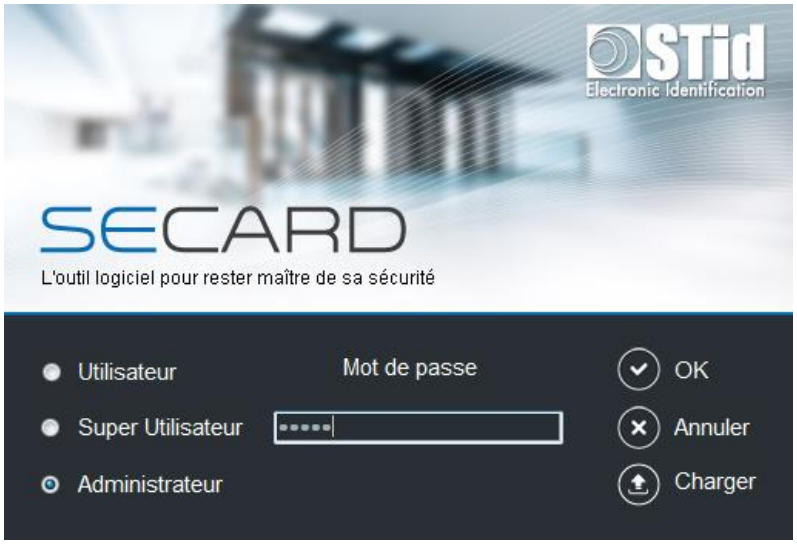
Lorsqu’un fichier .pse créé avec SECard V2.x est chargé et sauvegardé dans SECard V3.x avec des mots de passe, il n’est plus possible de le charger à nouveau dans SECard V2.x.

I. 6 - Démarrage du logiciel

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



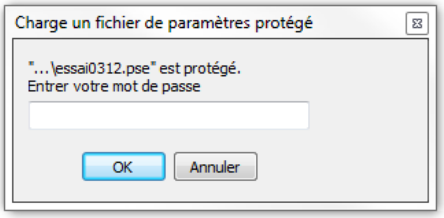
Il est possible d'installer le logiciel sur un nombre illimité de stations de travail, mais il n'est possible de l'utiliser qu'avec l'encodeur dont le numéro de série aura été renseigné. Ce numéro permet à SECard de s'authentifier avec l'encodeur fourni dans le kit. Si vous souhaitez commander un encodeur supplémentaire appairé à SECard, contacter le service commercial.



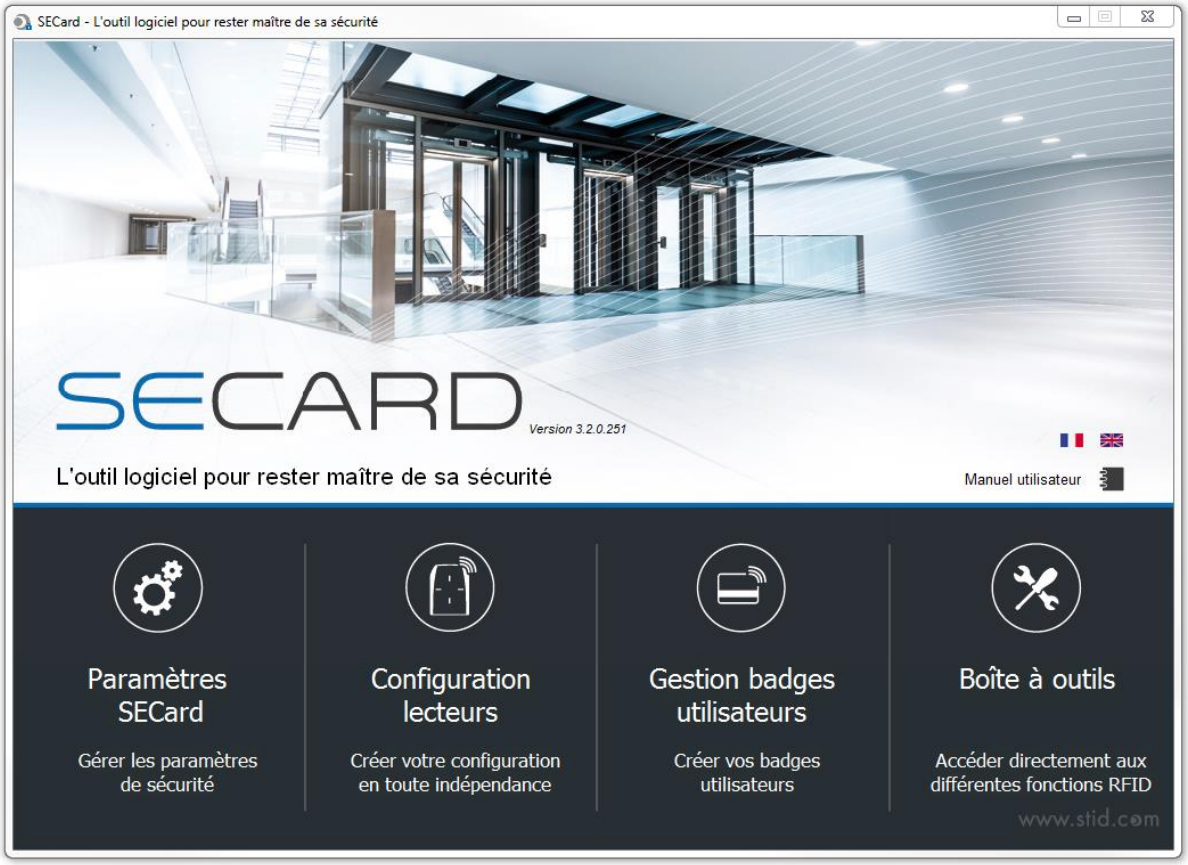
Lors du démarrage du logiciel, une fenêtre apparaît pour la saisie des identifiants de connexion ou le chargement d'un fichier de configuration spécifique.
Il y a trois niveaux d'accès, gérant différentes autorisations au sein du logiciel. Ces mots de passe sont sauvegardés dans le fichier de configuration.

Niveaux d'accès	Mots de passe par défaut	Droits associés
Administrateur	STidA	Paramétrage du logiciel et utilisation sans aucune restriction
Super Utilisateur	STidP	Paramétrables par l'Administrateur
Utilisateur	STidU	Création de badges utilisateurs

Note : Si la fenêtre suivante apparait et que le mot de passe demandé n'est pas connu, cliquer sur annuler et utiliser le bouton « Charger » pour charger un autre fichier. Le fichier par défaut se trouve dans le répertoire d'installation.



I. 7 - Généralités



❖ Le logiciel se décompose en quatre parties distinctes :

Paramétrage de SECard et de l'encodeur

Création des badges de configuration lecteurs

Création des identifiants utilisateurs

Outils

❖ Sur la page d'accueil vous avez le choix de la langue et l'accès au manuel utilisateur.
Le manuel utilisateur sera accessible à tout moment en appuyant sur la touche F1.

❖ Les champs de clés peuvent être remplis :

- aléatoirement en effectuant un clic droit à l'intérieur du champ et en sélectionnant l'action « *Remplir avec une valeur aléatoire* » ou en appuyant simultanément sur la touche CTRL+R.

Les valeurs aléatoires sont de niveau cryptographique et sont générées avec le générateur ISAAC.

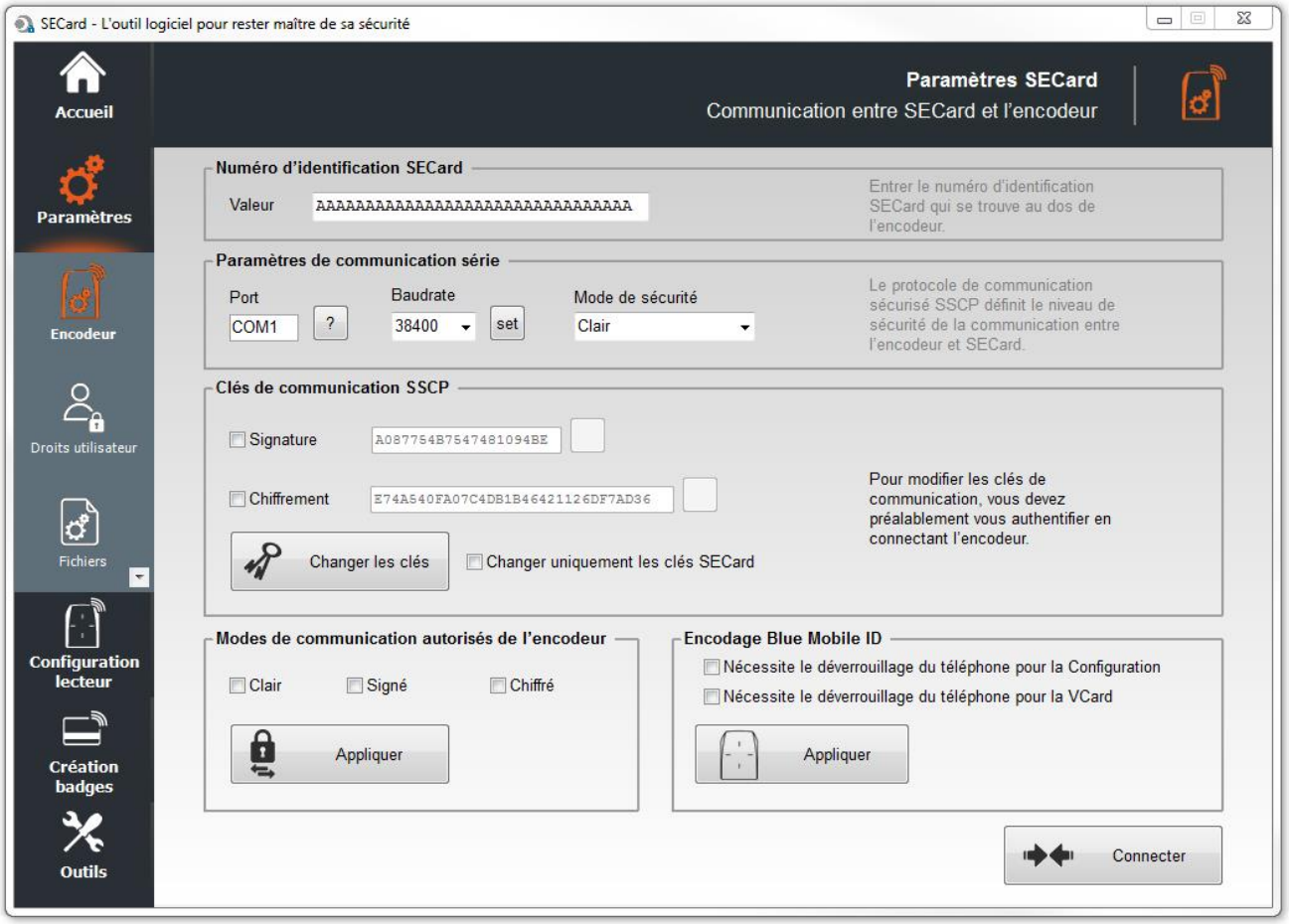
- à FF en appuyant simultanément sur la touche CTRL+F ou avec le clic droit de la souris.
- à 00 en appuyant simultanément sur la touche CTRL+O ou avec le clic droit de la souris.

❖ Les actions « *Copier / Coller* » peuvent être effectuées soit :

- avec un clic droit à l'intérieur du champ et en sélectionnant les actions « *Copier / Coller* ».
- en appuyant sur les touches CTRL+C / CTRL+V.

II. Paramètres SECard

II. 1 - Encodeur



Numéro d'identification SECard

Permet d'enregistrer un nouvel encodeur.

Paramètres de communication série

Permet de paramétrer la communication entre l'encodeur et SECard.

- La vitesse de communication par défaut de l'encodeur est 38400 bauds.
  Attention, cette vitesse doit être strictement la même que celle définie dans le logiciel.

  Pour changer la vitesse de communication il est possible de changer la valeur du Baudrate.
  Pour cela, s'assurer que la communication encodeur / SECard est ok, sélectionner une vitesse de communication dans le menu déroulant « Baudrate » (115200 Bauds étant la vitesse maximale) et cliquer sur le bouton « fixer ».

Note :

- Si vous ne connaissez pas le port de communication utilisé, il vous est possible de le retrouver automatiquement en cliquant sur le bouton [?].
  Il est nécessaire que le driver USB soit installé et que le lecteur encodeur soit raccordé.

- En appuyant sur le bouton [?] et en maintenant la touche CTRL gauche appuyée, SECard recherchera un lecteur connecté à toutes les vitesses et sur tous les ports de communication. Cette opération peut prendre un certain temps.

❖ La communication entre le logiciel SECard et l'encodeur s'effectue par liaison série ou liaison USB, elle repose sur le protocole de communication SSCP (STid Secure Common Protocol).
Les encodeurs intègrent des algorithmes publics de signature (*HMAC-SHA1*) et de chiffrement (*AES*) qui peuvent être utilisés dans la sécurisation des données sur la liaison série entre l'encodeur et SECard.
La communication peut être effectuée de quatre façons différentes :

- ✓ En clair : Communication encodeur / SECard en clair
- ✓ Signée : Communication encodeur / SECard signée
- ✓ Chiffrée : Communication encodeur / SECard chiffrée
- ✓ Signée et Chiffrée : Communication encodeur / SECard signée et chiffrée

Note :
La communication encodeur / SECard est plus sécurisée lorsque celle-ci est utilisée signée et chiffrée (mode de sécurité à « *Signé et Chiffré* »). Par opposition, une communication en clair (mode de sécurité à « *En clair* ») n'est pas sécurisée.

Clés de communication SSCP

Permet de changer les clés de communication entre l'encodeur et SECard.

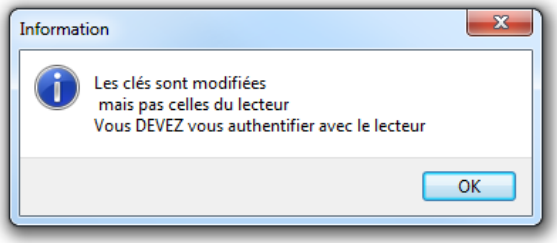
Lorsque la communication est signée et/ou chiffrée, le logiciel SECard et l'encodeur utilisent les clés utilisateurs par défaut suivantes :

Clé de signature : *A087754B7547481094BE*
Clé de chiffrement : *E74A540FA07C4DB1B46421126DF7AD36*

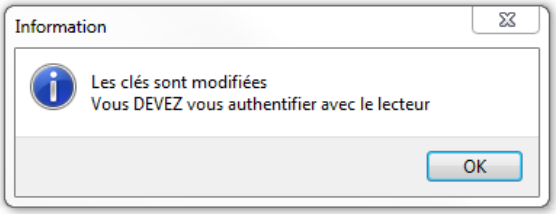
Afin de changer les valeurs de ces clés, il suffit de cocher les cases « Signature » et/ou « Chiffrement », de renseigner la nouvelle valeur. Puis de cliquer sur le bouton « Changer les clés ».

Note :

- ✓ Le bouton permet de restaurer les valeurs par défaut d'un champ.
- ✓ Les clés de l'encodeur **ET** du logiciel doivent être les mêmes afin que les deux éléments puissent communiquer.
- ✓ Si la case « *Changer uniquement les clés SECard* » est cochée, seules les clés du logiciel seront changées.



- ✓ Lors du changement des clés utilisateurs du logiciel et de l'encodeur, une fenêtre apparaîtra réclamant une authentification.



Attention

Il est important de connaître les clés utilisateurs en cours.
Si celles-ci venaient à être perdues, il ne serait plus possible de communiquer de façon sécurisée avec le lecteur.
Seul le mode « *En clair* » resterait exploitable si celui-ci est autorisé.

Modes de communication autorisés de l'encodeur

Permet d'autoriser / interdire certains modes de communication entre l'encodeur et SECard.

Afin d'autoriser un mode, il suffit de cocher la case du mode souhaité (il est possible d'autoriser plusieurs modes) et de cliquer sur le bouton « *Set modes* ».
Ceux n'étant pas cochés seront donc interdits.

Afin de les autoriser à nouveau, il suffira de relancer la commande dans un mode de communication autorisé tout en prenant soin de valider les modes souhaités.

Attention

Si le mode « *En clair* » n'est plus autorisé **et** que les clés utilisateurs sont perdues, il ne sera alors plus possible de communiquer avec l'encodeur.

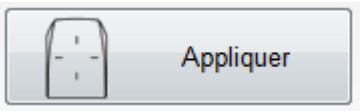
Il sera nécessaire de retourner le matériel en usine pour réinitialisation.

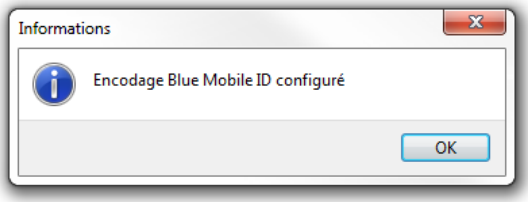
Encodage Blue Mobile ID

Permet de configurer l'encodeur Bluetooth (ARCS-W35-G-BT1-5AA) pour autoriser ou non l'encodage du smartphone en état de veille.

- Nécessite le déverrouillage du téléphone pour la Configuration.
  Si la case est cochée, le téléphone doit être déverrouillé pour encoder la configuration.

- Nécessite le déverrouillage du téléphone pour la VCard
  Si la case est cochée, le téléphone doit être déverrouillé pour encoder la carte virtuelle.

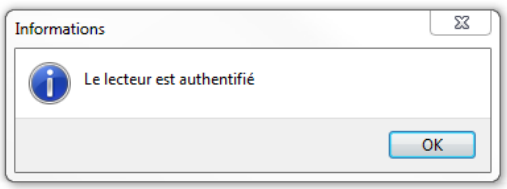
Valider le choix en cliquant sur le bouton : 



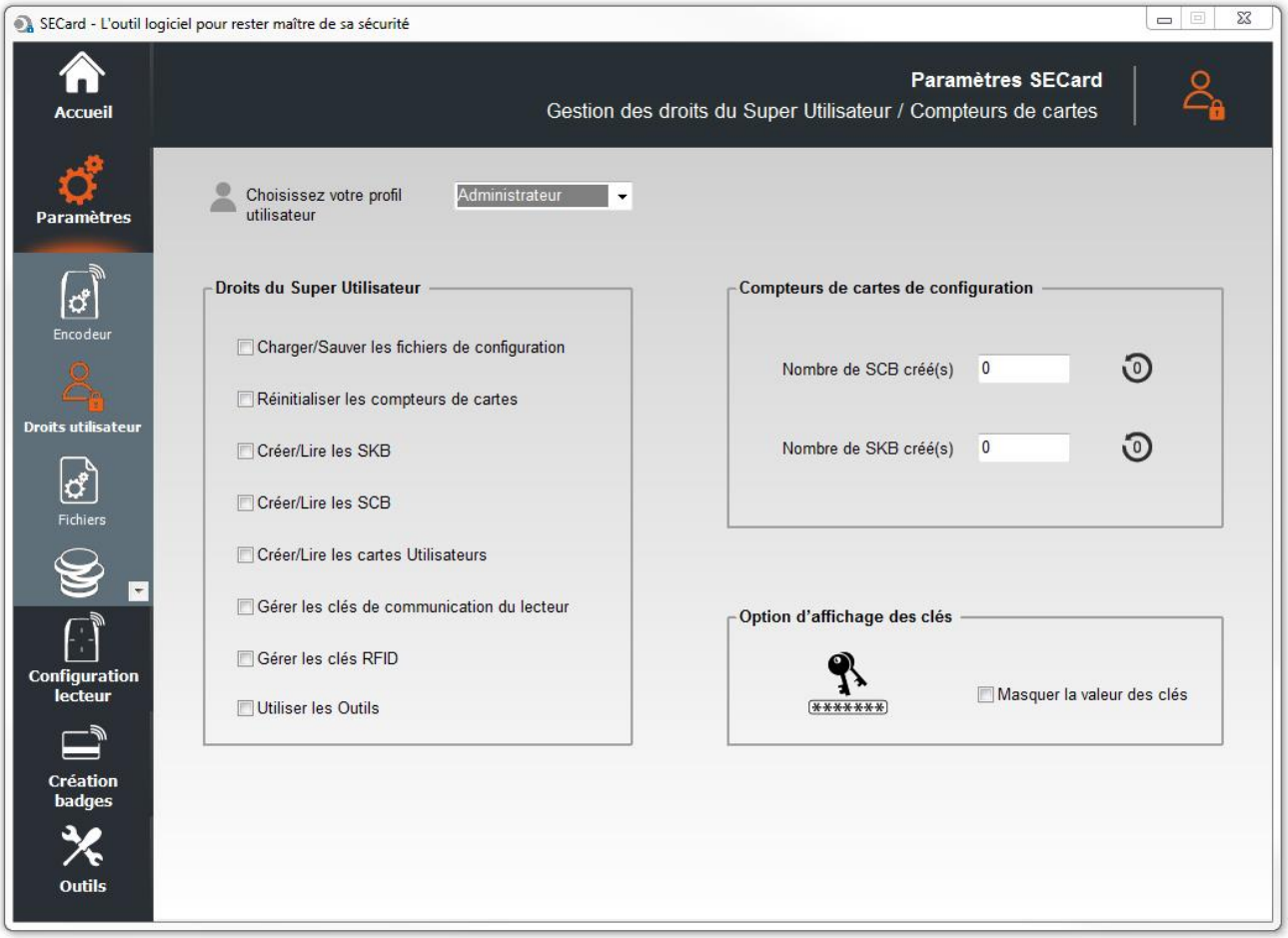
Connecter

Lors de l'alimentation du lecteur encodeur, celui-ci allume la LED blanche et émet un bip sonore.

Afin de vérifier les paramètres de communication avec l'encodeur, utiliser le bouton « *Connecter* ». Si la communication a été correctement configurée, le lecteur réagira par un signal sonore et lumineux. De plus une fenêtre d'acquittement apparaîtra à l'écran.



II. 2 - Droits Utilisateur



Changement du niveau d'accès

Permet de changer le niveau d'accès. Il faut connaître le mot de passe du niveau visé.
Changements autorisés :

- Administrateur vers Super Utilisateur et Utilisateur.
- Super Utilisateur vers Utilisateur et Administrateur

Droits du Super Utilisateur

Le mode « *Super Utilisateur* » est la transition entre les modes « *Administrateur* » et « *Utilisateur* ».
L'administrateur attribue les droits au Super Utilisateur.

Compteurs de cartes de configuration

Compteurs de visualisation du nombre de badges de configuration SCB créé et du nombre de badges de SKB créé.

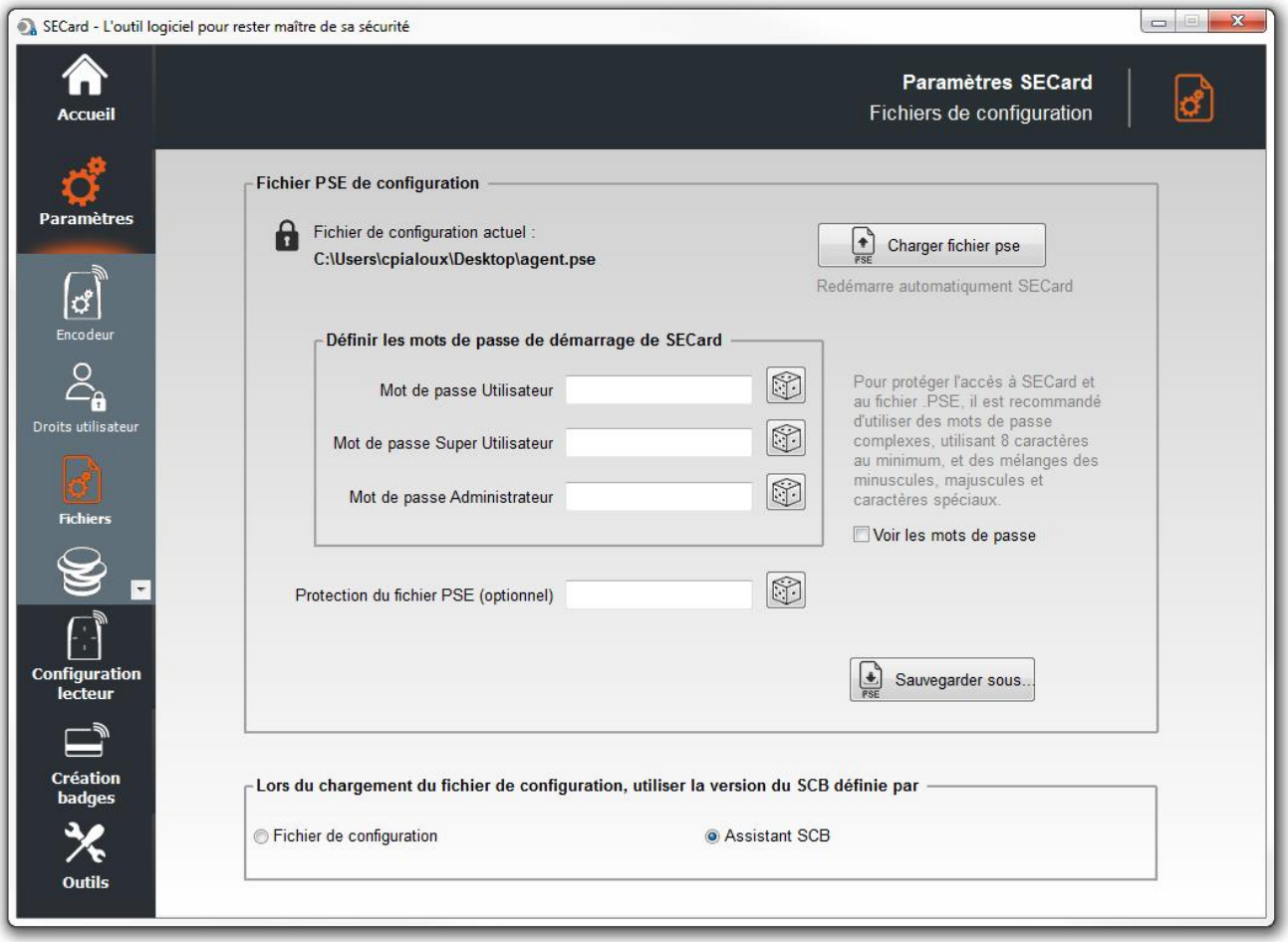
Ces valeurs peuvent être réinitialisées grâce aux boutons de reset par l'Administrateur ou, Super Utilisateur si autorisé.
Remarque : ces valeurs sont sauvegardées dans le fichier .pse.

Option d'affichage des clés

Il est possible de cacher les clés dans les champs clés du logiciel en cochant cette case.

Cette option est activable par l'Administrateur et est effective dans les modes Super Utilisateur ou Utilisateur.

II. 3 - Fichiers



Lors du chargement du fichier de configuration, utiliser la version du SCB définie par

La version du SCB est contenue dans le fichier de configuration .pse.
Il est possible de :

- conserver la version de SCB en cochant « Fichier de configuration »
  SECard récupère automatiquement la version du firmware dans le fichier .pse qui a été chargé et choisi la version de SECard compatible.

- choisir la version de SCB compatible avec le firmware du lecteur à configurer en cochant « Wizard SCB ».
  Ce choix se fait dans l'assistant SCB.

Fichier PSE de configuration

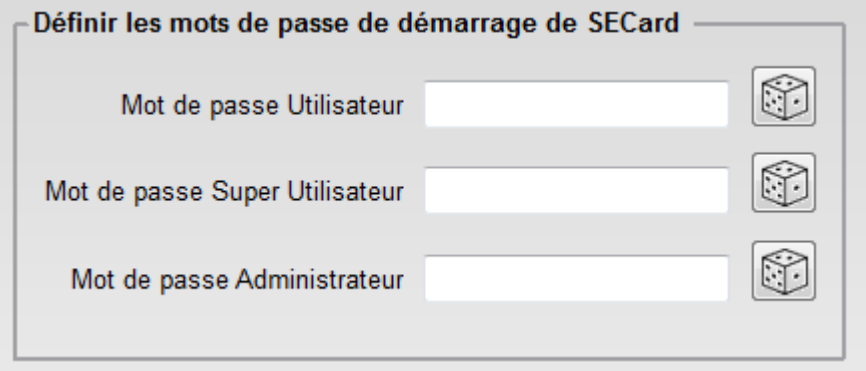
Les mots de passe de connexion sont contenus dans le fichier de configuration.
Cette page permet de sauvegarder le fichier de configuration contenant tous les paramètres de la configuration courante (clés, formats, lecteur,…). Vous pouvez sélectionner un emplacement, les mots de passe de connexion (Administrateur, Super Utilisateur et Utilisateur) et le mot de passe de lecture.

Lors du chargement d'un fichier de configuration (.pse), SECard revient automatiquement sur la fenêtre de connexion pour la saisie des mots de passe propres au ficher .pse.

Recommandations sur la sauvegarde des fichiers de configuration .pse *(cf.T15 - Recommandations sur la sauvegarde des fichiers PSE*

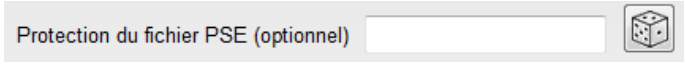
Sauver sous…

- Mots de passe pour le login de SECard.



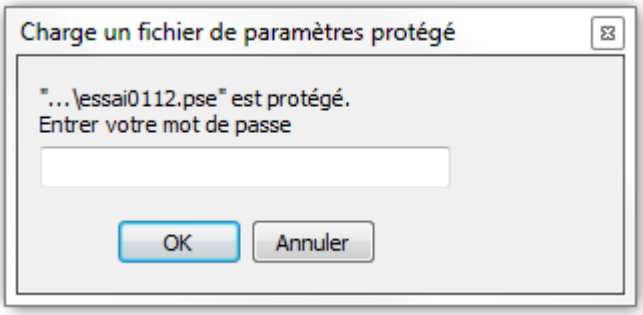
 *Générateur aléatoire de Mot de Passe permet de générer ces logins :*

Remarque : ces mots de passe sont nécessaires pour ouvrir SECard sur le fichier pse chargé dans la fenêtre de Login.

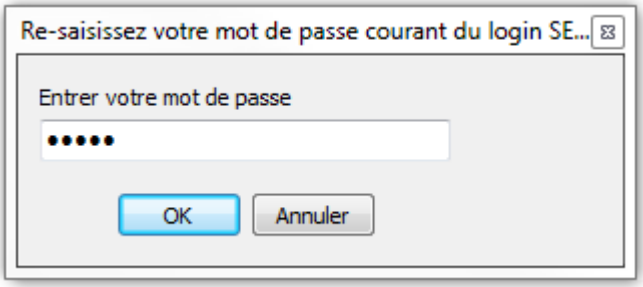
- 

Il s'agit du mot de passe de lecture du fichier .pse. Il est facultatif.

Remarque : il est demandé lorsqu'un fichier .pse est chargé dans SECard :



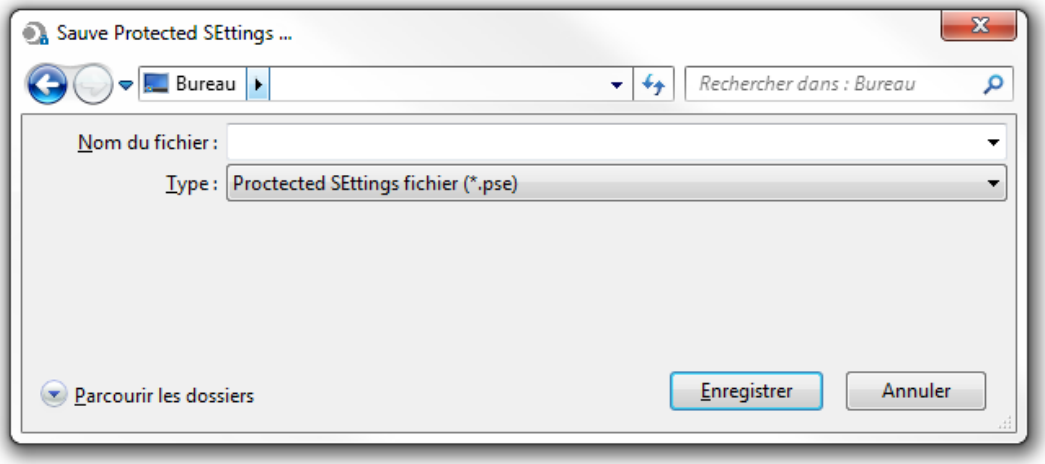
- Lorsqu'on clique sur le bouton Sauver sous… une fenêtre apparait demandant de saisir le mot de passe **administrateur pour le login de SECard** courant :



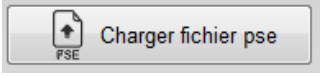
Par exemple STidA, si c'est le fichier SECard.pse par défaut qui a été chargé.

Remarque : un Super Utilisateur ayant le droit de « charger/sauver les fichiers de configuration » ne peut pas changer les mots de passe de LOGIN.

Une seconde fenêtre s'ouvre permettant de sélectionner l'emplacement pour la sauvegarde du fichier :

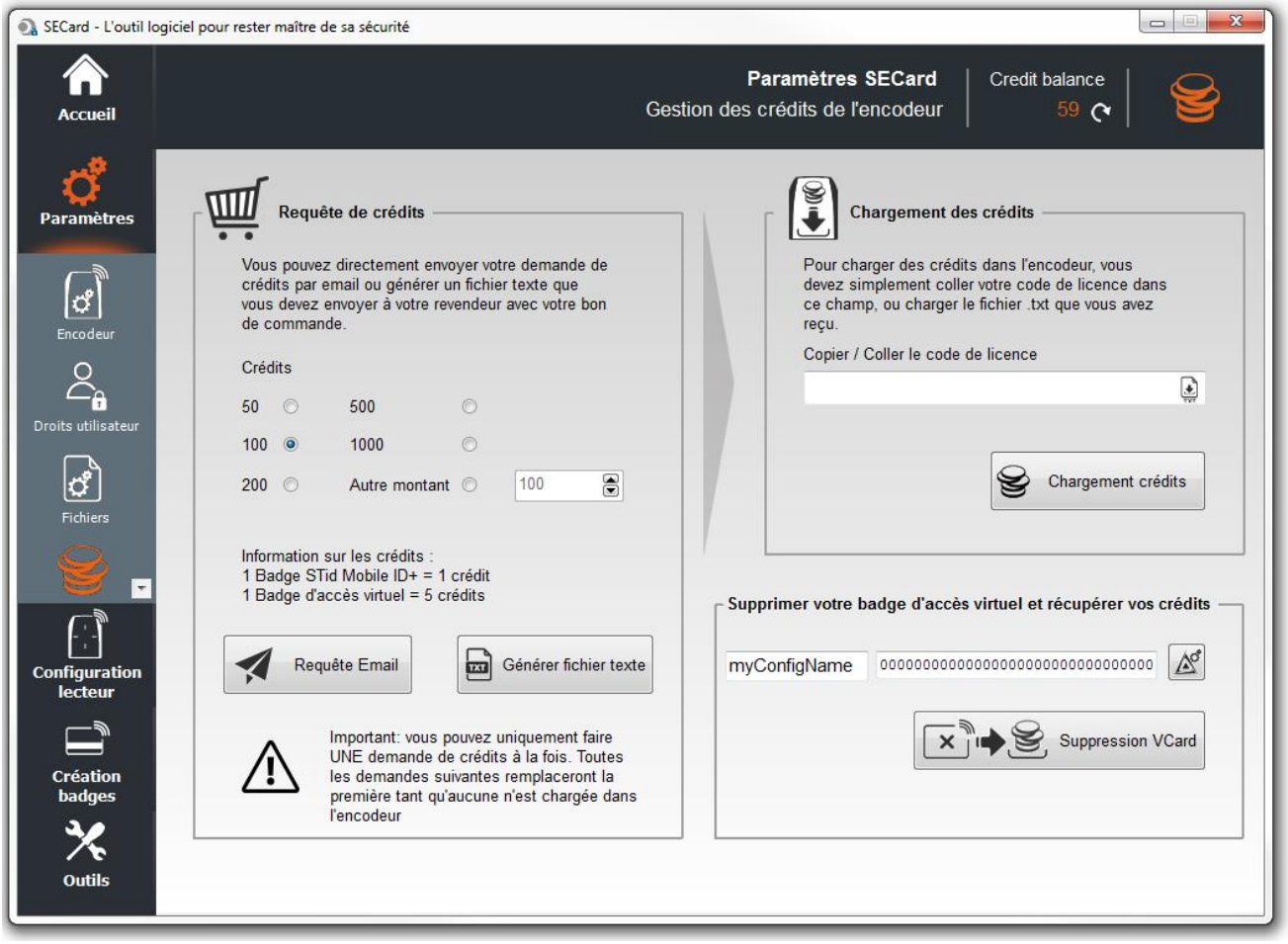


Une fois le nom et l'emplacement renseigné, cliquer sur Enregistrer.

- 

: charger un fichier .pse dans SECard sans passer par l'écran de démarrage.

II. 4 - Crédits Bluetooth



Principe : pour encoder des badges utilisateurs virtuels dans le téléphone, il faut acheter des crédits d'encodage qui seront chargés dans l'encodeur. La demande de crédits se fait par l'intermédiaire du Kit SECard.

ANDROID Google play | iOS Available on the App Store

STid propose trois badges d'accès :

Demande de Crédits

Cette partie du logiciel permet d'effectuer une demande de crédit auprès de votre fournisseur.

Deux méthodes sont proposées :

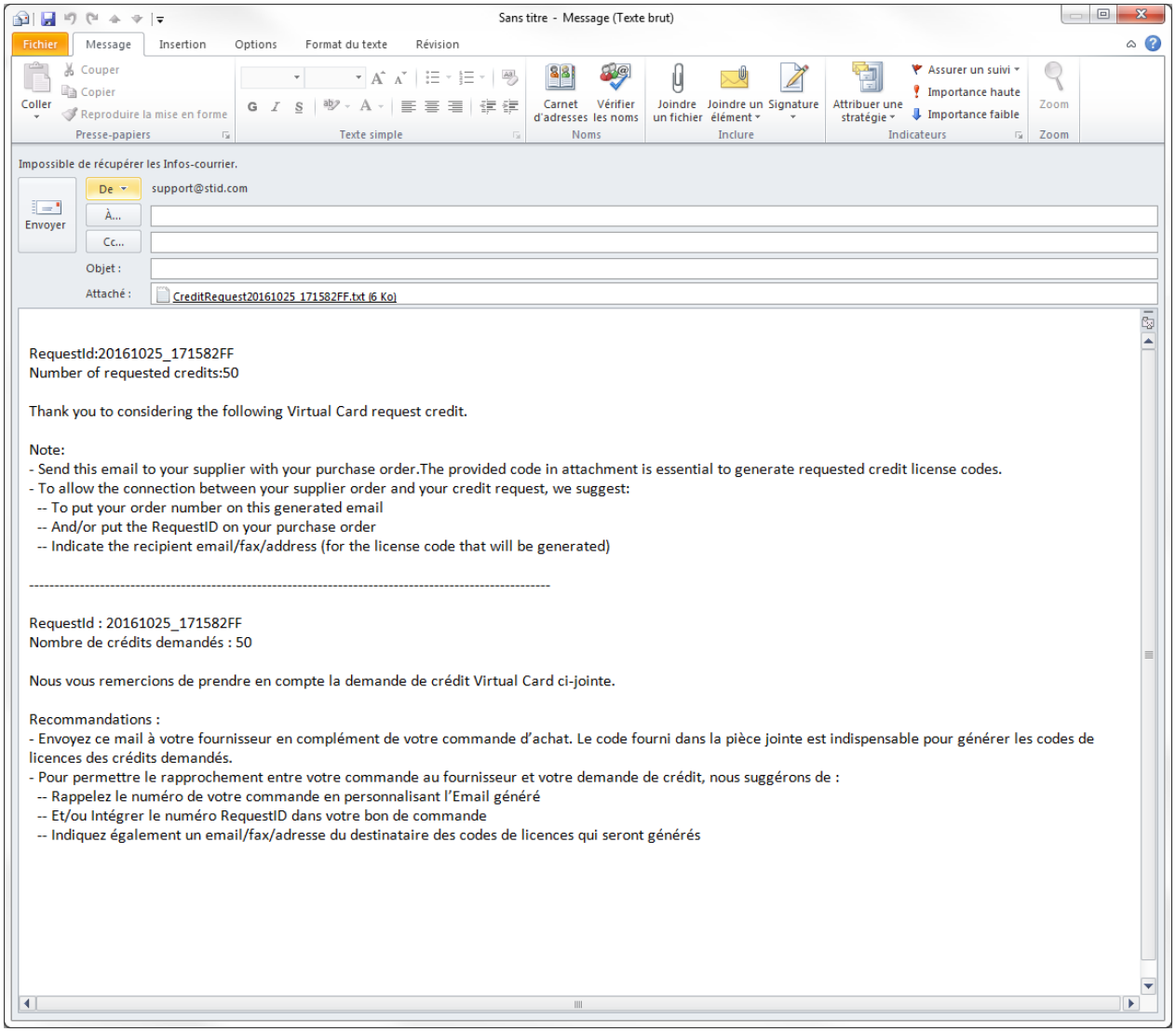
- « Demande par mail » si le poste sur lequel est installé SECard a une connexion internet et un logiciel de messagerie actif
- « Générer un fichier texte » qui pourra être envoyé par mail ou tout autre moyen.

Requête Email

Sélectionner le nombre de crédits désirés et cliquer sur 

.

Une fenêtre de votre messagerie email s'ouvre :



Suivre les instructions du message.

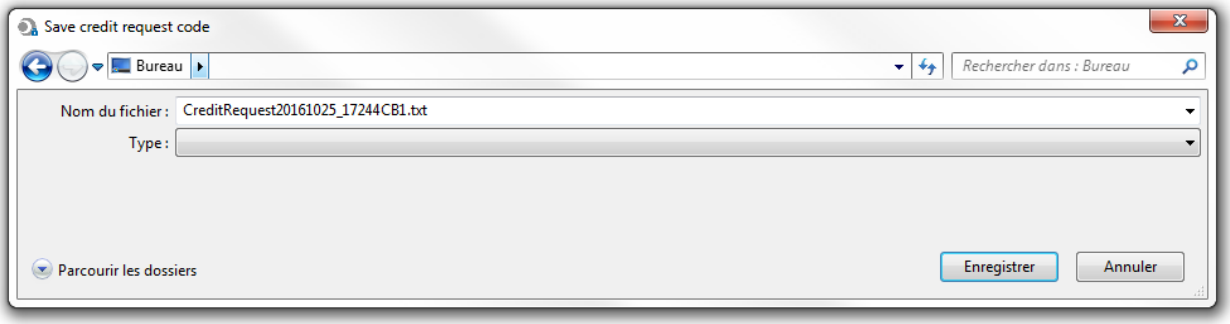
Attention : vous ne pouvez faire qu'une seule demande de crédits à la fois. Toute autre demande de crédits remplacera la précédente si le code de licence généré par la première demande n'a pas été utilisé.

Générer un fichier texte

Sélectionner le nombre de crédits désirés et cliquer sur 

.

Une fenêtre s'ouvre pour choisir l'emplacement pour l'enregistrement du fichier :

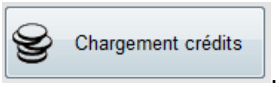


Envoyer un email à votre fournisseur avec votre bon de commande et le document en pièce-jointe. Le code fourni en pièce-jointe est indispensable pour générer les codes de licence des crédits demandés.

Pour permettre le rapprochement entre votre commande au fournisseur et votre demande de crédit, nous suggérons :

- Rappeler le numéro de votre commande sur votre email
- Et / ou intégrer le numéro RequestID dans votre bon de commande
- Indiquer l'adresse e-mail / fax / adresse du destinataire (pour le code de licence qui sera généré)

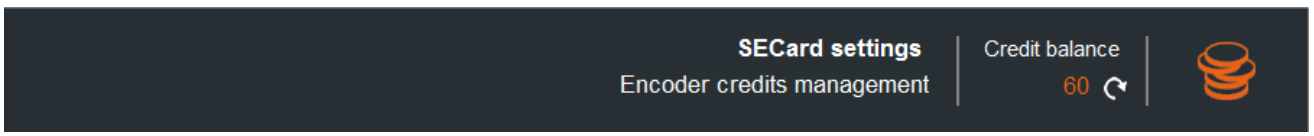
Chargement des crédits

1- Connecter l'encodeur qui a générer la demande de crédit.
2- Entrer le code licence fournit.
3- Cliquer sur 

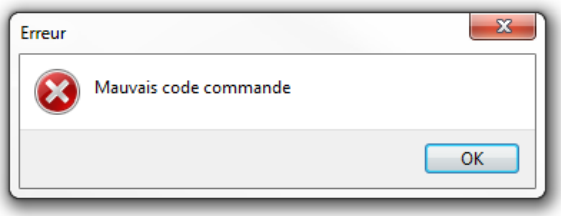
.

Solde de crédits

Permet de connaitre le solde de crédits disponible dans l'encodeur.
Le nombre de crédits est affiché comme ci-dessous :

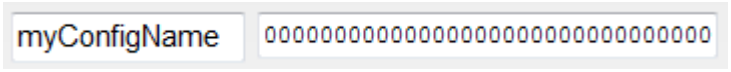


Si l'encodeur connecté n'est pas un encodeur Blue et que des commandes de gestion de crédits sont envoyées à l'encodeur le message d'erreur suivant s'affichera :



Supprimer votre badge d'accès virtuel et récupérer vos crédits

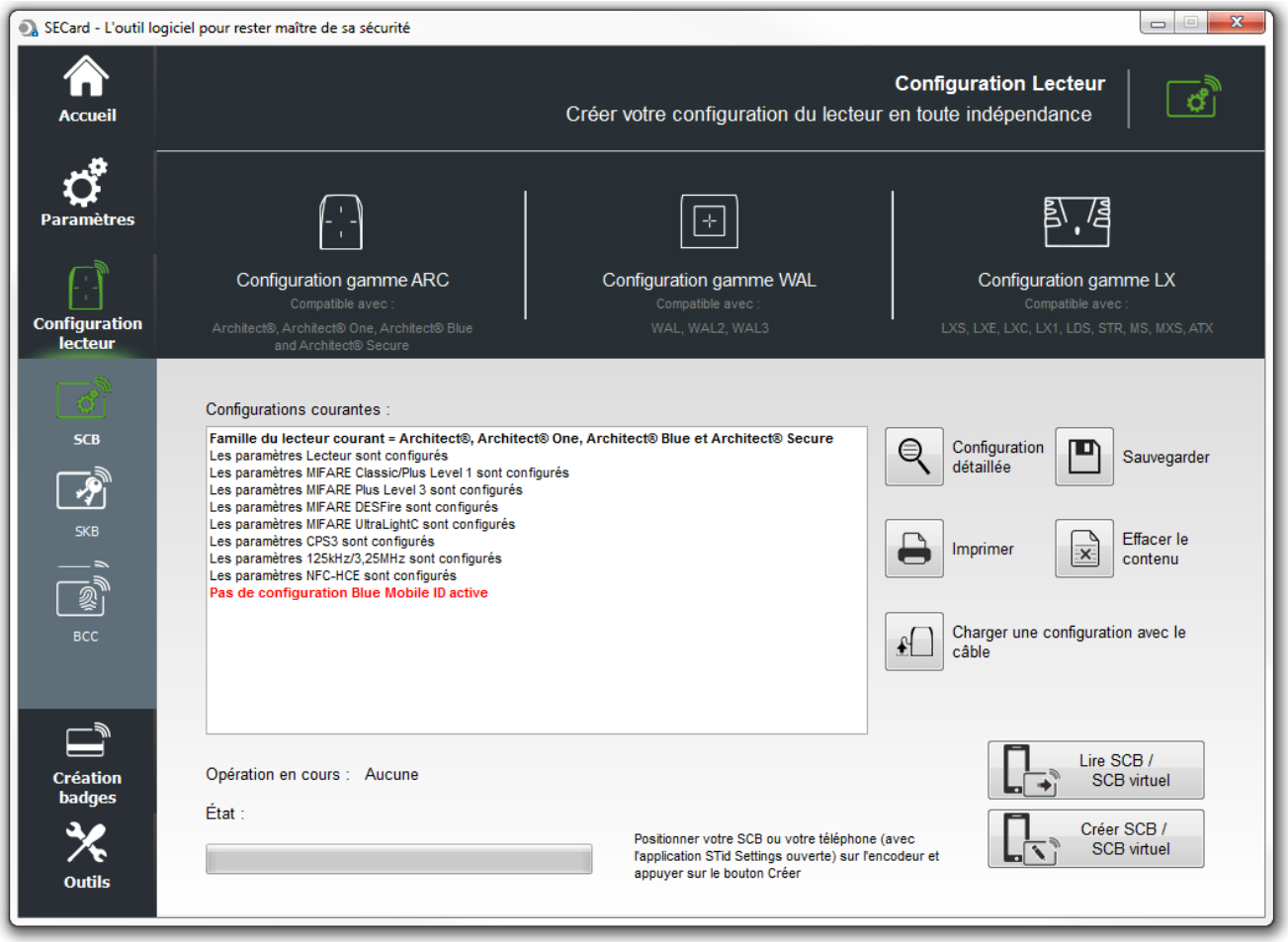
En mode Administrateur :
Renseigner le nom de la configuration et la clé d'écriture utilisées pour créer la carte virtuelle et cliquer sur Supprimer Carte. Les crédits sont automatiquement rechargés dans l'encodeur.

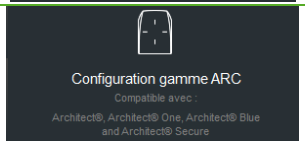
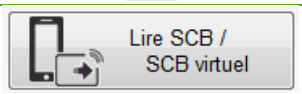
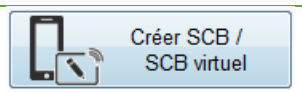



Permet de charger les paramètres de la configuration courante dans les champs.

En mode Super Utilisateur et Utilisateur :
Possibilité de supprimer uniquement une VCard correspondant à la configuration chargée.

III. Configuration lecteur – SCB

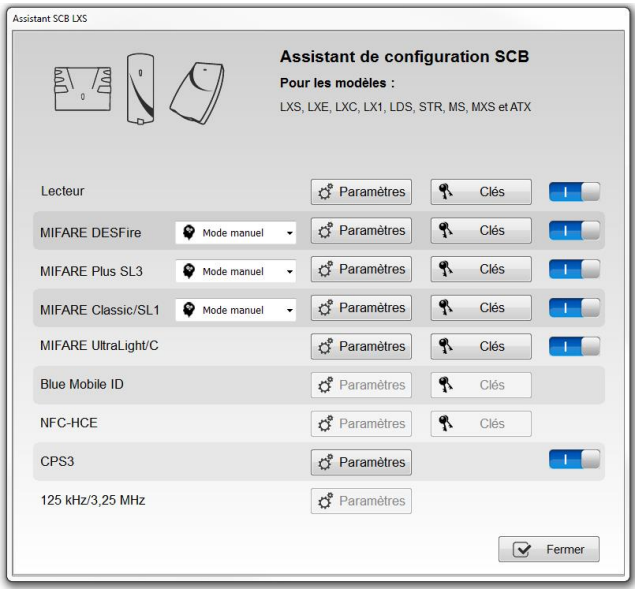


	Permet d'ouvrir l'assistant de configuration pour les lecteurs : LXS, LXE, LXC, LX1, LDS, STR, MS, MXS, WAL et ATX
	Permet d'ouvrir l'assistant de configuration pour les lecteurs : WAL (WAL, WAL2, WAL3)* *à partir du firmware Z18
	Permet d'ouvrir l'assistant de configuration pour les lecteurs : Architect®, Architect® One, Architect® Blue et Architect® Secure
	Permet d'imprimer les informations de configuration contenues dans la fenêtre.
	Permet de sauvegarder les informations de configuration contenues dans la fenêtre dans un fichier .rtf.
	Permet d'effacer les informations de configuration contenues dans la fenêtre.
	Permet d'afficher les informations détaillées des configurations courantes.
	Permet de charger la configuration dans le lecteur par la communication série.
	Permet de lire un badge de configuration SCB. Utilise la clé entreprise SCB définie dans l'assistant de configuration.
	Permet de créer un badge de configuration SCB ou SCB virtuel selon les paramètres définis dans l'assistant de configuration.

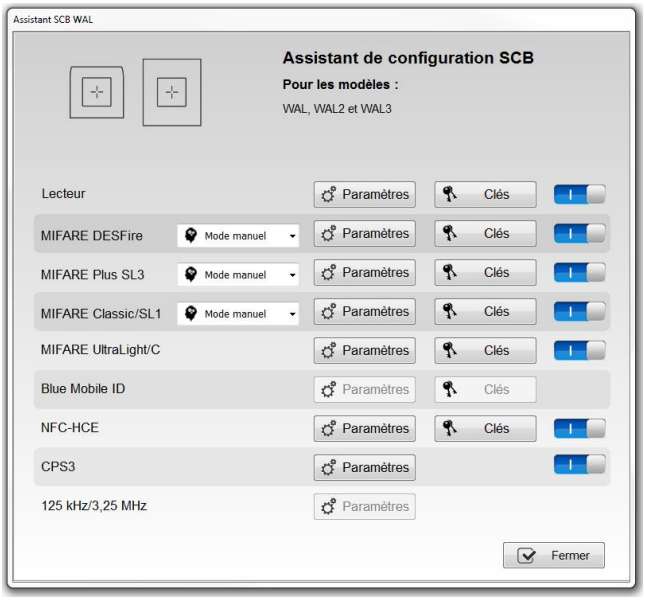
Cette version de SECard (V3.x.x) permet de créer la configuration des lecteurs de la gamme standard (LXS, LXE, LX1…), de la gamme WAL et de la gamme Architect® (ARC, ARC One, ARCS et ARCS Blue).

Pour se faire, le logiciel dispose de trois Assistants de configuration :

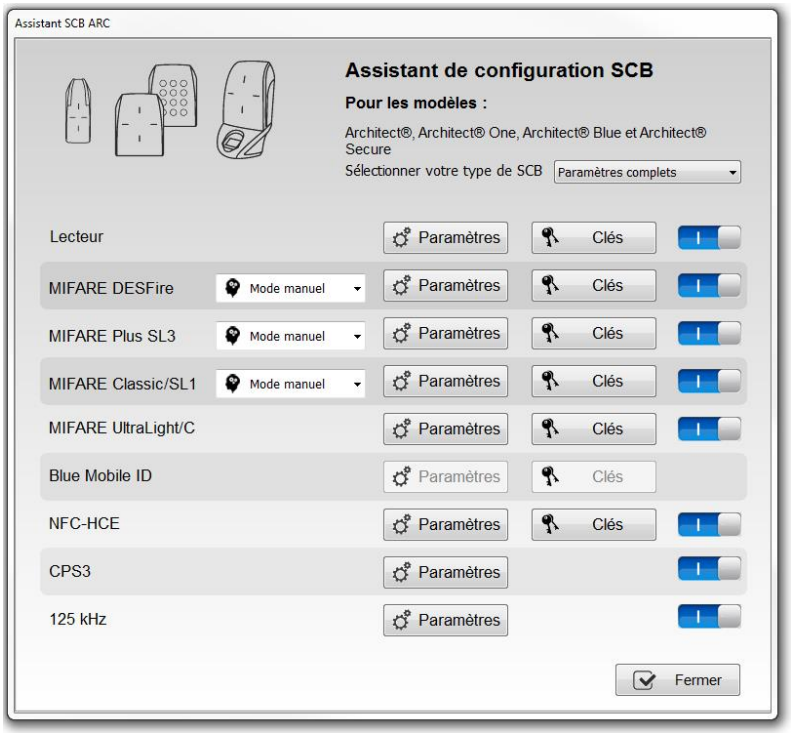
« Configuration gamme LX » pour la gamme standard



« Configuration gamme WAL» pour la gamme WAL



« Configuration gamme ARC » pour la gamme Architect®



Lorsque la configuration des paramètres est validée, le bouton passe sur la position 1  .

Ces boutons permettent d'activer ou désactiver la prise en compte des configurations.

<u>Remarque</u> :

- **pour les WAL dont le Firmware est inférieur ou égal à Z17, utiliser l'assistant « Configuration gamme LX ».**
- **les paramètres Moneo sont abandonnés à partir de la version 3.0.**

Charger une configuration avec le câble

A partir de la version 3.1.0, la configuration peut être chargée dans le lecteur par sa liaison série.

Quand tous les paramètres ont été renseignés dans l'assistant de configuration :

1- Dans « Paramètres de communication série » choisir le bon numéro de port de communication.

2- Connecter le lecteur ARC-R3x à configurer via un câble convertisseur au PC.

3- Cliquer sur « Envoi SCB via série » pendant que la LED clignote en orange au démarrage pour les lecteurs séries (R32, R33 et R35), à n'importe quel moment pour les lecteurs TTL (R31).

Création des badges SCB

A partir de la version V3.0.x de SECard, les badges de configuration SCB doivent être créés avec les technologies de badges ci-dessous :

Type de puce à utiliser (Réf STid)
MIFARE® DESFire® EV1/ EV2 non locked 4ko MIFARE® DESFire® EV1/ EV2 non locked 8ko

Il est possible de réutiliser un badge SCB dès lors que l'on connait sa clé Maître.

Attention

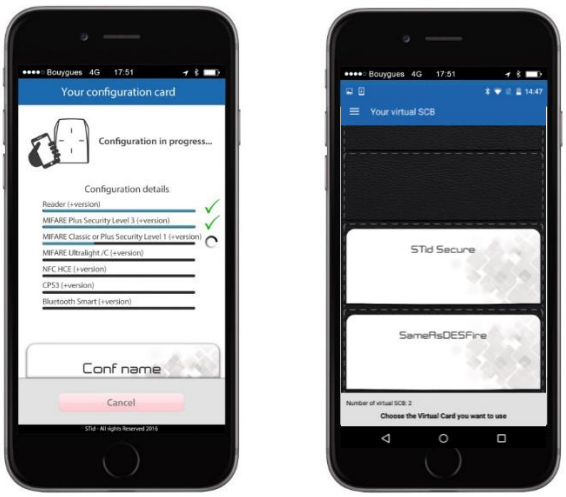
Il n'est pas possible de changer la référence d'un lecteur avec un *SCB.*

Exemple : un lecteur LXS-R31-E-103-xx ne pourra pas être reconfiguré en LXS-R31-E-PH5-xx.
Il est nécessaire de retourner le produit en usine pour un changement de référence.

Création des badges virtuels SCB (pour lecteur Bluetooth et application STid Mobile ID uniquement)

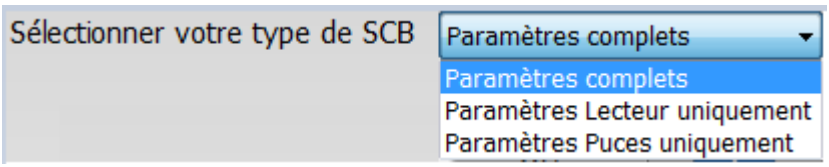
A partir de la version V3.0.x de SECard intégrant le paramétrage des lecteurs Bluetooth, les badges de configuration peuvent être créés en virtuel sur un smartphone sous Android ≥5 ou IOS ≥ 8.
Un smartphone peut contenir plusieurs badges virtuels de configuration.

L'application STid settings est requise.



III. 1 - Assistant SCB ARC : paramètres lecteurs

Niveau SCB

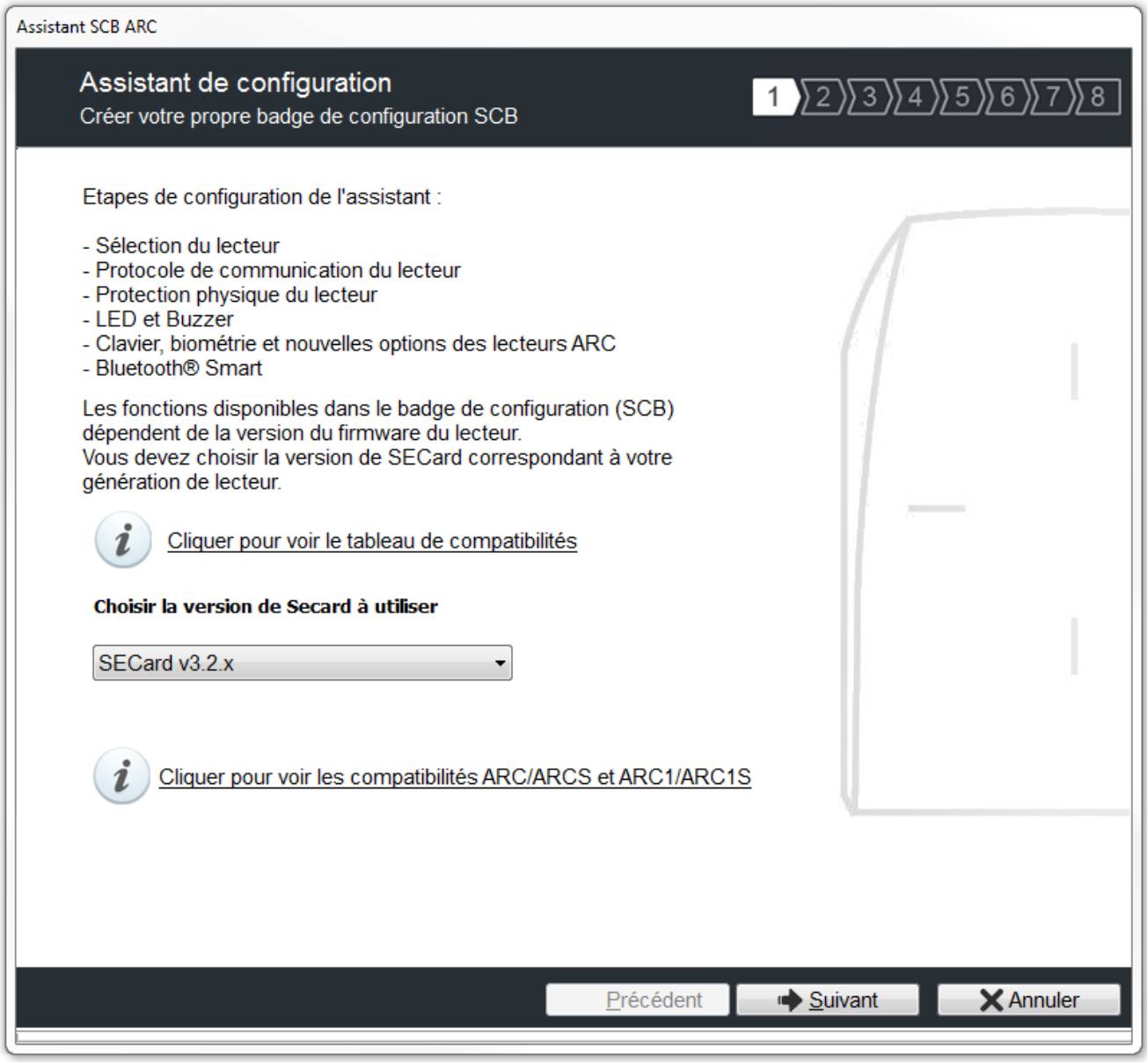


Permet de choisir les paramètres qui seront encodés dans le badge SCB.

- Tous les paramètres : les paramètres lecteur **et** puces seront encodés dans le badge SCB.
- Uniquement lecteur : seuls les paramètres de configuration et les clés du lecteur seront encodés.
- Uniquement puces RFID : seuls les paramètres et les clés des puces seront encodés, les paramètres lecteurs ayant été configurés via l'UHF ou via un autre badge SCB.

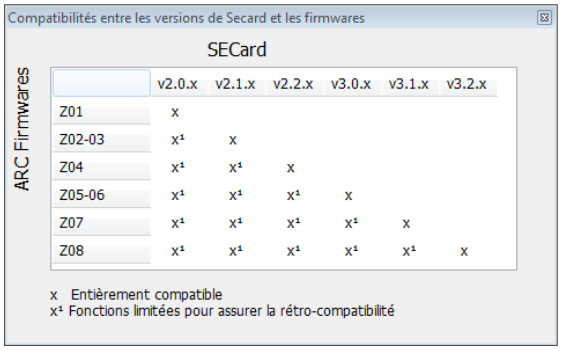
Lecteur « Paramètres » : la configuration du lecteur se fait en huit étapes, pour passer d'une étape à l'autre il faut cliquer sur « Suivant ».

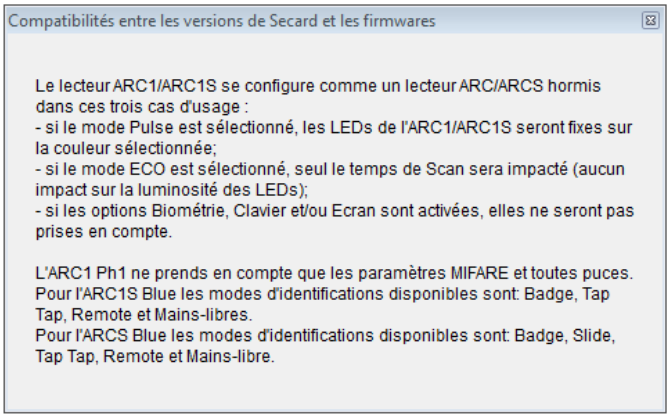
 Cliquez-ici	Assistant de configuration / Choix de la version de SECard
 Cliquez-ici	Sélection du lecteur
 Cliquez-ici	Protocole de communication du lecteur
 Cliquez-ici	Protections physiques du lecteur
 Cliquez-ici	LED et Buzzer
 Cliquez-ici	Clavier, biométrie et options des lecteurs ARC
 Cliquez-ici	Options écran tactile
 Cliquez ici	Options Blue Mobile ID



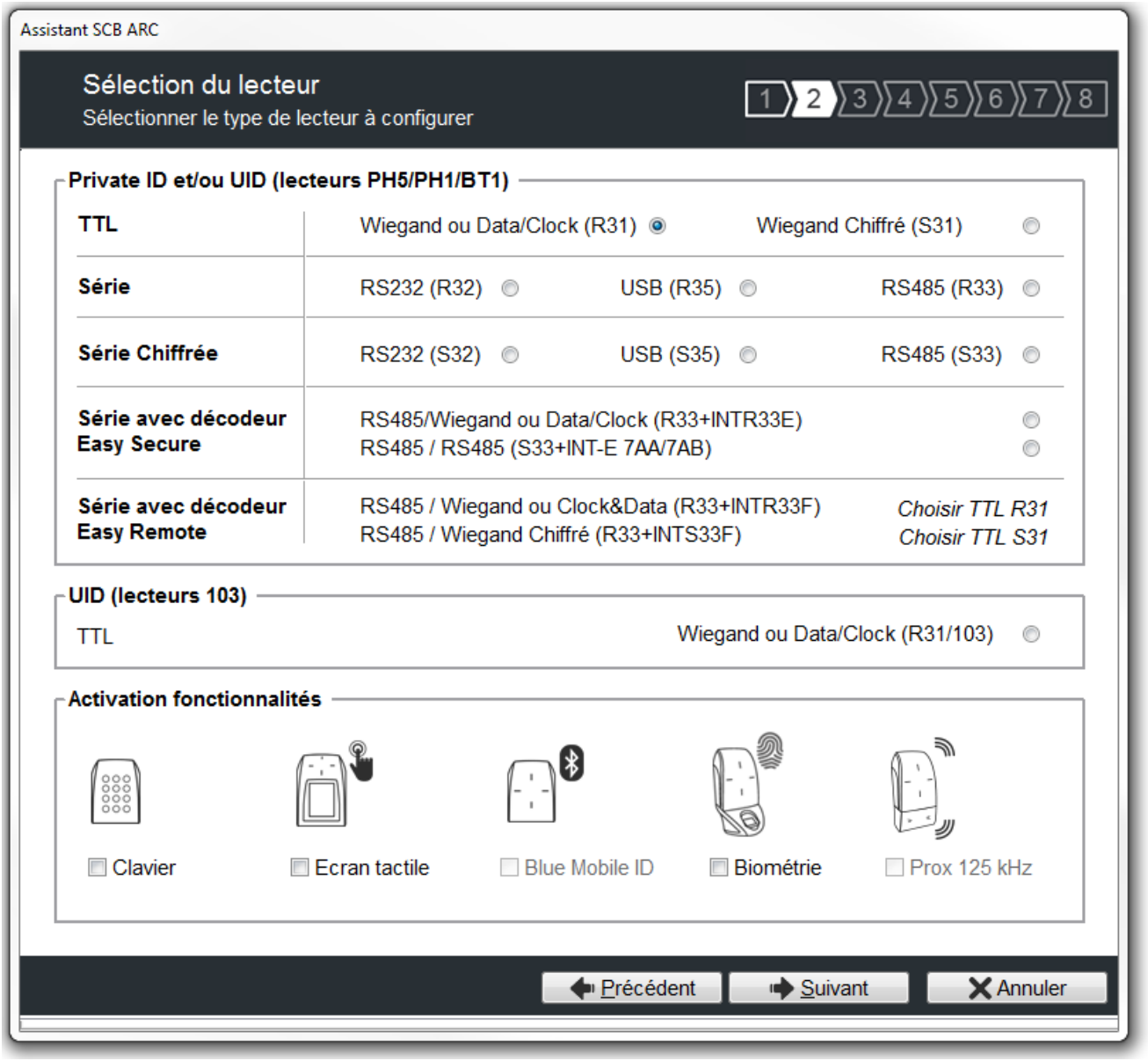
Les fonctionnalités disponibles et la compatibilité des badges SCB dépendent de la génération de firmware des lecteurs.

Pour assurer la compatibilité entre les différentes versions de SCB et de firmware, SECard donne le choix à l'utilisateur de la version de SECard à utiliser si l'option a été validée dans l'onglet « *Fichiers* ».*cf. II. 3 - Fichiers.*





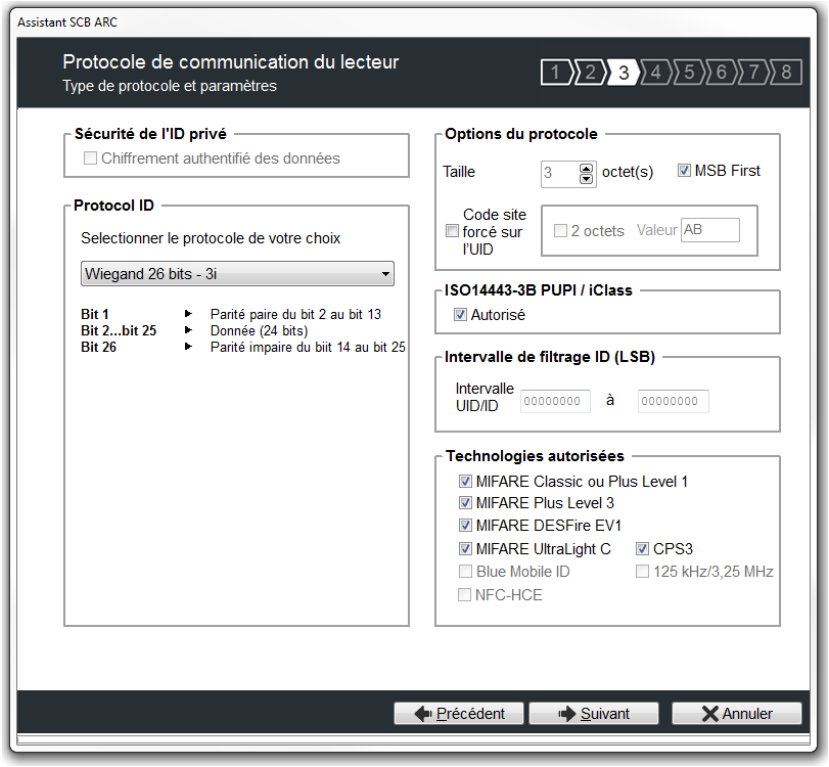
Pour connaître la version du firmware, se reporter au paragraphe *T2.1 - Mise sous tension*.

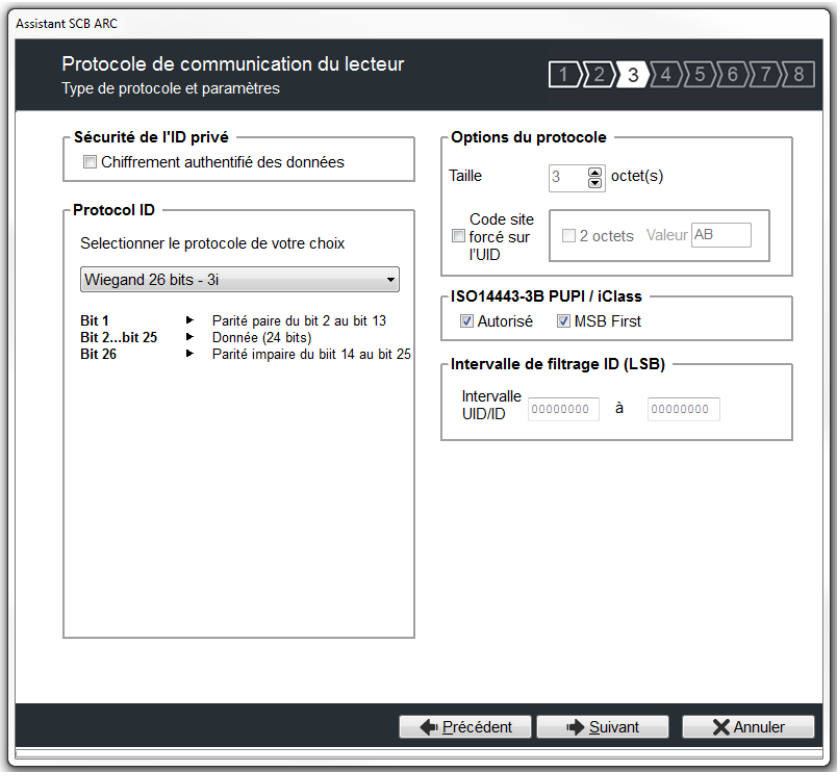


Cette étape permet :

- De choisir le type de lecteur à configurer.
- D'activer la configuration clavier.
- D'activer la configuration écran tactile.
- D'activer la configuration Blue Mobile ID.
- D'activer la configuration biométrique.
- D'activer la configuration du module 125kHz.

Cette fenêtre apparait lorsque le type de lecteur sélectionné à l'étape 2 est R31/103 :





Cette fenêtre apparait lorsque le type de lecteur sélectionné à l'étape 2 est en sortie TTL :

Protocole

Il contient les différents protocoles de communication TTL supportés par le lecteur.

Pour plus d'information sur les protocoles se reporter au paragraphe *T4 - Au sujet des protocoles de communication TTL*.

Note : lors de l'encodage d'un identifiant, celui-ci est réalisé au format du protocole en cours (Exemple : Décimal 13 caractères pour le protocole 2B – 10 caractères en hexadécimal pour le protocole 3Cb).

Options du protocole

- « *Taille* » permet d'ajuster la taille des protocoles personnalisables.

  Taille maximum en Wiegand : 48 octets
  Taille maximum en Data/Clock : 10 octets

- « *Code site forcé sur l'UID* » permet de forcer un code site quel que soit le protocole de communication. La valeur du code sera transmise en poids fort sur un ou deux octets. L'UID peut donc être tronqué selon le protocole utilisé. Cette option n'est pas disponible pour le Wiegand 64 bits - 3T.

ISO 14443-3B PUPI / iClass

Il est possible de gérer différemment les PUPI ISO14443-3B et 14443-2B exclusivement en calculant un code d'authentification de message utilisant une fonction de hachage cryptographique (SHA1) en combinaison avec une clé secrète (HMAC-SHA1). Les autres types de modulation (ISO14443-A) et fréquences (125 kHz / 3,25 MHz) ne sont pas affectés par cette option.

Si la taille du protocole est inférieure à 20 octets, un troncage LSB sera effectué sur les 20 octets de signature obtenus.
Si la taille du protocole est supérieure à 20 octets, un padding à zéro sera effectué.

Intervalle de filtrage ID (LSB)

Il est possible de restituer un UID/ID uniquement si celui-ci est compris dans une plage spécifique bornée sur 4 octets.

Si la taille de l'UID/ID est supérieure à 4 octets, l'intervalle s'effectuera sur les 4 octets LSB (prise en compte de l'option MSB First au préalable). Les bornes sont incluses, limite basse ≤ UID/ID ≤ limite haute.

Si l'UID/ID est compris dans l'intervalle, le lecteur restituera le code suivant le protocole en cours et effectuera une action badge LED + Buzzer (SCB). Dans le cas contraire, le lecteur allumera la LED rouge + Buzzer durant 400ms (non paramétrable et non désactivable).

L'UID/ID comparé est la valeur hexadécimale après prise en compte du paramètre MSB First et avant mise en forme protocolaire.
Par exemple pour un protocole 2S, le code comparé sera le code sur 4oct avant codage au format 2S.

Technologies autorisées

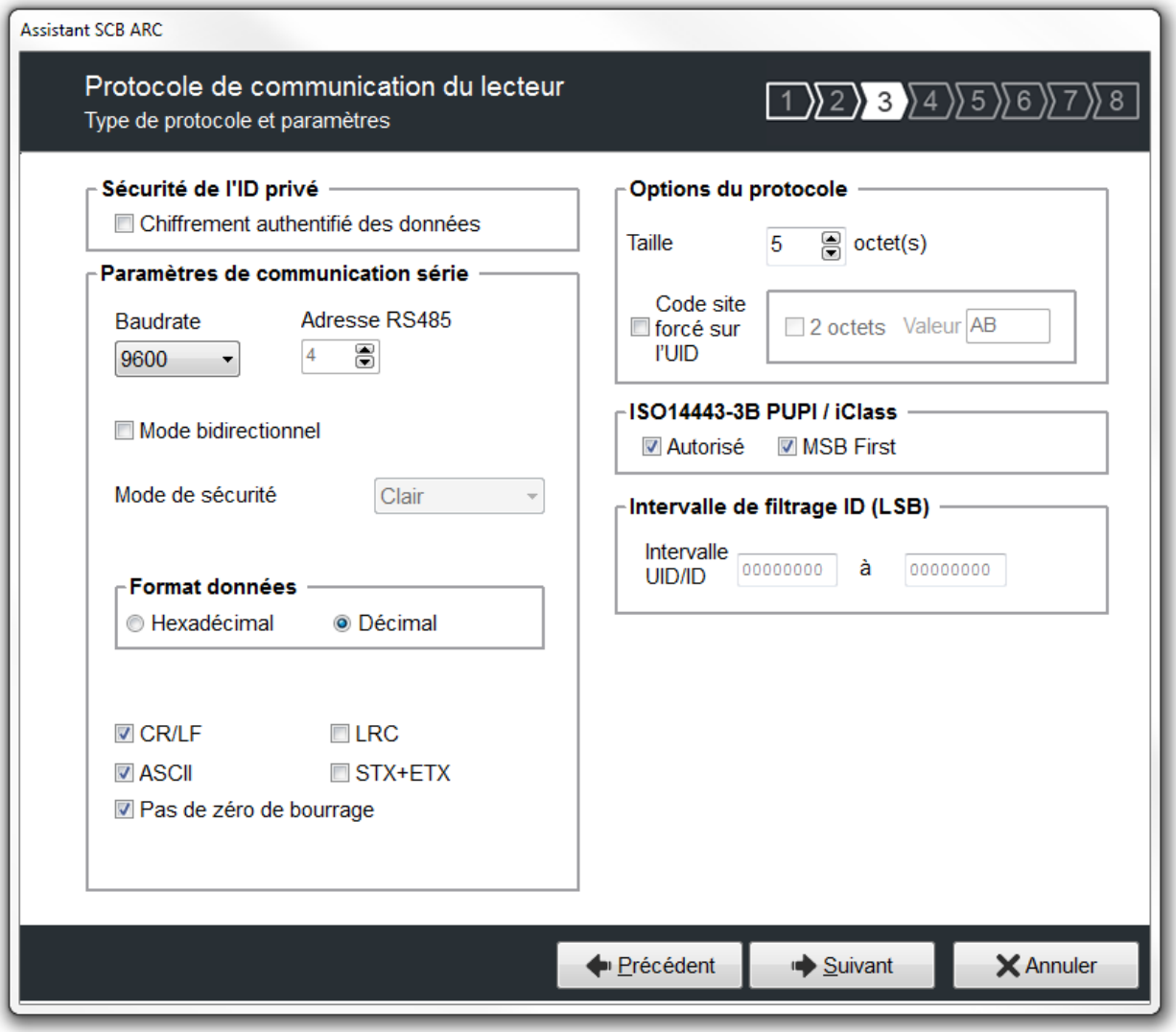
Lorsque le lecteur sélectionné est de type UID seul, cette liste permet de sélectionner le type de technologies de puce pouvant être lues par le lecteur.

Sécurité de l'ID privé

Les identifiants privés peuvent être chiffrés ET signés avant d'être écrits dans le badge. Le lecteur déchiffrera et authentifiera l'identifiant privé ainsi protégé avant de l'envoyer sur son média de sortie. Seul identifiant correctement déchiffré et authentifié produira un code de sortie, sinon le lecteur restera muet.
Le chiffrement-authentification utilise le mode AtE (Authenticate Then Encrypt).

Remarque : la taille de l'identifiant privé est limitée à 12 octets.

Cette fenêtre apparait lorsque le type de lecteur sélectionné à l'étape 2 est en sortie série :



Paramètres de communication série

Il contient les différents paramètres de communication série.

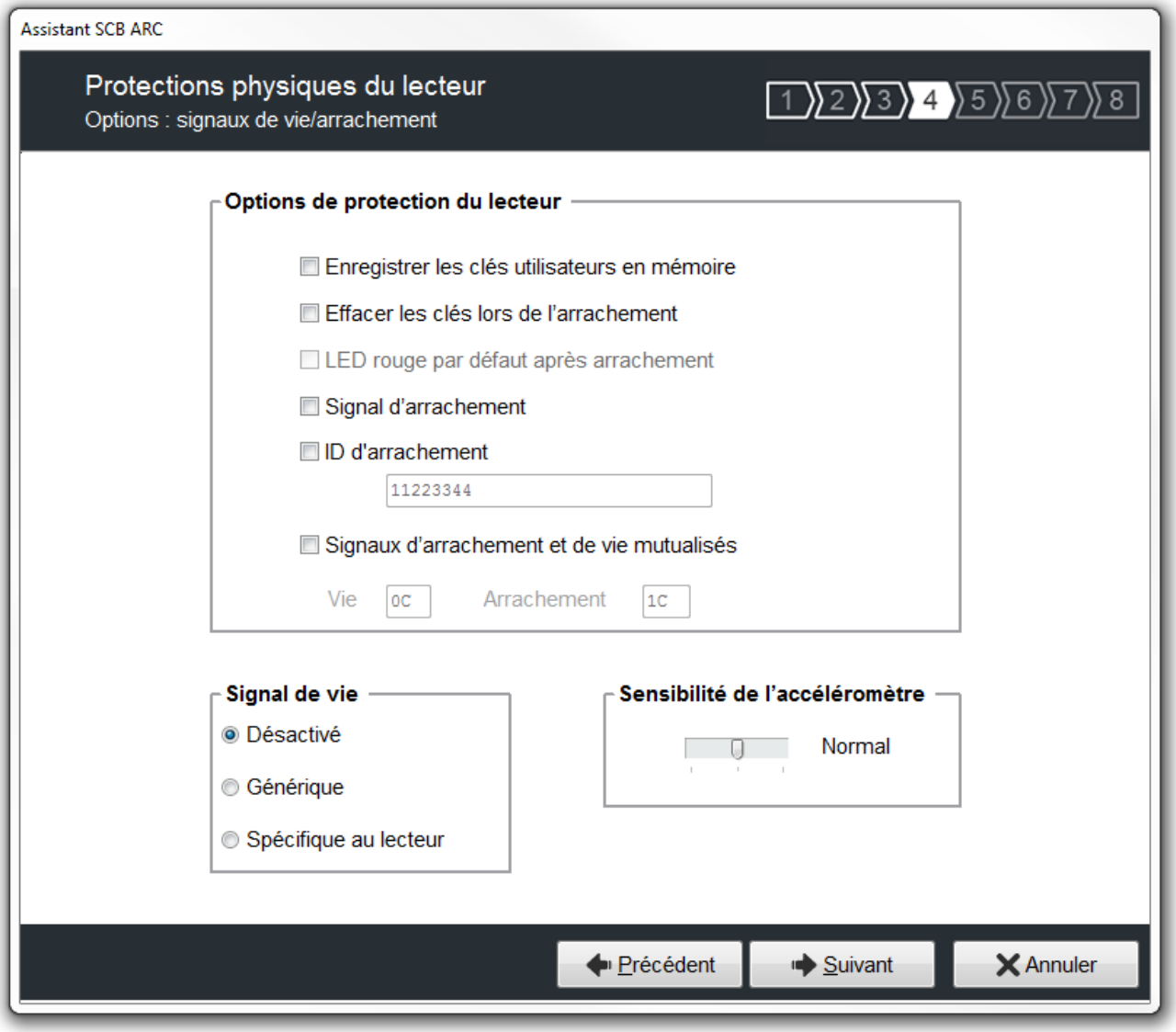
Pour plus d'information sur les protocoles se reporter au paragraphe *T5 - Au sujet des protocoles de communication Série*.

Options du protocole

« *Taille* » permet d'ajuster la taille des données.

Taille maximum en Wiegand : 48 octets
Taille maximum en Data/Clock : 10 octets

Note :
Il est possible d'augmenter la taille du champ au-delà des tailles maximums, pour cela, maintenir la touche CTRL enfoncée et cliquer dans le champ « *Taille données* », la valeur apparait alors soulignée. Cette manipulation ne fonctionne pas pour un encodage mais uniquement pour la relecture d'un identifiant. Uniquement disponible sur les lecteurs séries.



Options de protection du lecteur

- Enregistrer les clés utilisateurs en mémoire : permet de sauvegarder les clés, de façon chiffrée, en cas de coupure d'alimentation. Les clés sont enregistrées en EEPROM mémoire non volatile.
- Effacer les clés lors de l'arrachement : permet d'effacer toutes les clés du lecteur (sauf clé entreprise) si un changement d'état intervient sur l'accéléromètre du lecteur.
- LED rouge par défaut après arrachement : nécessite l'activation de l'arrachement.
  Si un changement d'état intervient sur l'accéléromètre du lecteur la LED passe sur la couleur rouge indiquant que les clés ont été effacées.
- Signal d'arrachement : permet d'activer le signal d'arrachement. Se reporter au paragraphe *T11 - Signal d'arrachement*
- ID d'arrachement : permet d'activer l'envoi d'une valeur spécifique dans une trame correspondant au protocole en cours. Se reporter au paragraphe *T12 - ID d'arrachement*
- Signaux d'arrachement et de vie mutualisés : permet d'activer l'envoi dans une trame d'un signal d'arrachement et de vie, disponible uniquement pour les lecteurs *R31*, *S31et R33+INTR33E*. Se reporter au paragraphe *T13 - Signal de vie / arrachement mutualisés.*.

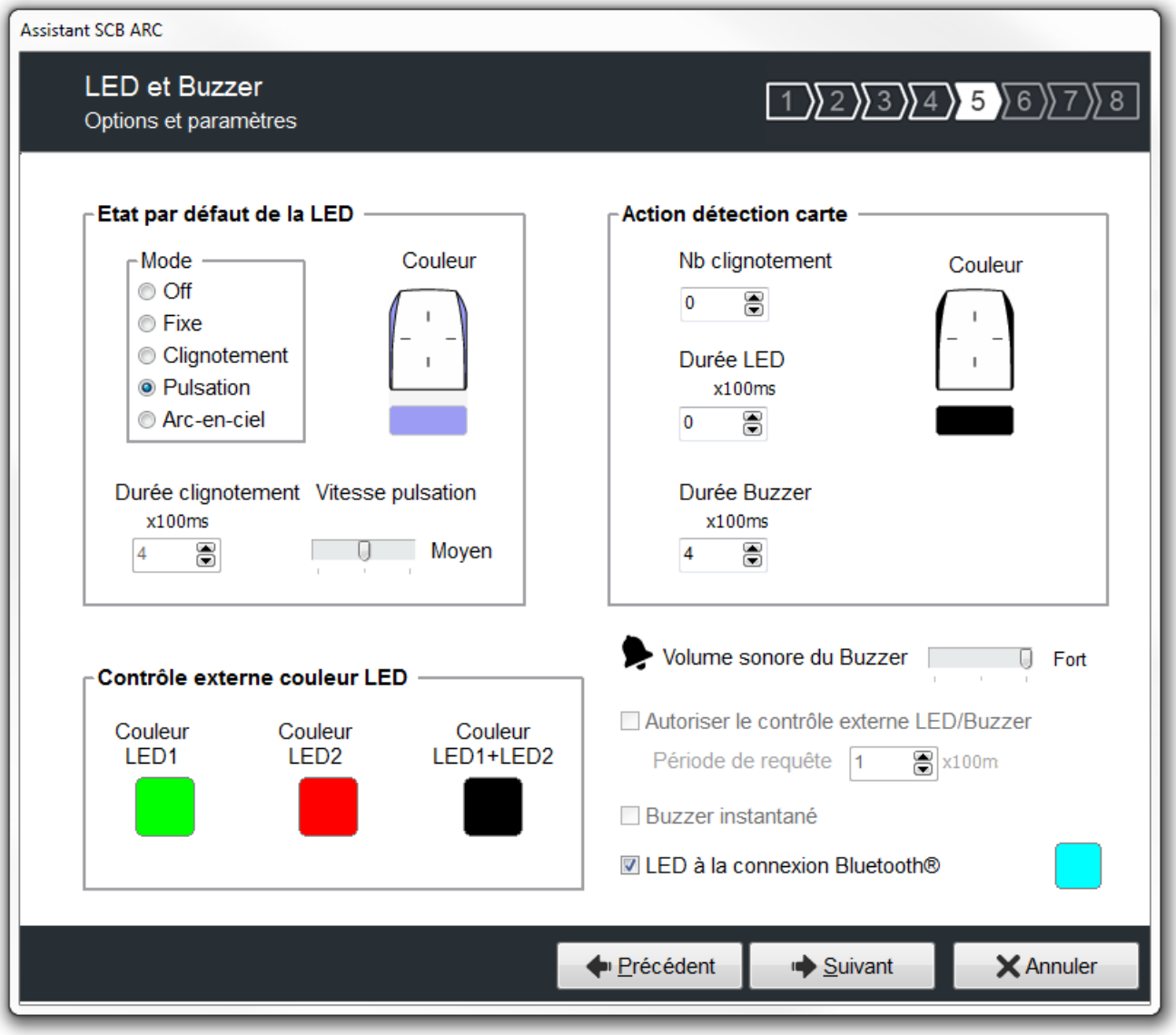
Note : il n'y a pas de gestion de l'arrachement sur les lecteurs USB.

Signal de vie

Permet d'activer / désactiver le signal et de choisir le type de signal « Générique » ou « Spécifique ».
Se reporter à *T10 - Signal* de vie.

Sensibilité de l'accéléromètre

Les lecteurs de la gamme ARC sont équipés d'un accéléromètre pour détecter l'arrachement du lecteur. En fonction du support / lieu d'installation du lecteur, il peut être nécessaire de régler la sensibilité du capteur afin que seul un arrachement effectif soit détecté.



Etat par défaut de la LED

Permet de définir l'état (couleur & mode de clignotement) de la LED en fonctionnement normal.
Sur la gamme ARC plusieurs modes sont disponibles :

- Off
- Fixe
- Clignotement classique
- Pulsation
- Arc-en-ciel

Le schéma à droite vous permet de visualiser l'effet sélectionné : le clignotement et la couleur.

Action détection carte

Permet de définir l'état (couleur & clignotement) de la LED et du buzzer lors de la détection d'un identifiant. Cette information est indépendante de l'acceptation de l'identifiant.

Nb clignotement ou Durée LED définit pour l'ARC écran le temps d'affichage de l'état « Image et texte détection badge ».

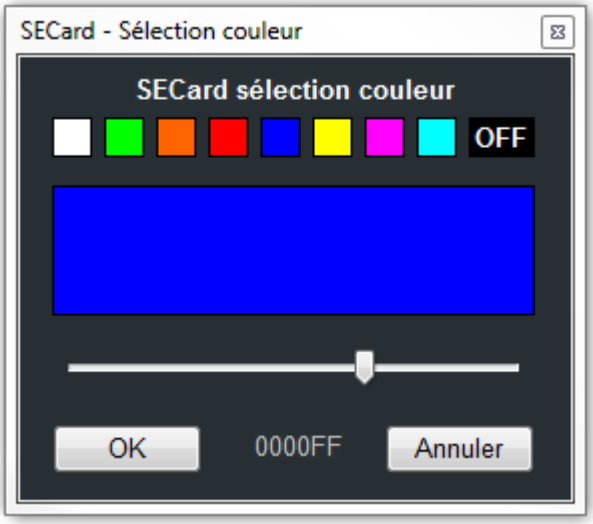
Volume sonore du Buzzer

Permet de définir le niveau sonore du buzzer **uniquement pour les ARCS, ARC1 et ARC1S.**

Contrôle externe couleur LED

Permet de définir la couleur de l'entrée LED1, de l'entrée LED2 et des deux entrées LED si elles sont commandées simultanément.

Pour modifier et sélectionner une couleur, cliquer sur le symbole de l'ARC ou sur les boutons de couleur, la fenêtre suivante s'ouvre :



Pour sélectionner une couleur prédéfinie, cliquer sur un des carrés de couleur.

Pour sélectionner une autre couleur, déplacer le curseur. La valeur qui s'affiche correspond au code RGB en hexadécimal de la couleur sélectionnée. Il est possible de copier la valeur en double cliquant dessus.

Autoriser le contrôle externe LED / Buzzer

Permet de contrôler la LED et le buzzer de façon externe. La période d'interrogation est réglable par pallier de 100ms. Disponible uniquement pour les lecteurs séries (R/S-32 et R/S-33) en mode bidirectionnel.

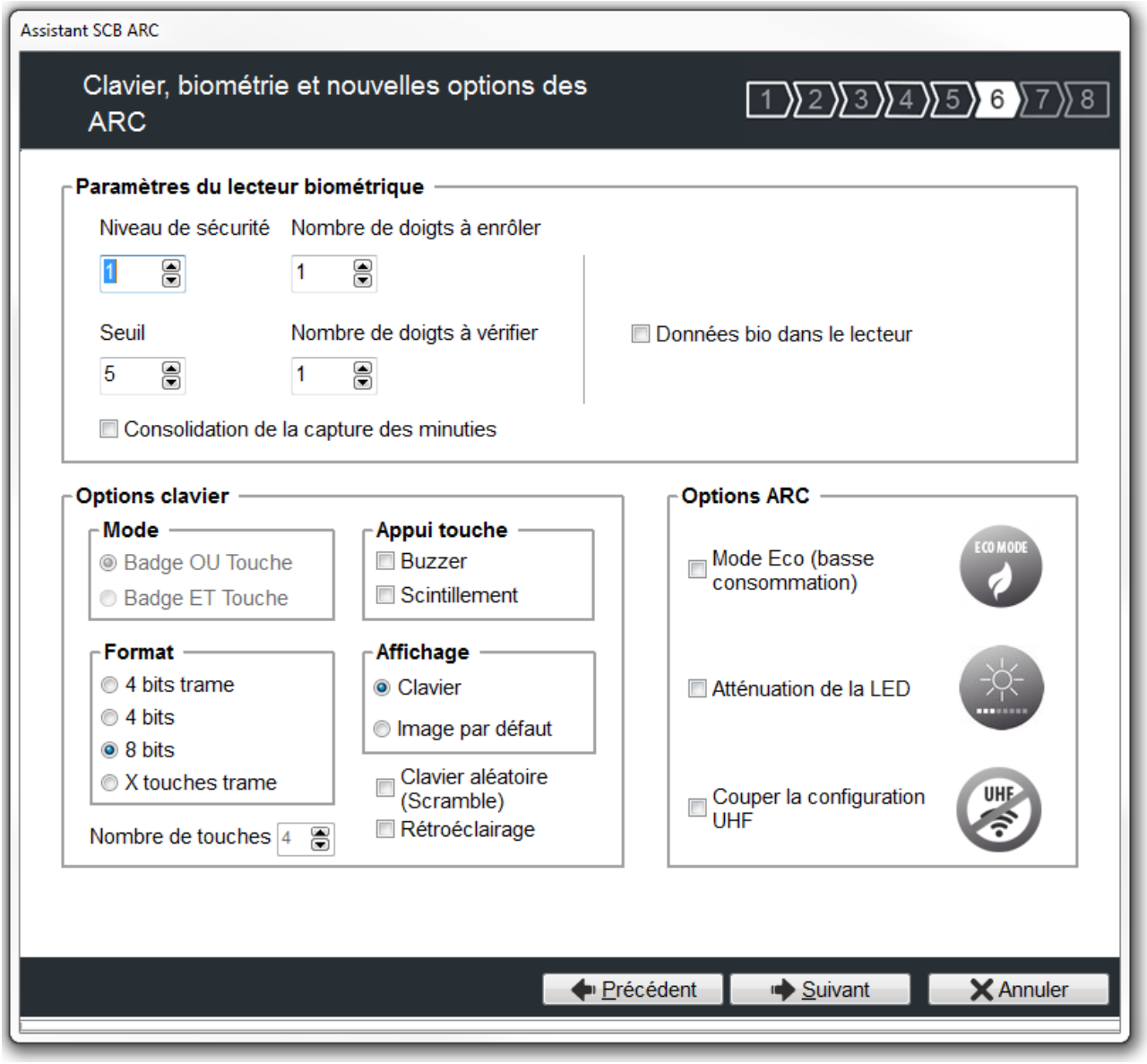
Buzzer instantané

Permet au lecteur d'activer le buzzer à chaque détection d'identifiant sans attendre de commande du système. Disponible uniquement pour les lecteurs séries (R/S-32 et R/S-33) en mode bidirectionnel.

LED à la connexion Bluetooth

Permet d'allumer brièvement la LED du lecteur lors de la connexion avec un smartphone. La couleur peut être sélectionnée en cliquant sur le carré de droite.

Cette action, indépendante de la détection du badge virtuel, permet d'informer l'utilisateur que la communication entre le smartphone et le lecteur est en cours.



Paramètres du lecteur biométrique

- Niveau de sécurité : représente le taux de fiabilité entre l'empreinte encodée dans la puce et celle lue par le capteur biométrique du lecteur.
  - Niveau de sécurité = 1 : niveau faible de sécurité de faux doigts (recommandé par Sagem Morpho),
  - Niveau de sécurité = 2 : niveau moyen de sécurité de faux doigts,
  - Niveau de sécurité = 3 : niveau élevé de sécurité de faux doigts.

- Seuil : représente la qualité de l'empreinte à encoder dans la puce de 0 à 10.
  Un seuil bas entraine moins de rejet. Recommandation Morpho Sagem : 5.

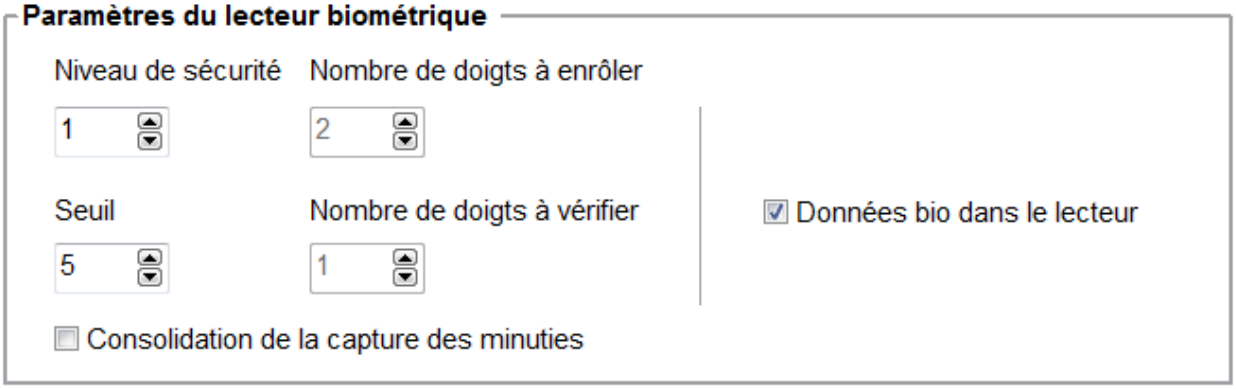
- Nombre de doigts à enrôler : représente le nombre de doigts à encoder dans la puce généralement les deux index.

- Nombre de doigts à vérifier : représente le nombre de doigts à vérifier sur le lecteur pour autoriser l'accès, généralement un doigt.

- Consolidation de la capture des minuties : permet de faire trois captures par doigt lors de l'encodage, le capteur biométrique retiendra la meilleure des trois empreintes.

Note : un ré-encodage avec un nombre de doigts différent nécessite un formatage de la puce.

❖ Données Bio dans le lecteur.



Lorsque ce mode est sélectionné, le nombre de doigts à enrôler est fixé à 2 et le nombre de doigts à vérifier est fixé à 1. La consolidation de la capture des minuties est activée par défaut.

Pour créer les Badges de Configuration Biométrique se reporter au menu 

.

Dans ce mode, l'encodage des templates dans le badge utilisateur n'est pas disponible.

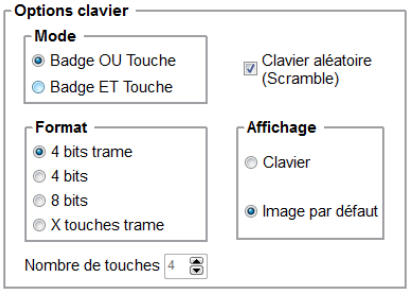
Attention : Il est de la responsabilité de l'utilisateur final de s'assurer de la conformité de son installation avec la réglementation locale en matière de gestion et stockage des données biométriques.

Pour plus d'information sur ce mode de fonctionnement se reporter à *T9 - Biométrie dans le lecteur.*

Options clavier

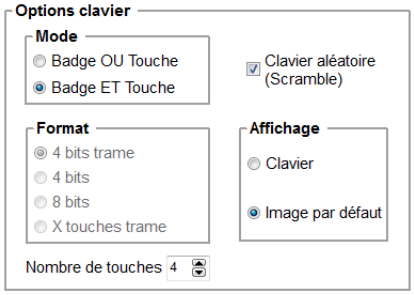
Permet de choisir entre les deux modes « Badge OU Touche » et « Badge ET Touche »

❖ Badge OU Touche + choix du format :



En cas de présentation d'un badge, son identifiant est immédiatement transmis suivant le protocole en cours, suivi d'un acquittement sonore.
En cas de frappe d'une touche, et suivant les modes de format définis dans l'encadré *Format*, sa valeur est immédiatement transmise suivant le protocole en cours, suivi d'un acquittement sonore.

❖ Badge ET Touche + nombre de touches :



Lorsque la séquence de touches est complète, le lecteur attend un identifiant pendant un délai de 6 secondes (émission d'un bip sonore pour indiquer l'attente de l'identifiant).

Pour plus de détail, sur le fonctionnement et le format, se reporter à *T6 - Au sujet des* lecteurs Clavier.

Attention

Le format Wiegand 26 bits n'est pas disponible en mode Badge ET Touche.

❖ Appui touche :

Permet d'activer / désactiver la LED et/ou le Buzzer lorsqu'un utilisateur appuie sur une touche du clavier.

❖ Affichage :

Permet de choisir l'affichage par défaut de l'écran tactile lorsque la fonction clavier est active.

- Clavier :
  Affiche le clavier par défaut à l'écran.

- Image par défaut :
  Affiche l'image et le texte par défaut (voir étape 7) à l'écran.

  Pour faire afficher le clavier toucher une première fois l'écran tactile.

  L'affichage repasse sur l'image par défaut après un timeout de 10s.

❖ Clavier aléatoire (Scramble) :

Disponible uniquement sur l'ARC écran. Permet d'activer le clavier aléatoire.

Le scramble est effectué en :

- Badge ET Touche :
  - après chaque séquence : saisie du nombre de touches configurées et lecture d'un badge valide.
  - après un time out de 6 secondes suivant la saisie du nombre de touches configurées et sans présentation d'un badge valide.
  - suite à l'annulation par la touche * ou #.

- Badge OU Touche :
  - après la lecture d'un badge valide.
  - toutes les 30 secondes. L'appui sur une touche ou la lecture d'un badge réinitialise le chrono.

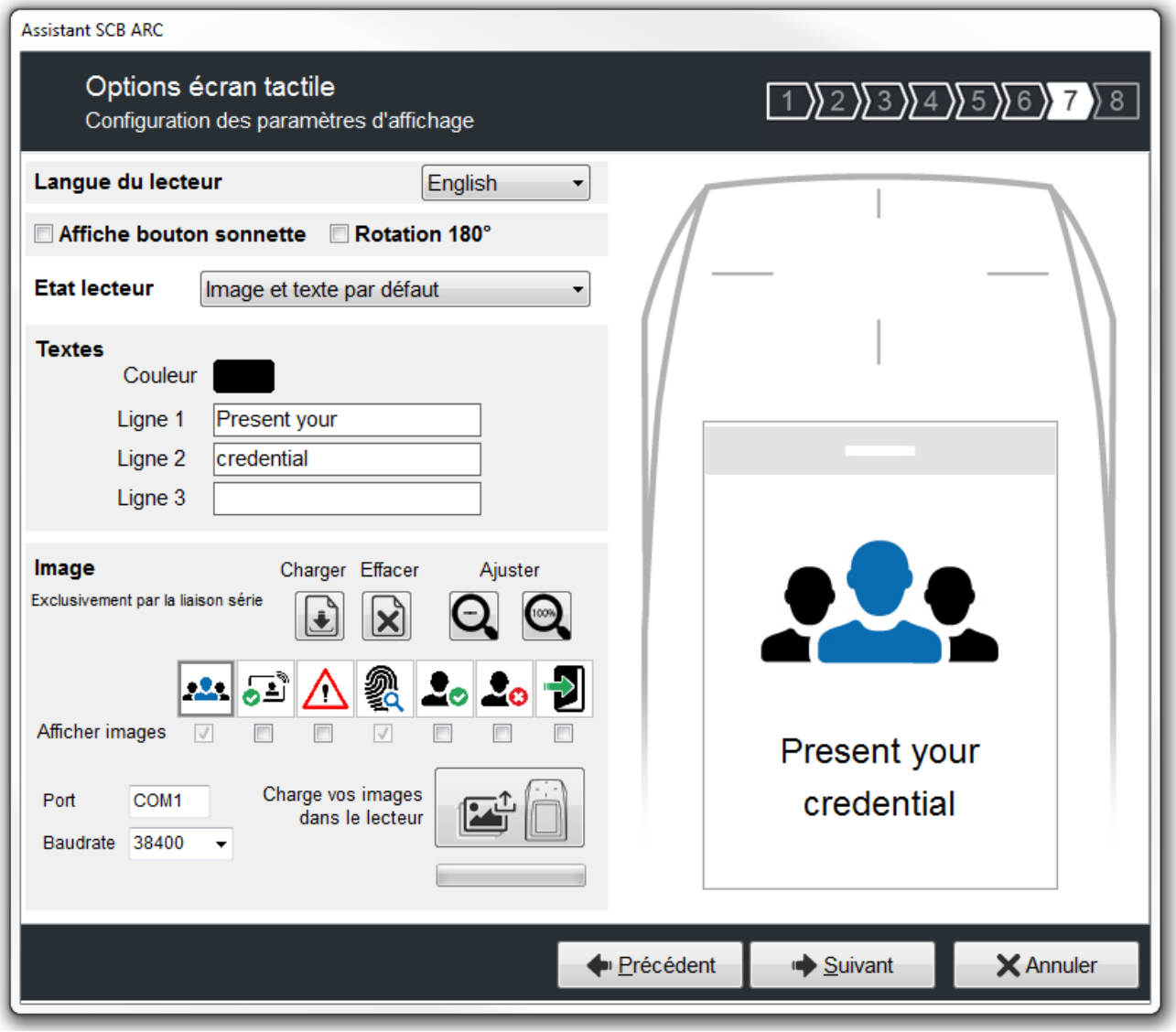
❖ Rétroéclairage : permet d'activer / désactiver le rétroéclairage du clavier.

ARC options

❖ Mode Eco (basse consommation)
Dans ce mode, l'éclairage est moins intense et les cycles de Scan sont réduis ce qui permet de réduire la consommation du lecteur d'environ 25%.

❖ Atténuation de la LED
Réduit drastiquement l'intensité des LED.

❖ Couper la configuration UHF
Permet de désactiver la puce UHF. Pour plus de détails sur la configuration par UHF, se reporter à *VII. 10 - UHF config.*



Affiche bouton sonnette : Permet d'activer / désactiver l'affichage du bouton sonnette sur l'écran. Lors d'un appui sur la sonnette celle-ci sera activée durant 1s.

	Apparence du bandeau
Clavier inactif et Sonnette inactive	
Clavier actif en mode Badge ET touche et Sonnette inactive	_ _ _ _ _
Clavier actif en mode Badge ET touche et sonnette active	_ _ _ _ _
Clavier inactif et Sonnette active	

Attention

Lorsque la sonnette est active et si le lecteur possède un écran alors l'arrachement ne sera plus effectif au niveau du relais statique (utilisé pour la sonnette)

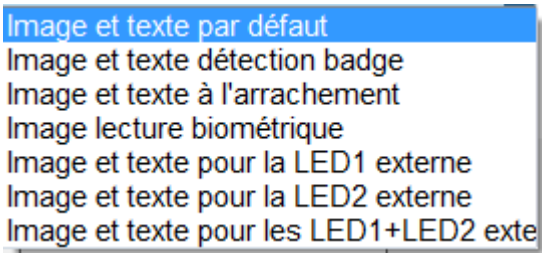
Rotation 180° : Permet de faire une rotation de l'image à 180°.

Langue du lecteur

Permet de choisir la langue utilisée pour afficher le texte sur l'écran : Anglais (par défaut) ou Français.

Etat lecteur

Permet de sélectionner l'état à modifier, soit à partir du menu déroulant, soit en cliquant sur l'icône correspondante.



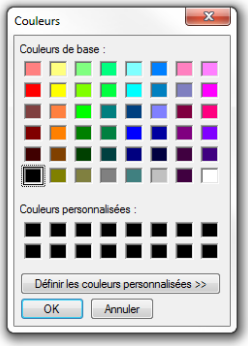
Les cases à cocher permettent de sélectionner les états qui seront activés par le SCB et valident l'image sur l'écran. Un double clic sur l'image de l'état permet de charger une image.

Pour chaque état, il est possible de modifier l'image, le texte et la couleur du texte.

Remarque : pour la biométrie, le texte n'est pas modifiable car il prend en compte le nombre de doigts défini dans l'assistant de configuration.

Textes

Pour changer la couleur du texte, cliquer sur le bouton de couleur.



La couleur s'applique aux trois lignes de textes.

Image

Permet de charger un fichier image dans la mémoire du lecteur.

Charger	Permet de charger un fichier image pour l'état sélectionné.
Effacer	Permet de supprimer le fichier image de l'état sélectionné.
Ajuster	Permet de diminuer l'image à l'écran.

Remarque : les formats classiques d'images sont supportés (bmp, png, jpeg …). Par contre, l'écran du lecteur ne gère pas de transparence, la couleur de fond est le blanc.

Chargement des images dans le lecteur :

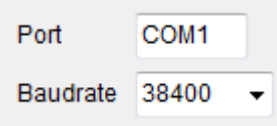
Après avoir chargé les images dans SECard pour les sept états différents, il faut les charger dans le lecteur.

Les cases à cocher permettent de sélectionner les états qui seront activés par le SCB. Les états « par défaut » et « biométrie » sont automatiquement activés.

Attention

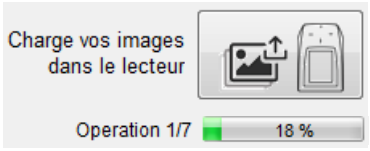
Le chargement des images dans le lecteur se fait par la liaison série du lecteur, pas par le SCB.

1 - Connecter le lecteur écran à votre poste de travail par la série du lecteur et paramétrer la communication :

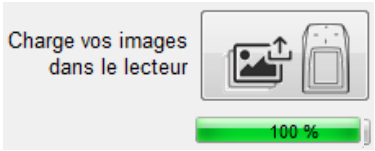


2 - Mettre le lecteur sous tension et cliquer sur le bouton  **n'importe quel moment pour un lecteur TTL et au démarrage du lecteur pendant que la LED orange clignote pour un lecteur série**.

3 - L'avancement du chargement est indiqué par la barre de progression : L'opération est répétée pour chaque image, soit sept fois.

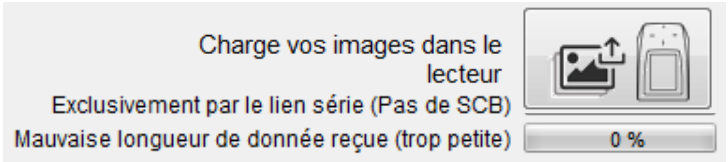


A la fin du chargement, le message suivant est affiché :



Remarque :

* Chaque image ayant un index, un nouveau chargement efface l'image précédemment chargée.
* Si vous obtenez le message ci-dessous, vos paramètres de communication ne sont pas corrects, revenir à l'étape 1.



* Si l'image qui a été chargée dans SECard a été déplacée, l'aperçu ne sera plus disponible et l'image suivante sera affichée dans l'IHM de SECard :

* **Le temps d'affichage de l'état « Image et texte détection badge » est défini à l'étape 5 « LED et Buzzer » avec « Nb clignotement » si le clignotement est activé ou « Durée LED ».**

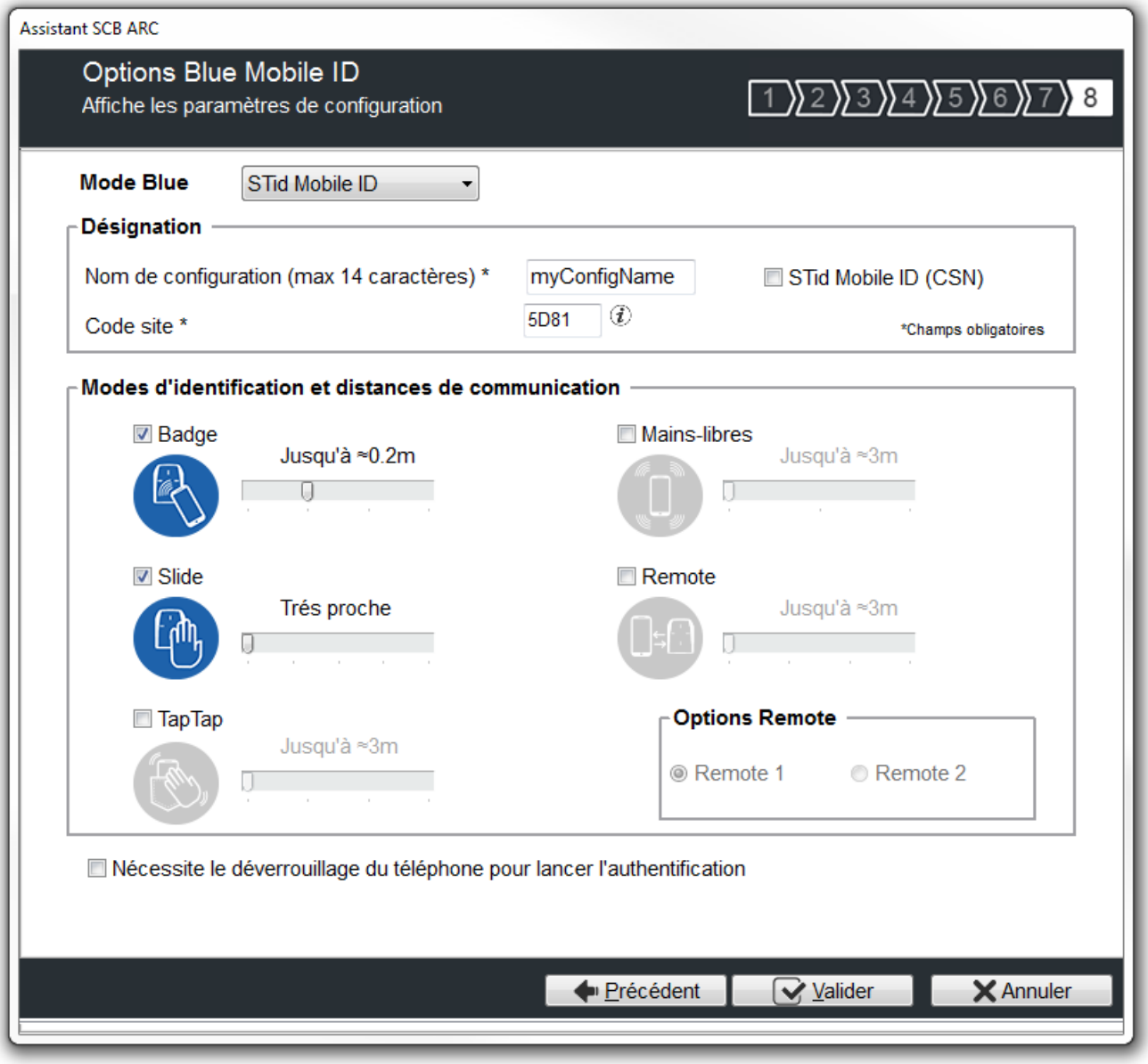
Image et texte par défaut

	Visuel
Image et texte par défaut	 Présentez votre badge
Image et texte détection badge*	 Badge détecté
Image et texte à l'arrachement	 Alerte Tentative d'arrachement
Image lecture biométrique (texte non modifiable)	 Présentez votre doigt sur le capteur
Image et texte pour la LED1 externe	 Accès autorisé
Image et texte pour la LED2 externe	 Accès refusé
Image et texte pour les LED1 &LED2 externes	 Accès libre

Note importante

Un badge de configuration créé avec une version de SECard < V2.1 (soit SCB < V8) pour un lecteur standard activera automatiquement l'écran s'il est présenté à un lecteur ARC écran, avec uniquement l'image « Image et texte par défaut » et les images liées à l'état LED1 et LED2.

De même, un badge de configuration créé avec une version de SECard < V2.1 (soit SCB < V8) pour un lecteur clavier standard activera automatiquement l'écran en mode clavier s'il est présenté à un lecteur ARC écran avec uniquement les images liées à l'état LED1 et LED2. L'image par défaut étant le clavier.

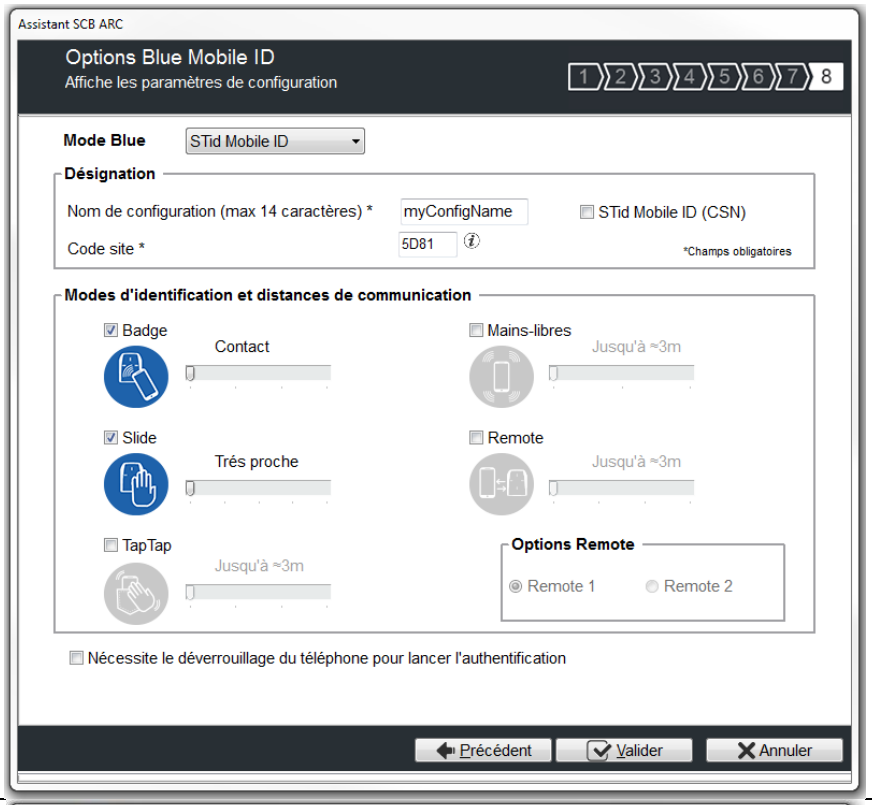
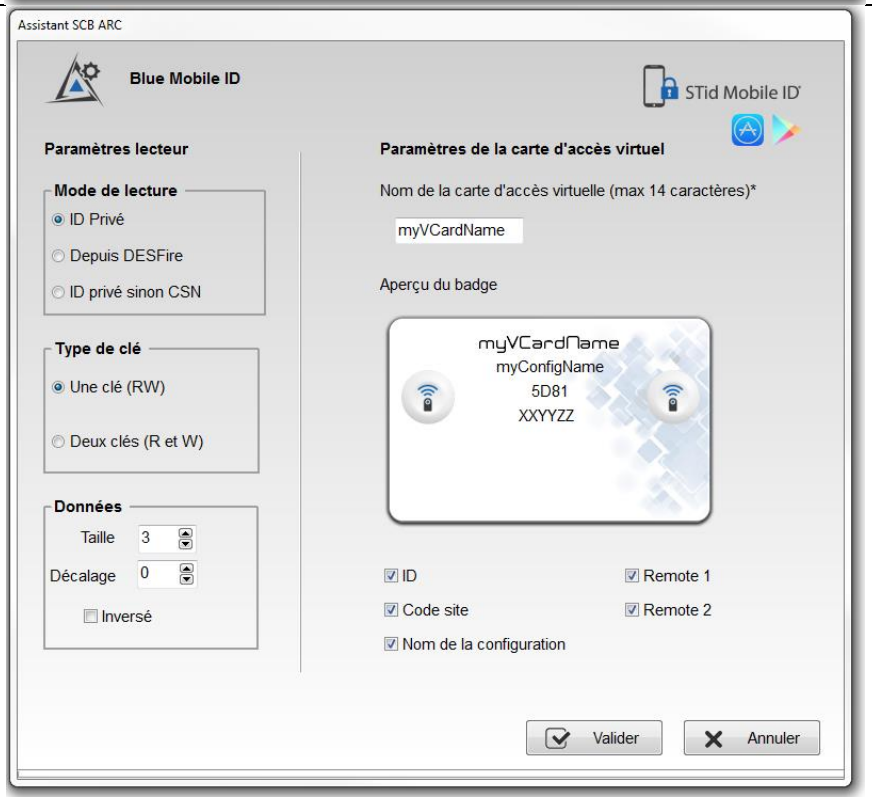


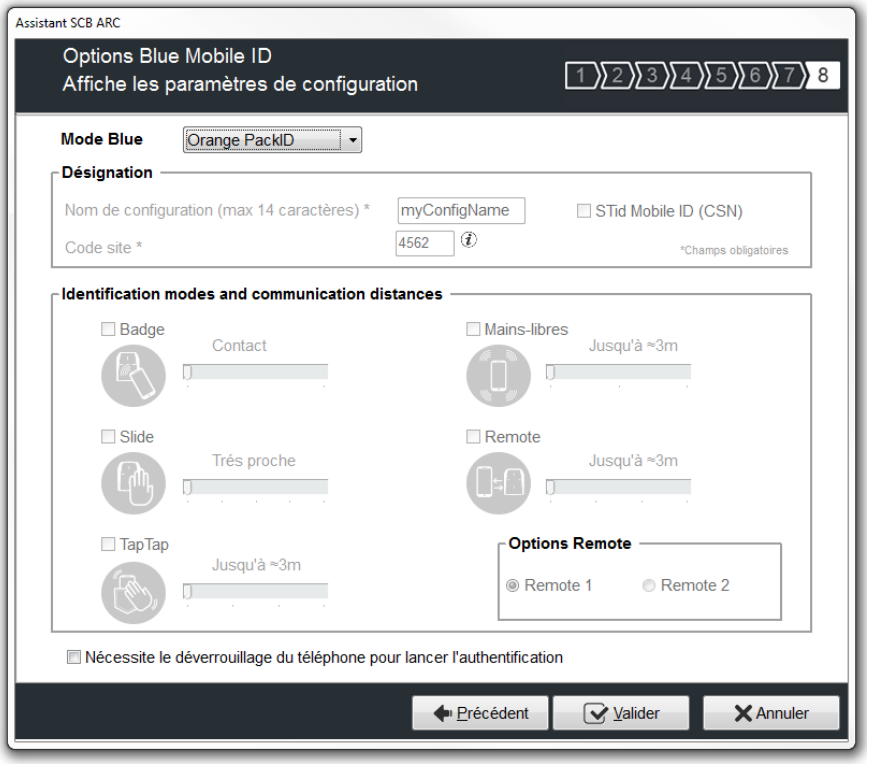
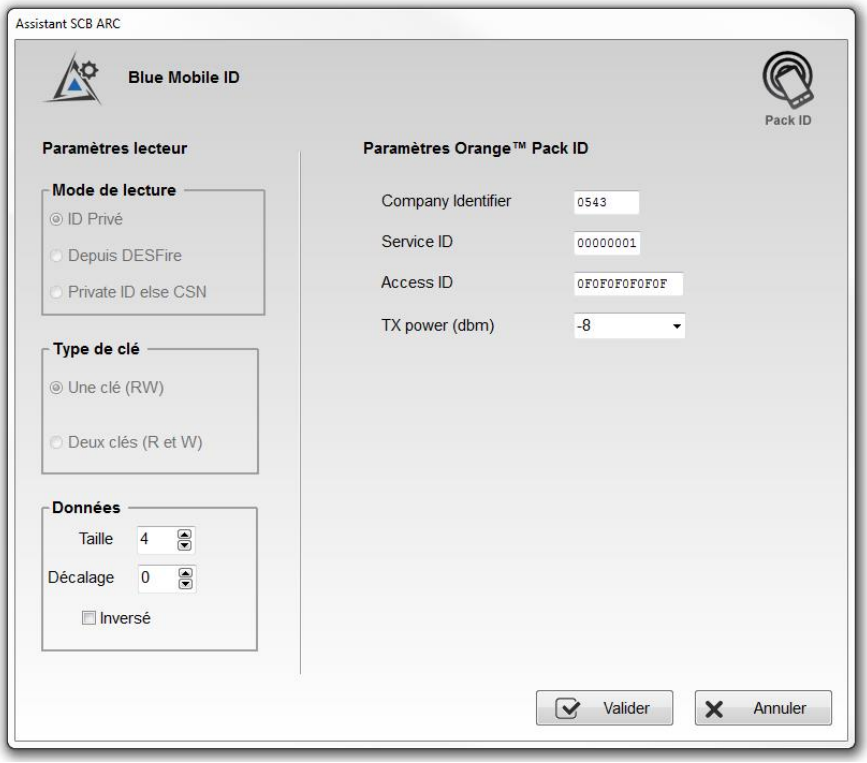
Quatre configurations sont disponibles pour l'authentification Bluetooth :

Nom de la Configuration / Caractéristiques	Conf Mobile ID	Conf Mobile ID	SameAsDESFire	Personnalisable
Nom du badge virtuel d'accès	STid Mobile ID	STid Mobile ID+	STid Secure ID	Personnalisable
Modes d'identification	Seulement Badge	Tous disponibles sauf Remote	Seulement Badge jusqu'à 0.5m	Tous disponibles
Verrouillage du Smartphone pour l'authentification	Choisi par le client	Choisi par le client	Non	Personnalisable
Code Site	51BC	51BC	CRC16 CCITT AID DESFire	Personnalisable

Mode Blue

Permet de configurer le lecteur Bluetooth® pour fonctionner avec l'application STid Mobile ID® ou Orange™ PAckID ou Open Mobile Protocol.
Ce choix a un impact sur les écrans de l'assistant de configuration Etape 8 et Blue Mobile ID Paramètres :

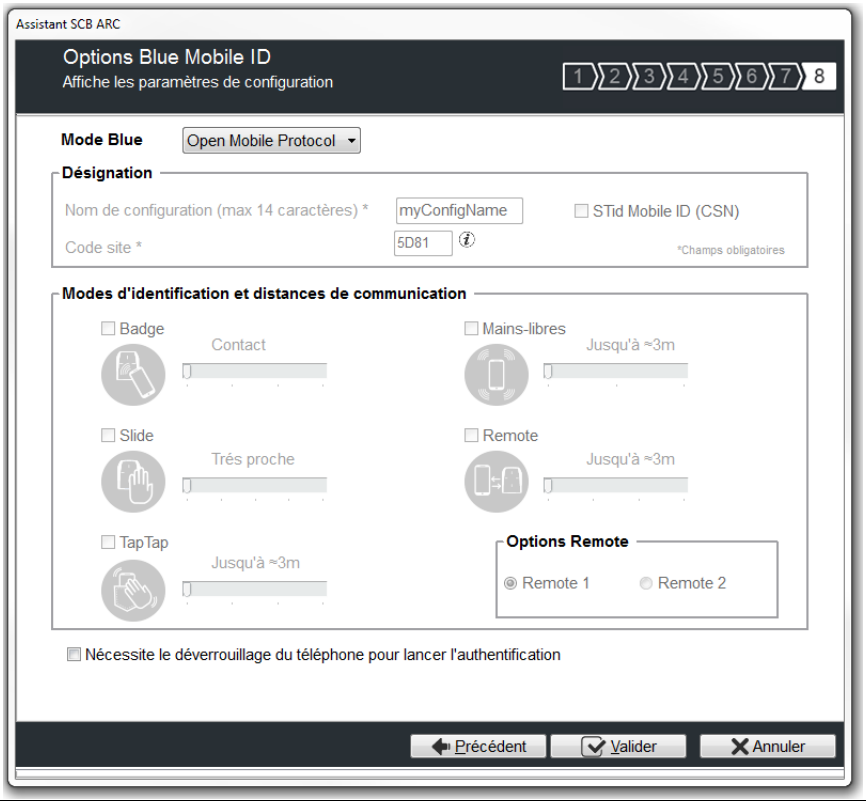
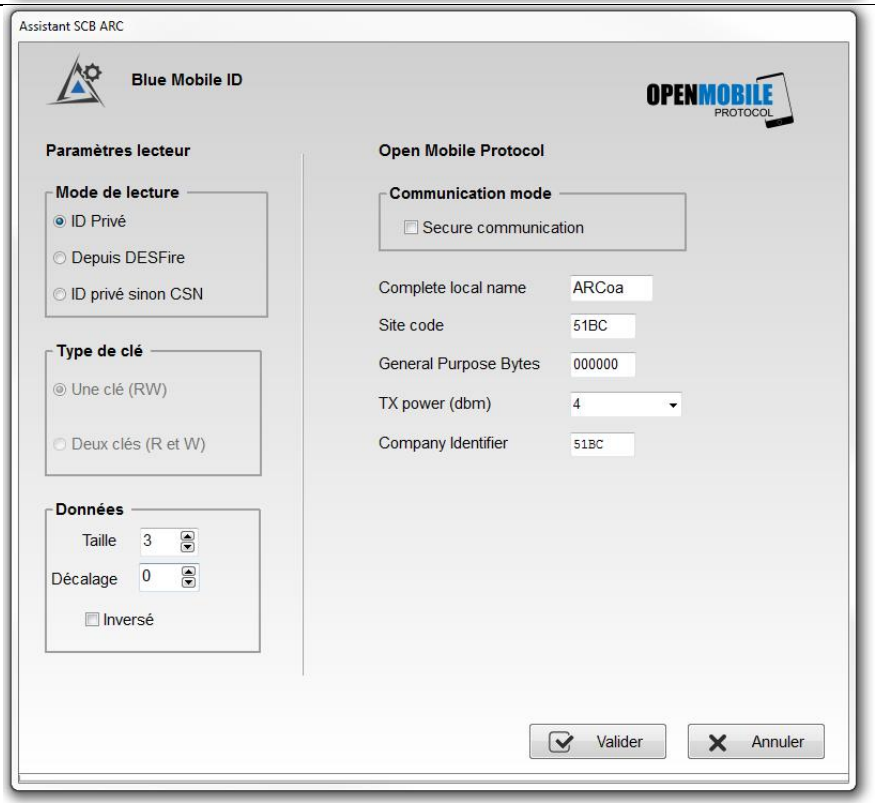
	STidMobile ID
Wizard Step 8	
Wizard Blue Mobile ID settings	

	Orange Pack ID
Wizard Step 8	
Wizard Blue Mobile ID settings	

Mode Blue Orange Pack ID

Le mode de détection pour cette application est fixé au contact.

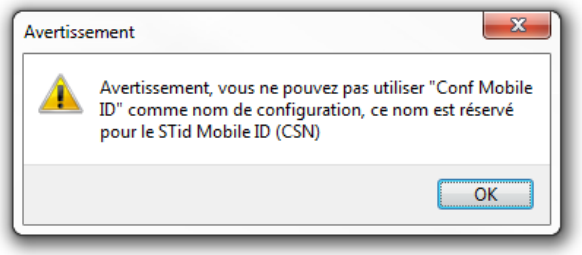
Attention : Pour configurer le lecteur pour cette application, vous devez créer un badge SCB physique et non pas un SCB virtuel.

	Open Mobile Protocol
Wizard Step 8	
Wizard Blue Mobile ID settings	

Mode STid Mobile ID

Désignation

- Nom de la configuration : entrer le nom pour la configuration Mobile ID.
  Le nom doit comporter un maximum de 14 caractères.
  Le nom de configuration « Conf Mobile ID » est réservé pour la configuration STid Mobile ID :



- Code site : nombre sur deux octets hexadécimaux désignant le code site de la configuration.
  Le code site 51BC est réservé pour la configuration STid Mobile ID.

- STid Mobile ID (CSN) : configure le lecteur pour lire le CSN uniquement.

Modes d'identification et distances de communication

Pour chaque mode d'identification, la distance de communication est réglable**.**

- **Badge :**

Fonctionne en présentant le smartphone devant le lecteur (comme un badge)

- Contact : le smartphone doit être en contact avec le lecteur
- Jusqu'à 0.2m : le smartphone doit être dans une zone de 0.2m autour du lecteur
- Jusqu'à 0.3m : le smartphone doit être dans une zone de 0.3m autour du 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

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

- **TapTap :**

Fonctionne en tapotant deux fois le téléphone dans la poche.

- Jusqu'à 3m
- Jusqu'à 5m
- Jusqu'à 10m
- Jusqu'à 15m

- **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

❖ **Remote options**

Si le mode d'identification « Remote » a été activé, permet d'associer la configuration en cours au bouton Remote 1 ou Remote 2.

Nécessite le déverrouillage du téléphone pour lancer l'authentification : option de sécurité

- Si cochée : le smartphone doit être déverrouillé pour s'authentifier avec le 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.

Remarque :

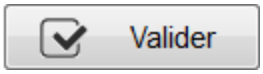
La notion de distance en Bluetooth correspond à une zone autour du lecteur, pas seulement en façade.

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.

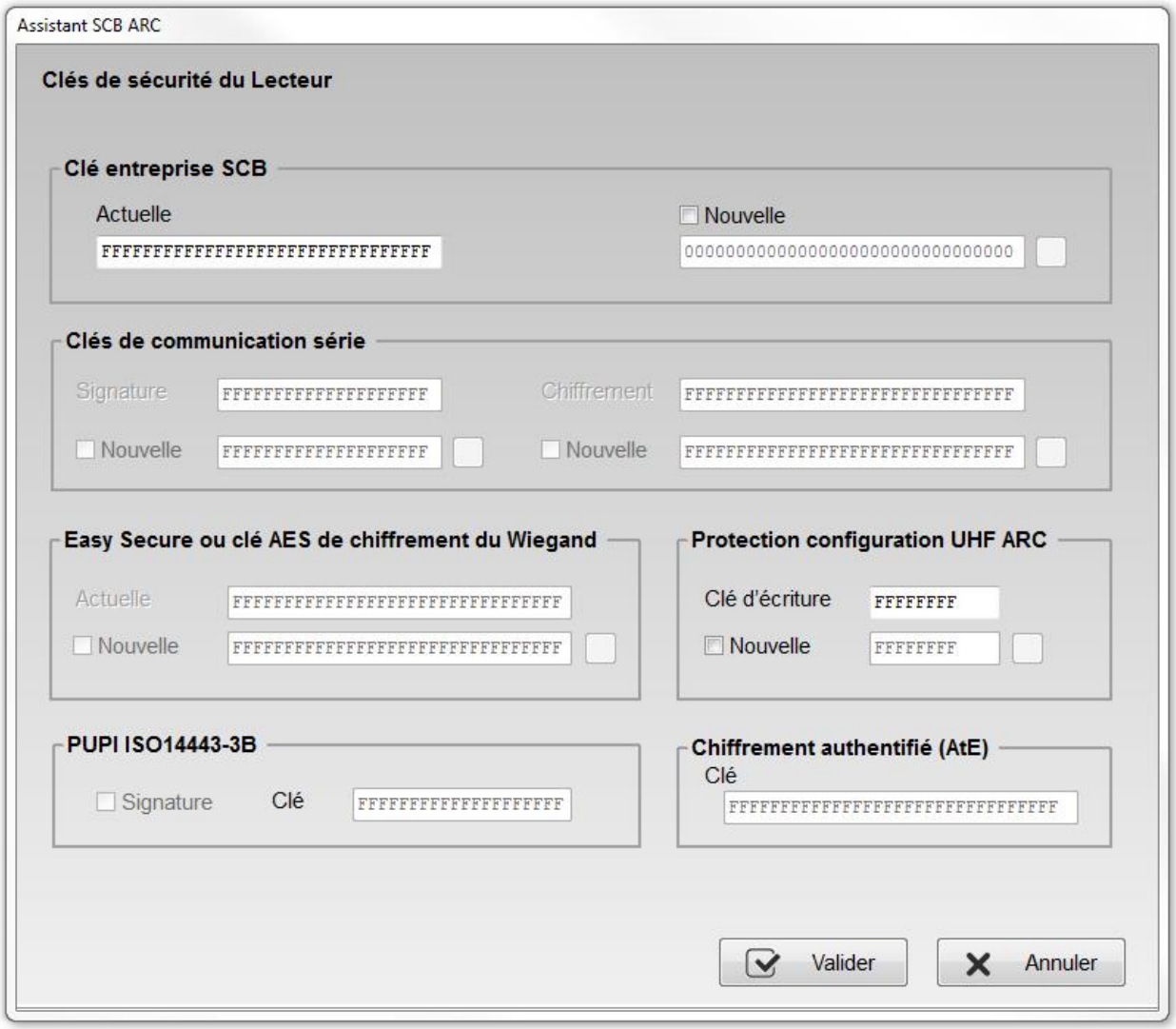
Attention

Lorsque des lecteurs Architect® Blue sont installés les uns à côté des autres, les distances de détection doivent être définies pour tenir compte de la distance entre les lecteurs.

Cliquer sur le bouton 

pour terminer la configuration des paramètres lecteurs.

III. 2 - Assistant SCB ARC : clés de communication



Clé entreprise SCB

Les lecteurs configurables par les badges « *SCB* » sont livrés initialement avec une configuration par défaut (clé usine 0XFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF).
Ceux-ci pourront donc être configurés par un SCB de clé courante 0xFF…FF vers une nouvelle clé entreprise.
Elle peut être saisie manuellement ou automatiquement en appuyant CTRL+R ou en effectuant un clic droit « *Remplir avec une valeur aléatoire* ».

Après la première configuration et afin de pouvoir reconfigurer le lecteur, il sera nécessaire de présenter au lecteur des badges « *SCB* » possédant une clé entreprise identique à celle enregistrée par le lecteur.

Attention

Cette clé est importante et doit absolument être connue de l'administrateur. Elle protège les données du « *SCB* » et permet des modifications sur la configuration des lecteurs.

En cas de perte de cette clé, le lecteur ne pourra plus être reconfiguré par un autre « *SCB* » et devra obligatoirement être réinitialisé en usine.

Clés de communication série

Permet de modifier la clé de signature et la clé de chiffrement utilisateur pour les lecteurs séries chiffrés (S32 / S35 / S33).
Pour plus de détail sur la communication série sécurisée se reporter au paragraphe *T5.2 - Mode de communication bidirectionnel.*

Easy Secure ou clés AES de chiffrement du Wiegand

Permet de modifier la clé de chiffrement utilisée pour sécuriser la liaison des lecteurs S31 et R33+INTR33E.

Note :
La valeur de la clé de chiffrement AES par défaut (sortie usine) est égale à :
«*FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF*».

Il est obligatoire de modifier cette clé afin que la sortie soit chiffrée.

PUPI ISO 14443-3B

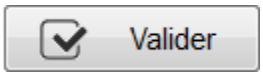
Permet de renseigner la clé utilisée pour le calcul de la signature dite « clé secrète » sur 10 octets.

Protection configuration UHF ARC

Permet de modifier la clé d'écriture de la configuration UHF si elle est activée (cf. **Erreur ! Source du renvoi introuvable.**Il est recommandé de la modifier afin de protéger la configuration en écriture dans la puce.

Chiffrement authentifié (AtE) :

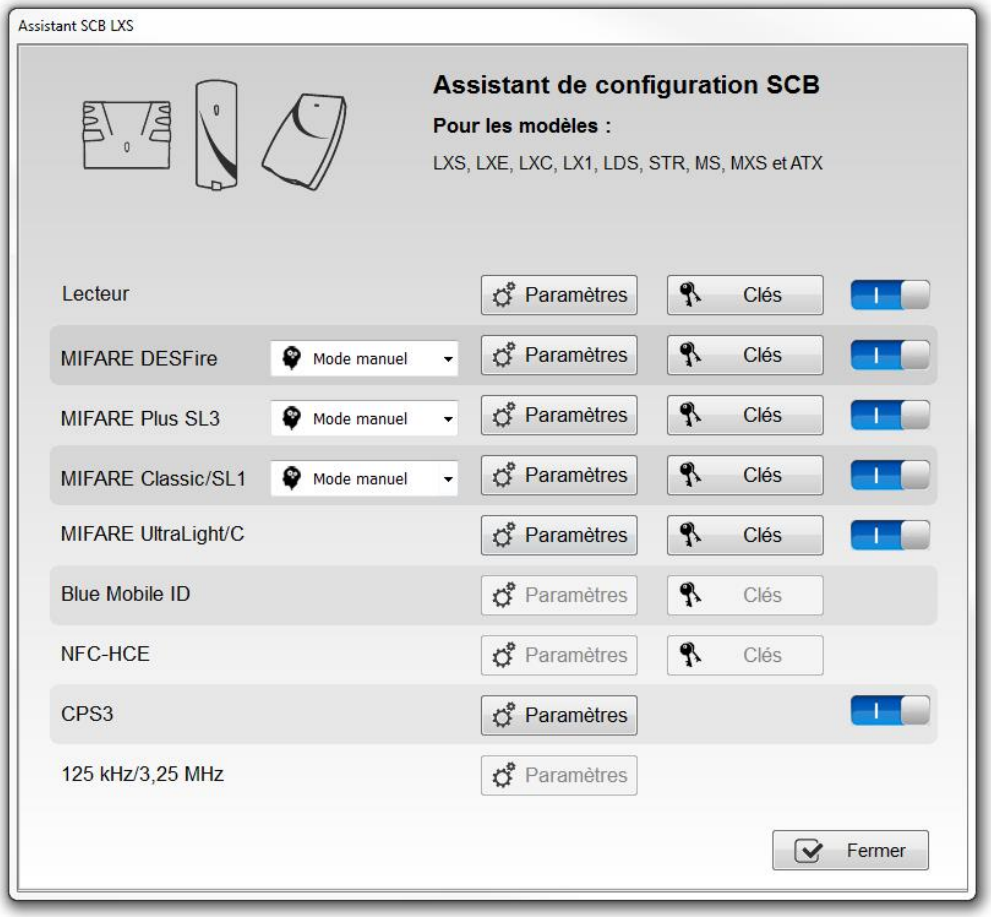
Permet de renseigner la clé pour le chiffrement authentifié.

Cliquer sur le bouton 

pour terminer la configuration des clés.

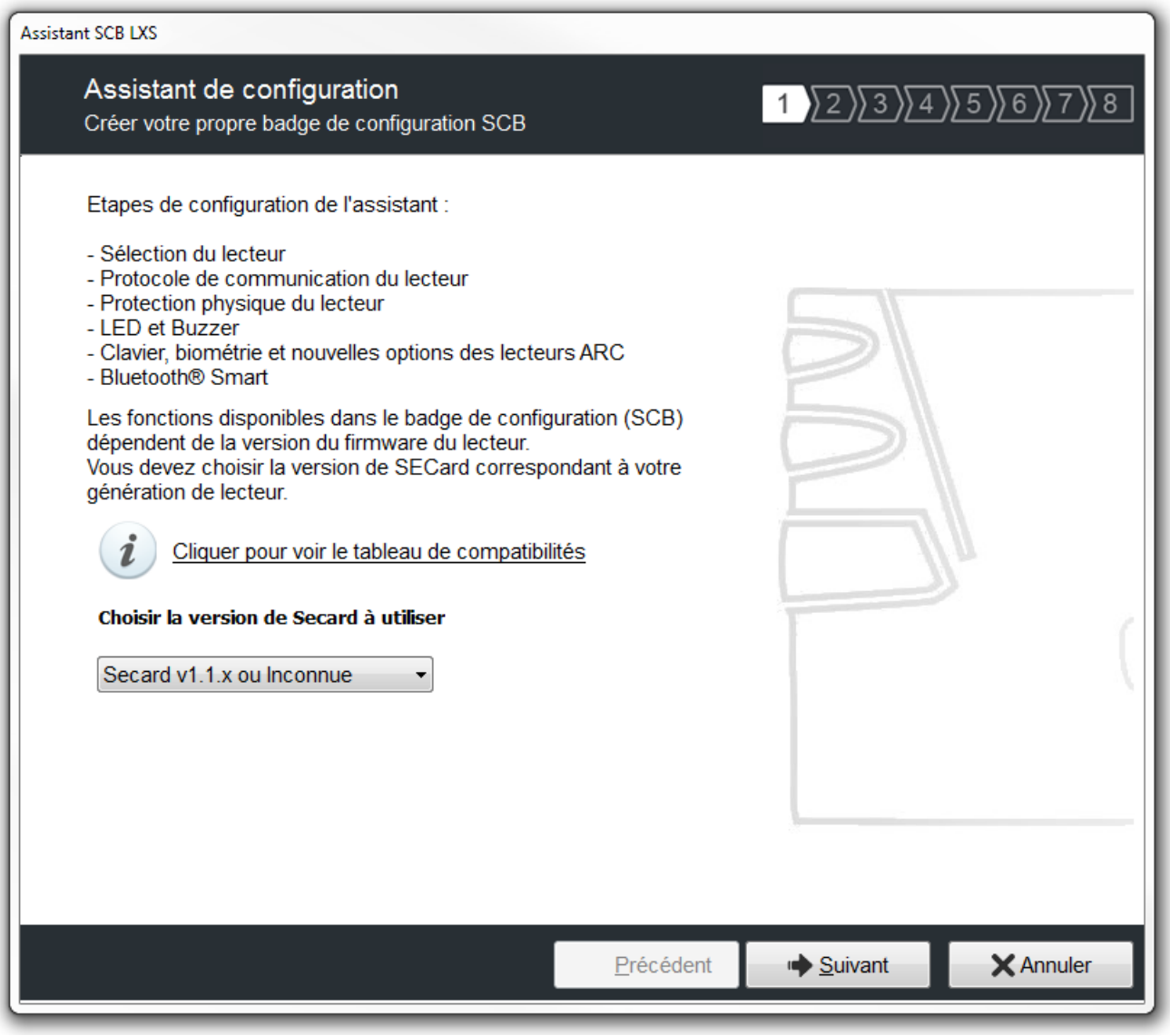
III. 3 - Assistant SCB LXS : paramètres lecteurs

Aucun Ajout de fonctionnalités lié à SECard V3.2.



Lecteur « Paramètres » : la configuration du lecteur se fait en six étapes, pour passer d'une étape à l'autre il faut cliquer sur « Suivant ».

1 2 3 4 5 6 7 8 Cliquez-ici	Assistant de configuration / Choix de la version de SECard
1 2 3 4 5 6 7 8 Cliquez-ici	Sélection du lecteur
1 2 3 4 5 6 7 8 Cliquez-ici	Protocole de communication du lecteur
1 2 3 4 5 6 7 8 Cliquez-ici	Protections physiques du lecteur
1 2 3 4 5 6 7 8 Cliquez-ici	LED et Buzzer
1 2 3 4 5 6 7 8 Cliquez-ici	Clavier, biométrie et options des lecteurs
1 2 3 4 5 6 7 8	Non utilisé pour les lecteurs standards
1 2 3 4 5 6 7 8	Non utilisé pour les lecteurs standards



Les fonctionnalités disponibles et la compatibilité des badges SCB dépendent de la génération de firmware des lecteurs.

Pour assurer la compatibilité entre les différentes versions de SCB et de firmware, SECard V3.x.x donne le choix à l'utilisateur de la version de SECard à utiliser si l'option a été validée dans l'onglet « *Fichiers* ». *cf. II. 3 - Fichiers.*

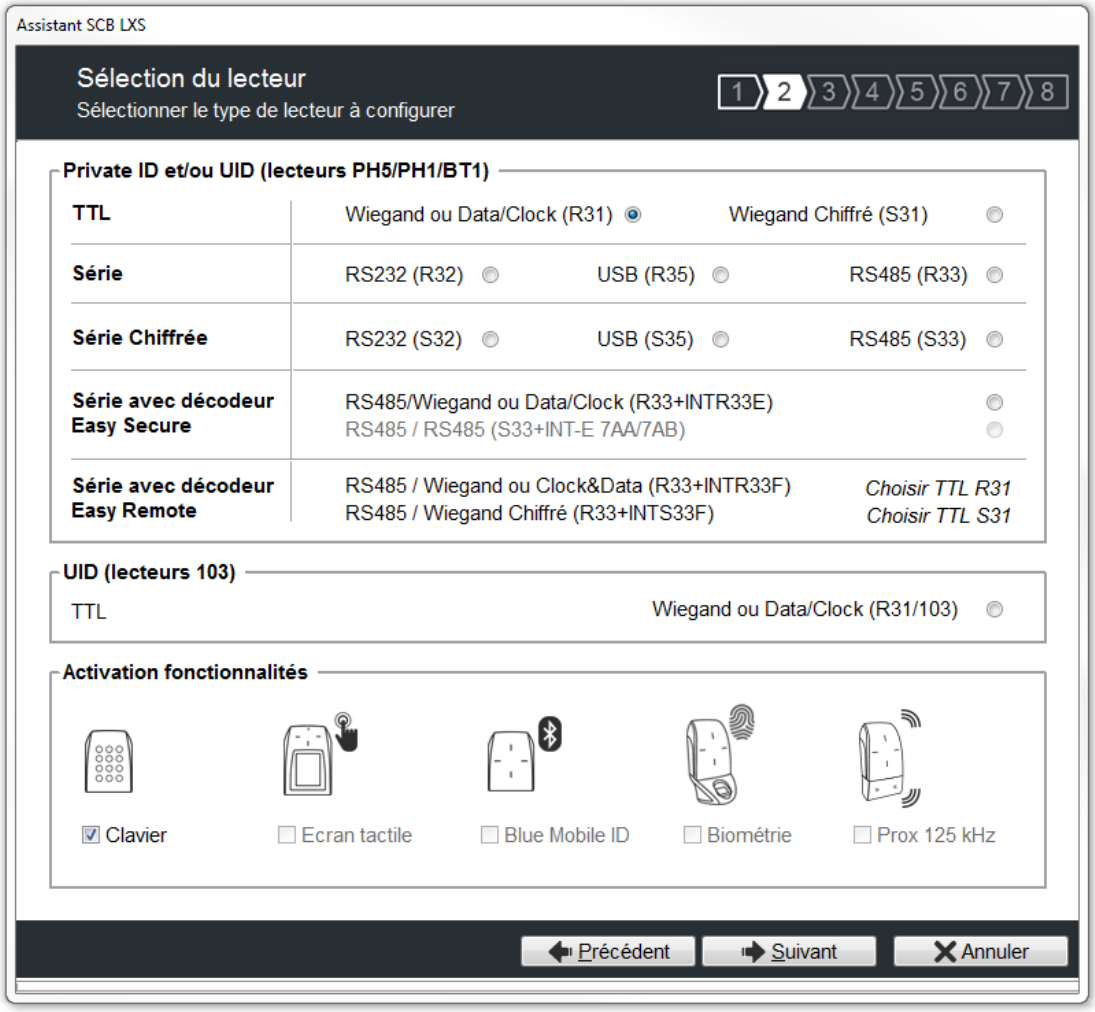
Compatibilités entre les versions de Secard et les firmwares

SECard

Standard Firmwares	v1.1.x	v1.2.x	v1.3.x	v1.4.0	v1.4.1	v1.4B.x
U7	x					
U8-U10	x¹	x				
U11-U12	x¹	x¹	x			
U13-U18	x¹	x¹	x¹	x	x	
>=U20	x¹	x¹	x¹	x¹	x¹	x

x Entièrement compatible
x¹ Fonctions limitées pour assurer la rétro-compatibilité

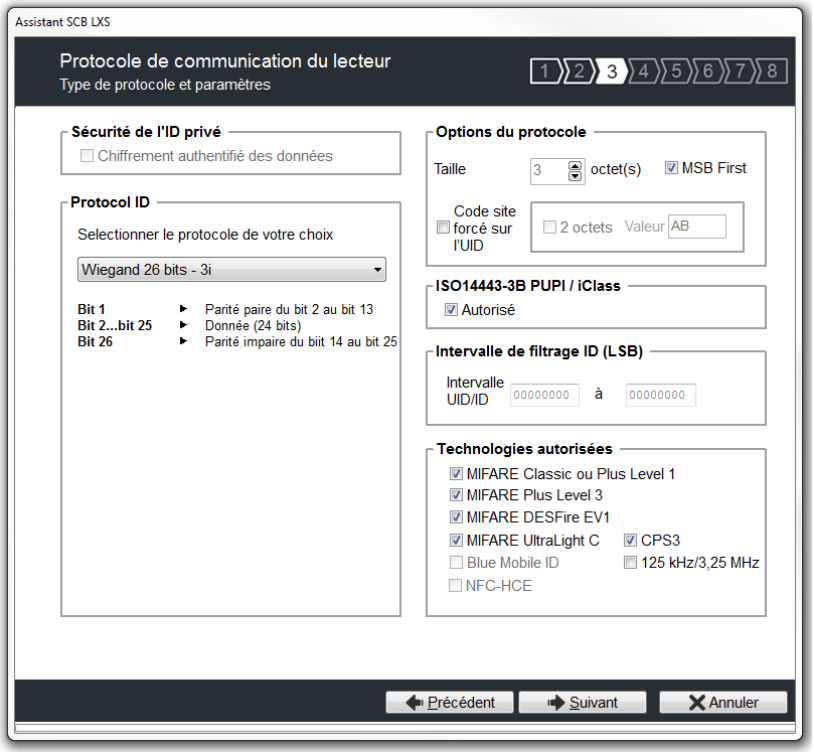
Pour connaître la version du firmware, se reporter au paragraphe *T2.1 - Mise sous tension*.



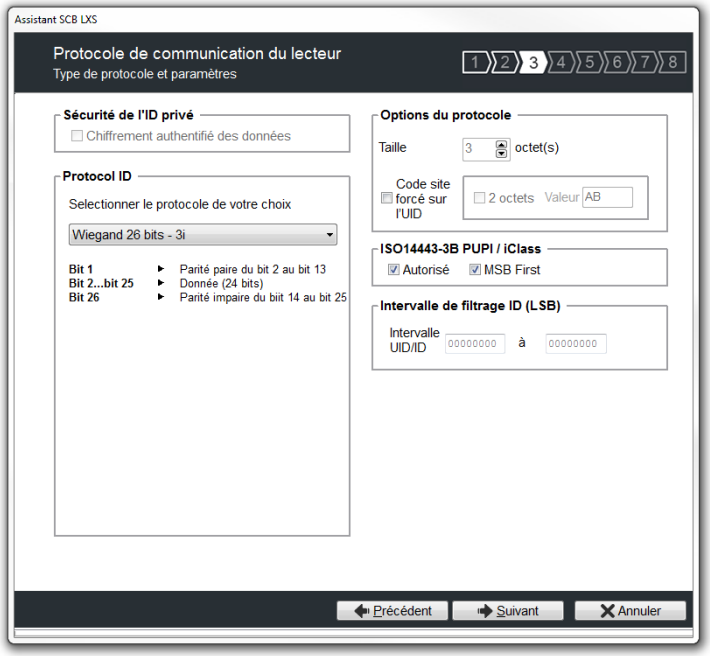
Cette étape permet :

- De choisir le type de lecteur à configurer.
- D'activer la configuration biométrique, disponible uniquement sur TTL Wiegand ou Data/Clock (R31), TTL Wiegand chiffré (S31) et Série avec décodeur (R33+INTR33E).
- D'activer la configuration clavier.
- Les configurations écran tactile et Blue Mobile ID ne sont pas disponible sur les lecteurs de la gamme standard.

Cette fenêtre apparait lorsque le type de lecteur sélectionné à l'étape 2 est R31/103 :



Cette fenêtre apparait lorsque le type de lecteur sélectionné à l'étape 2 est en sortie TTL :



Protocole

Il contient les différents protocoles de communication TTL supportés par le lecteur.

Pour plus d'information sur les protocoles se reporter au paragraphe *T4 - Au sujet des protocoles de communication TTL*.

Note : Lors de l'encodage d'un identifiant, celui-ci est réalisé au format du protocole en cours (exemple : Décimal 13 caractères pour le protocole 2B – 10 caractères en hexadécimal pour le protocole 3Cb).

Options du protocole

- « *Taille* » permet d'ajuster la taille des protocoles personnalisables.

  Taille maximum en Wiegand : 48 octets
  Taille maximum en Data/Clock : 10 octets

- « *Code site forcé sur l'UID* » permet de forcer un code site quel que soit le protocole de communication. La valeur du code sera transmise en poids fort sur un ou deux octet(s). L'UID peut donc être tronqué selon le protocole utilisé. Cette option n'est pas disponible pour le Wiegand 64 bits - 3T.

ISO 14443-3B PUPI / iClass

Il est possible de gérer différemment les PUPI ISO14443-3B et 14443-2B exclusivement en calculant un code d'authentification de message utilisant une fonction de hachage cryptographique (SHA1) en combinaison avec une clé secrète. Les autres types de modulation (ISO14443-A) et fréquences (125 kHz /3.25 MHz) ne sont pas affectés par cette option.

Si la taille du protocole est inférieure à 20 octets, un troncage LSB sera effectué sur les 20 octets de signature obtenus.
Si la taille du protocole est supérieure à 20 octets, un padding à zéro sera effectué.

Intervalle de filtrage ID (LSB)

Il est possible de restituer un UID/ID uniquement si celui-ci est compris dans une plage spécifique bornée sur 4 octets.

Si la taille de l'UID/ID est supérieure à 4 octets, l'intervalle s'effectuera sur les 4 octets LSB (prise en compte de l'option MSB First au préalable). Les bornes sont incluses, limite basse ≤ UID/ID ≤ limite haute.

Si l'UID/ID est compris dans l'intervalle, le lecteur restituera le code suivant le protocole en cours et effectuera une action badge LED + Buzzer (SCB). Dans le cas contraire, le lecteur allumera la LED rouge + Buzzer durant 400ms (non paramétrable et non désactivable).

L'UID/ID comparé est la valeur hexadécimale après prise en compte du paramètre MSB First et avant mise en forme protocolaire.
Par exemple pour un protocole 2S, le code comparé sera le code sur 4oct avant codage au format 2S

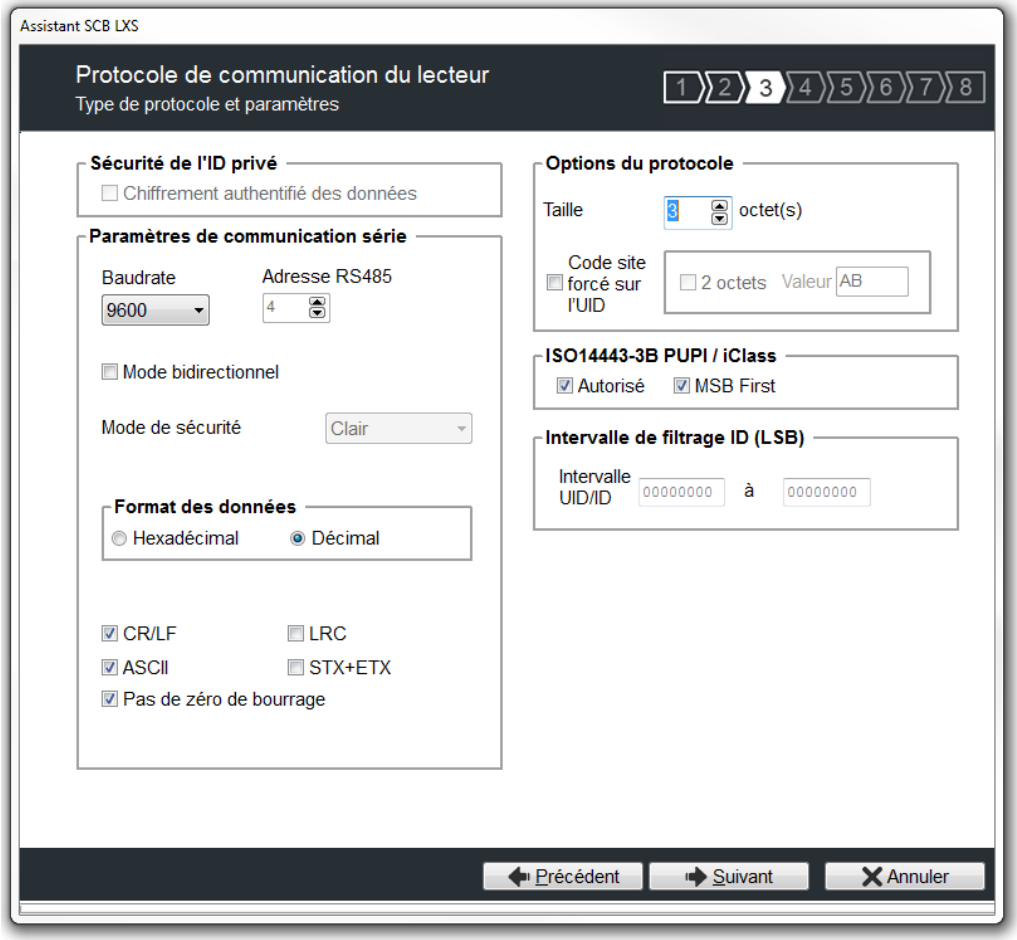
Technologies autorisées

Lorsque le lecteur sélectionné est de type UID (103 uniquement) cette liste permet de sélectionner le type de technologies de puce pouvant être lues par le lecteur.

Sécurité de l'ID privé

Paramètre non disponible pour les lecteurs standards, uniquement disponible pour les lecteurs WAL et ARC.

Cette fenêtre apparait lorsque le type de lecteur sélectionné à l'étape 2 est en sorite série :



Paramètres de communication série

Il contient les différents paramètres de la communication série.

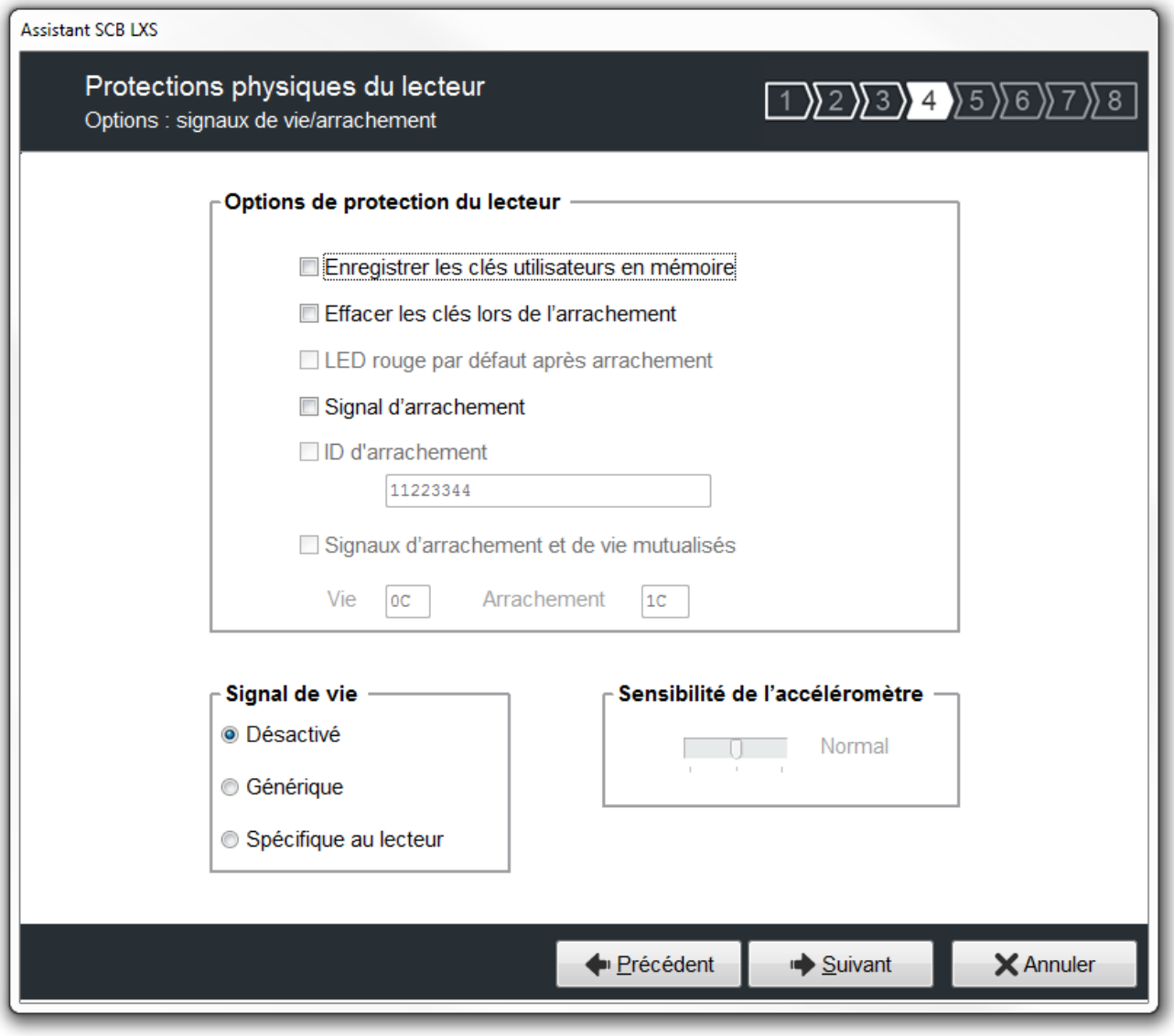
Pour plus d'information sur les protocoles se reporter au paragraphe *T5 - Au sujet des protocoles de communication Série*.

Options du protocole

« *Taille* » permet d'ajuster la taille des données.

Taille maximum en Hexadécimal : 48 octets
Taille maximum en Décimal : 10 octets

Note :
Il est possible d'augmenter la taille du champ au-delà des tailles maximums. Pour cela, maintenir la touche CTRL enfoncée et cliquer dans le champ « *Taille données* », la valeur apparait alors soulignée. Cette manipulation ne fonctionne pas pour un encodage mais uniquement pour la relecture d'un identifiant. Uniquement disponible sur les lecteurs séries.



Options de protection du lecteur

- Enregistrer les clés utilisateurs en mémoire : permet de sauvegarder les clés, de façon chiffrée, en cas de coupure d'alimentation. Les clés sont enregistrées en EEPROM mémoire non volatile.
- Effacer les clés lors de l'arrachement : permet d'effacer toutes les clés du lecteur si un changement d'état intervient sur l'entrée « Switch ».
- LED rouge par défaut après arrachement : *paramètre non disponible pour les lecteurs standards, uniquement accessible depuis le Wizard des lecteurs WAL et ARC*.
- Signal d'arrachement : permet d'activer le signal d'arrachement. Se reporter au paragraphe *T11 - Signal d'arrachement.*
- ID signal d'arrachement : *paramètre non disponible pour les lecteurs standards, uniquement accessible depuis le Wizard des lecteurs ARC*.
- Signaux d'arrachement et de vie mutualisés : permet d'activer l'envoi dans une trame, d'un signal d'arrachement et de vie, disponible uniquement pour les lecteurs *R31*, *S31 et R33+INTR33E*. Se reporter au paragraphe *T13 - Signal de vie / arrachement mutualisés.*

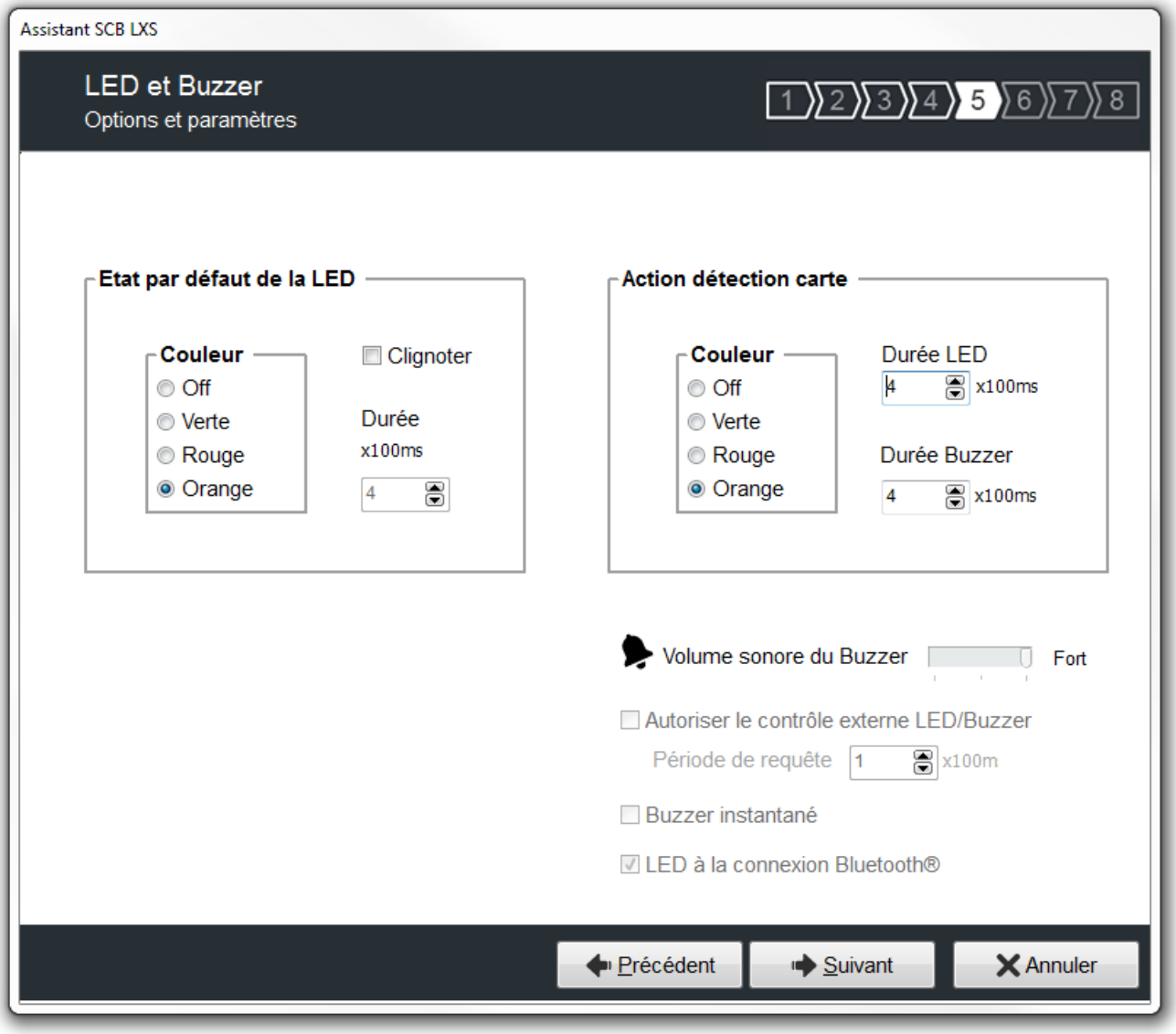
Note : il n'y a pas de gestion de l'arrachement sur les lecteurs USB.

Signal de vie

Permet d'activer/ désactiver le signal et de choisir le type de signal « Générique » ou « Spécifique ».
Se reporter au paragraphe *T10 - Signal* de vie.

Sensibilité de l'accéléromètre

Paramètre non disponible pour les lecteurs standards, uniquement accessible depuis le Wizard des lecteurs WAL et ARC.



Etat par défaut de la LED

Permet de définir l'état (couleur & clignotement) de la LED en fonctionnement normal.

Action détection carte

Permet de définir l'état (couleur & clignotement) de la LED et du buzzer lors de la détection d'un identifiant. Cette information est indépendante de l'acceptation de l'identifiant.

Buzzer instantané

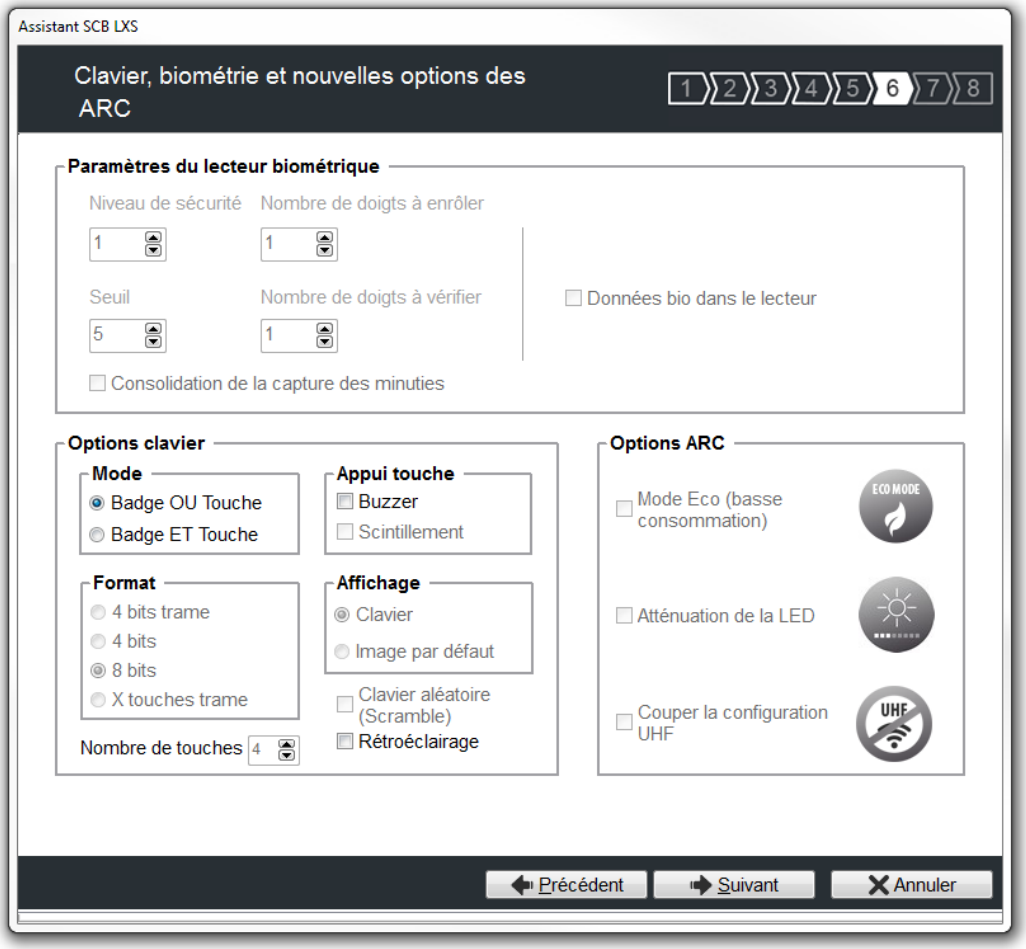
Permet au lecteur d'activer le buzzer à chaque détection d'identifiant sans attendre de commande du système. Disponible uniquement pour les lecteurs séries (R/S-32 et R/S-33) en mode bidirectionnel.

Autoriser le contrôle externe LED / Buzzer

Permet de contrôler la LED et le buzzer de façon externe. La période d'interrogation est réglable par pallier de 100ms. Disponible uniquement pour les lecteurs séries (R/S-32 et R/S-33) en mode bidirectionnel.

Volume sonore du Buzzer & LED à la connexion Bluetooth®

Paramètre non disponible pour les lecteurs standards, uniquement accessible depuis le Wizard des lecteurs ARCS.



Paramètres du lecteur biométrique

- Niveau de sécurité : représente le taux de fiabilité entre l'empreinte encodée dans la puce et celle lue par le capteur biométrique du lecteur.
  - Niveau de sécurité = 1 : niveau faible de sécurité de faux doigts (recommandé par Sagem Morpho),
  - Niveau de sécurité = 2 : niveau moyen de sécurité de faux doigts,
  - Niveau de sécurité = 3 : niveau élevé de sécurité de faux doigts.

- Seuil : représente la qualité de l'empreinte à encoder dans la puce de 0 à 10.
  Un seuil bas entraine moins de rejet. Recommandation Morpho Sagem : 5.

- Nombre de doigts à enrôler : représente le nombre de doigts à encoder dans la puce, généralement les deux index.

- Nombre de doigts à vérifier : représente le nombre de doigts à vérifier sur le lecteur pour autoriser l'accès, généralement un doigt.

- Consolidation de la capture des minuties : permet de faire trois captures par doigt lors de l'encodage, le capteur biométrique retiendra la meilleure des trois empreintes.

Note : un ré encodage avec un nombre de doigts supérieur nécessite un formatage de la puce DESFire®.

- Donnée bio dans le lecteur : *paramètre non disponible pour les lecteurs standards, uniquement accessible depuis le Wizard des lecteurs ARC*.

Options clavier

Permet de choisir entre les deux modes « Badge OU Touche » et « Badge ET Touche »

- Badge OU Touche + choix du format :
  En cas de présentation d'un badge, son identifiant est immédiatement transmis suivant le protocole en cours, suivi d'un acquittement sonore.
  En cas de frappe d'une touche, et suivant les modes de format définis dans l'encadré *Format*, sa valeur est immédiatement transmise suivant le protocole en cours, suivi d'un acquittement sonore.

- Badge ET Touche + nombre de touches :
  Lorsque la séquence de touches est complète, le lecteur attend un identifiant pendant un délai de 6 secondes (émission d'un bip sonore pour indiquer l'attente de l'identifiant).

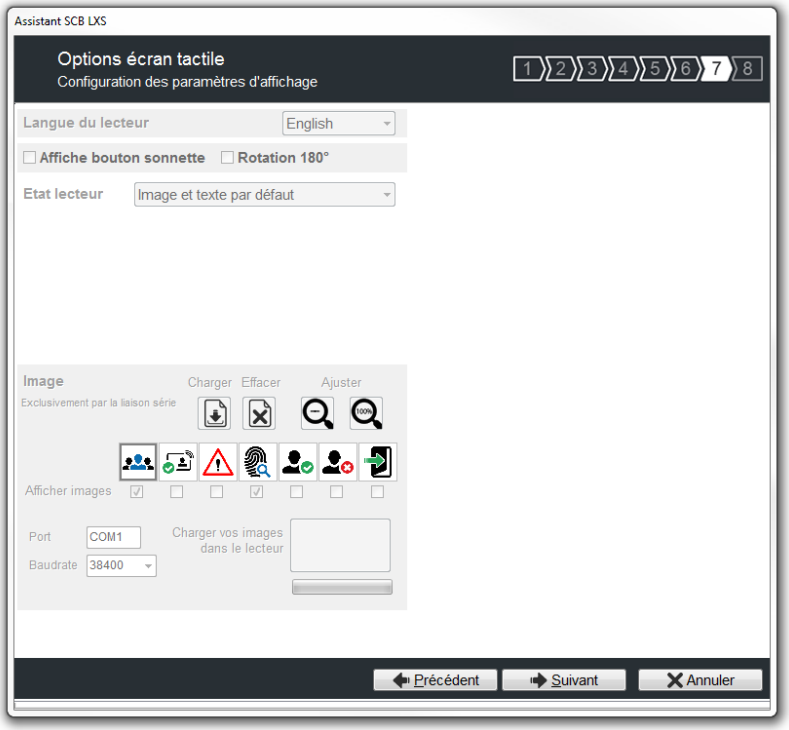
- Appui touche, Clavier aléatoire (Scramble) et Rétroéclairage : *paramètres non disponibles pour les lecteurs standards, uniquement accessible depuis le Wizard des lecteurs ARC.*

Pour plus de détails sur le fonctionnement et le format se reporter au paragraphe *T6 - Au sujet des lecteurs Clavier*

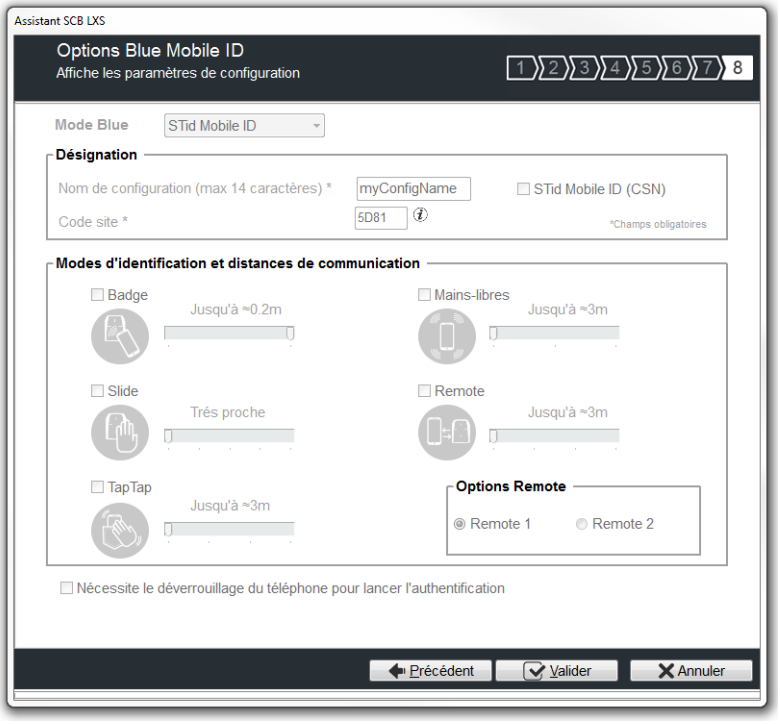
Attention

En mode Badge ET Touche le format Wiegand 26 bits n'est pas disponible.

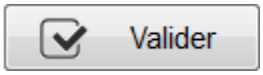
Options ARC : *non disponible pour les lecteurs standards*.



Configuration écran tactile non disponible pour les lecteurs standards, uniquement accessible depuis le Wizard des lecteurs ARC.

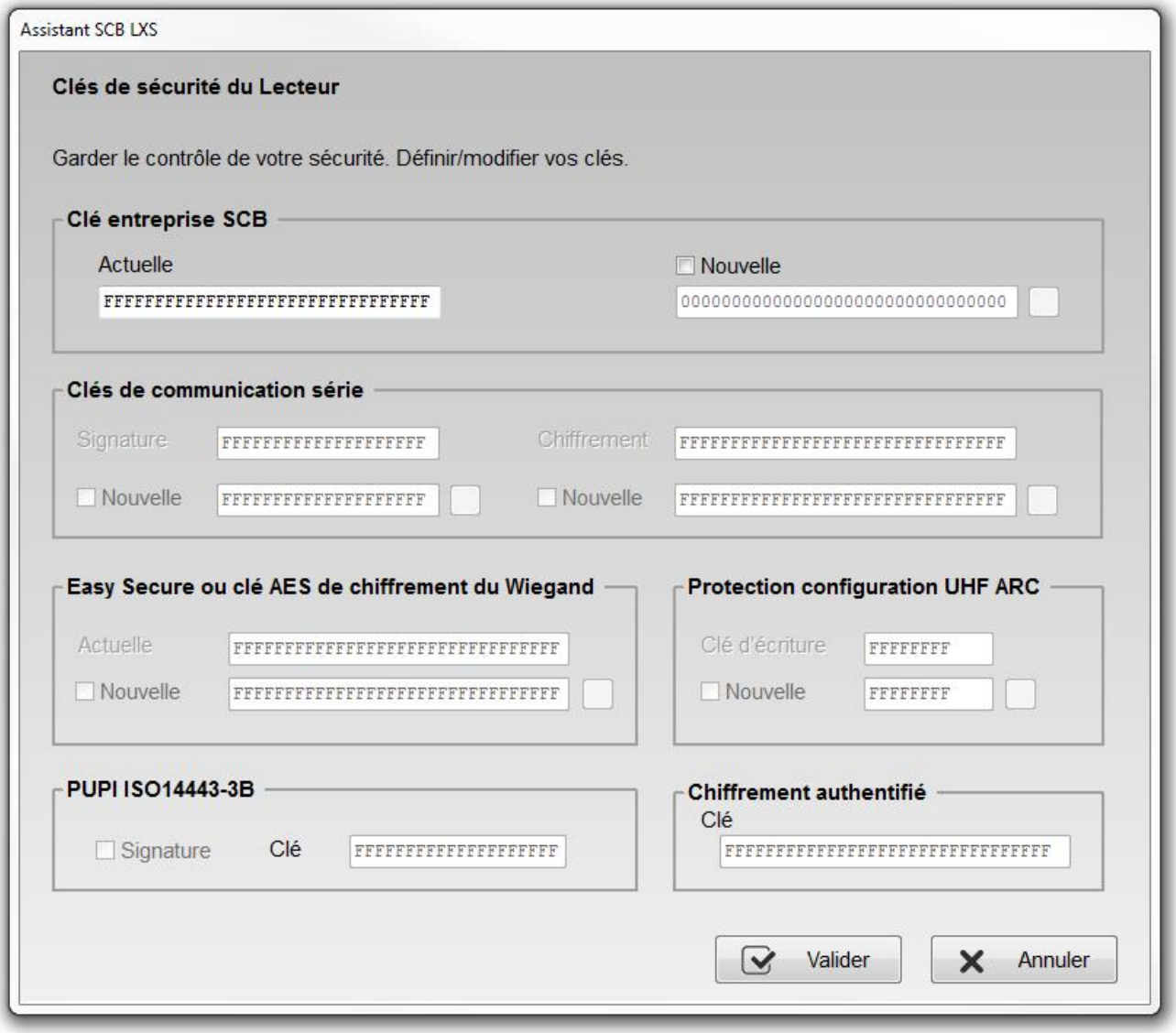


Configuration Blue Mobile ID non disponible pour les lecteurs standards, uniquement accessible depuis le Wizard des lecteurs ARC.

Cliquer sur le bouton 

pour terminer la configuration des paramètres lecteurs.

III. 4 - Assistant SCB LXS : clés de sécurité du lecteur



Clé entreprise SCB

Les lecteurs configurables par les badges « *SCB* » sont livrés initialement avec une configuration par défaut (clé usine 0XFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF).
Ceux-ci pourront donc être configurés par un SCB de clé courante 0xFF…FF vers une nouvelle clé entreprise.
Elle peut être saisie manuellement ou automatiquement en appuyant CTRL+R ou en effectuant un clic droit « *Remplir avec une valeur aléatoire* ».

Après la première configuration et afin de pouvoir reconfigurer le lecteur, il sera nécessaire de présenter au lecteur des badges « *SCB* » possédant une clé entreprise identique à celle enregistrée par le lecteur.

Attention

Cette clé est importante et doit absolument être connue de l'administrateur. Elle protège les données du « *SCB* » et permet des modifications sur la configuration des lecteurs.

En cas de perte de cette clé, le lecteur ne pourra plus être reconfiguré par un autre « *SCB* » et devra obligatoirement être réinitialisé en usine.

Note : la clé entreprise représente également lors de la création d'un badge utilisateur MIFARE Plus® les valeurs de la clé Maître Badge, de la clé configuration badge et de la clé de changement de niveau 3.

Clés de communication série

Permet de modifier la clé de signature et la clé de chiffrement utilisateur pour les lecteurs série chiffrés (S32 / S35 / S33).
Pour plus de détail sur la communication série sécurisée, se reporter au paragraphe *T5.2 - Mode de communication bidirectionnel.*

Easy Secure ou clé AES de chiffrement du Wiegand

Permet de modifier la clé de chiffrement utilisée pour sécuriser la liaison du lecteur S31 ou la communication entre le lecteur et l'interface du lecteur R33+INTR33E.

Note :
La valeur de la clé de chiffrement AES par défaut (sortie usine) est égale à :
«*FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF*».
Il est obligatoire de changer la valeur de cette clé afin que la sortie soit chiffrée.

PUPI ISO 14443-3B

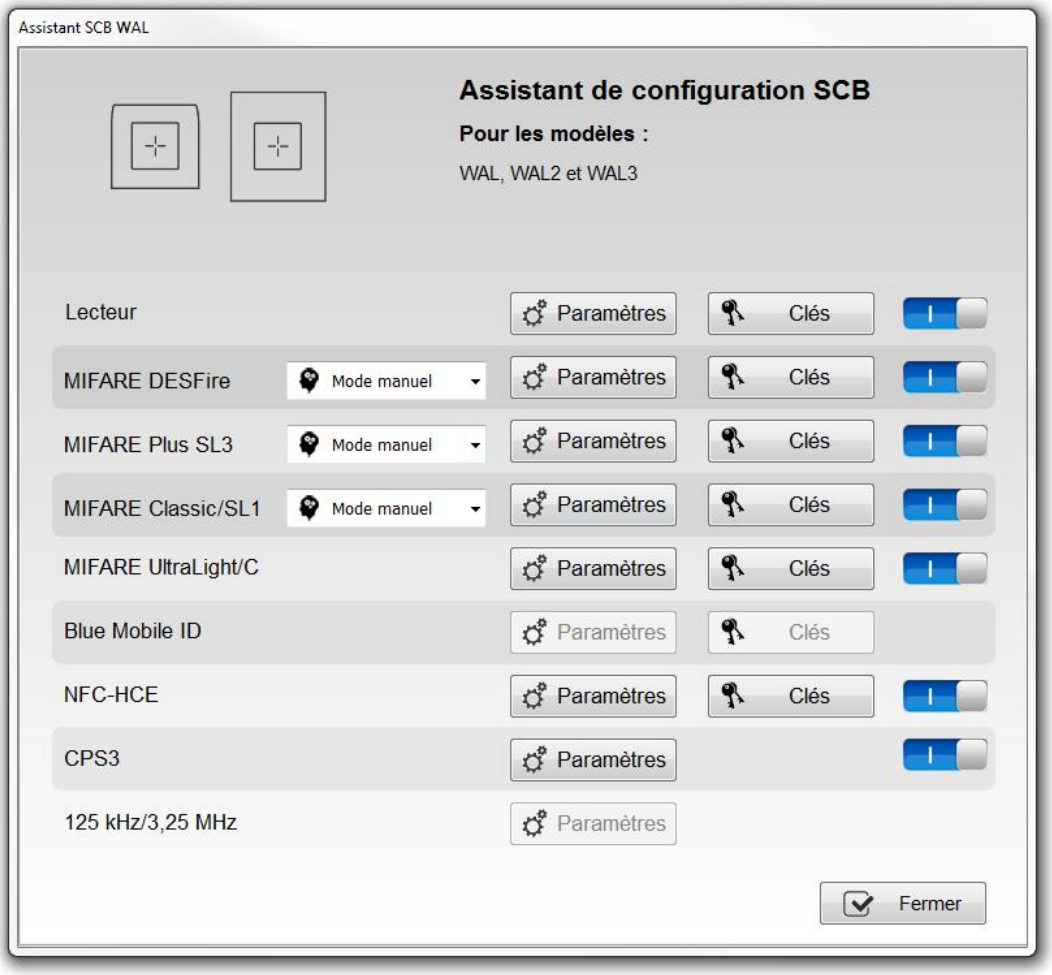
Permet de renseigner la clé utilisée pour le calcul de la signature dite « clé secrète » sur 10 octets.

Protection configuration UHF ARC : *non disponible pour les lecteurs standards*.

Chiffrement authentifié : *non disponible pour les lecteurs standards*.

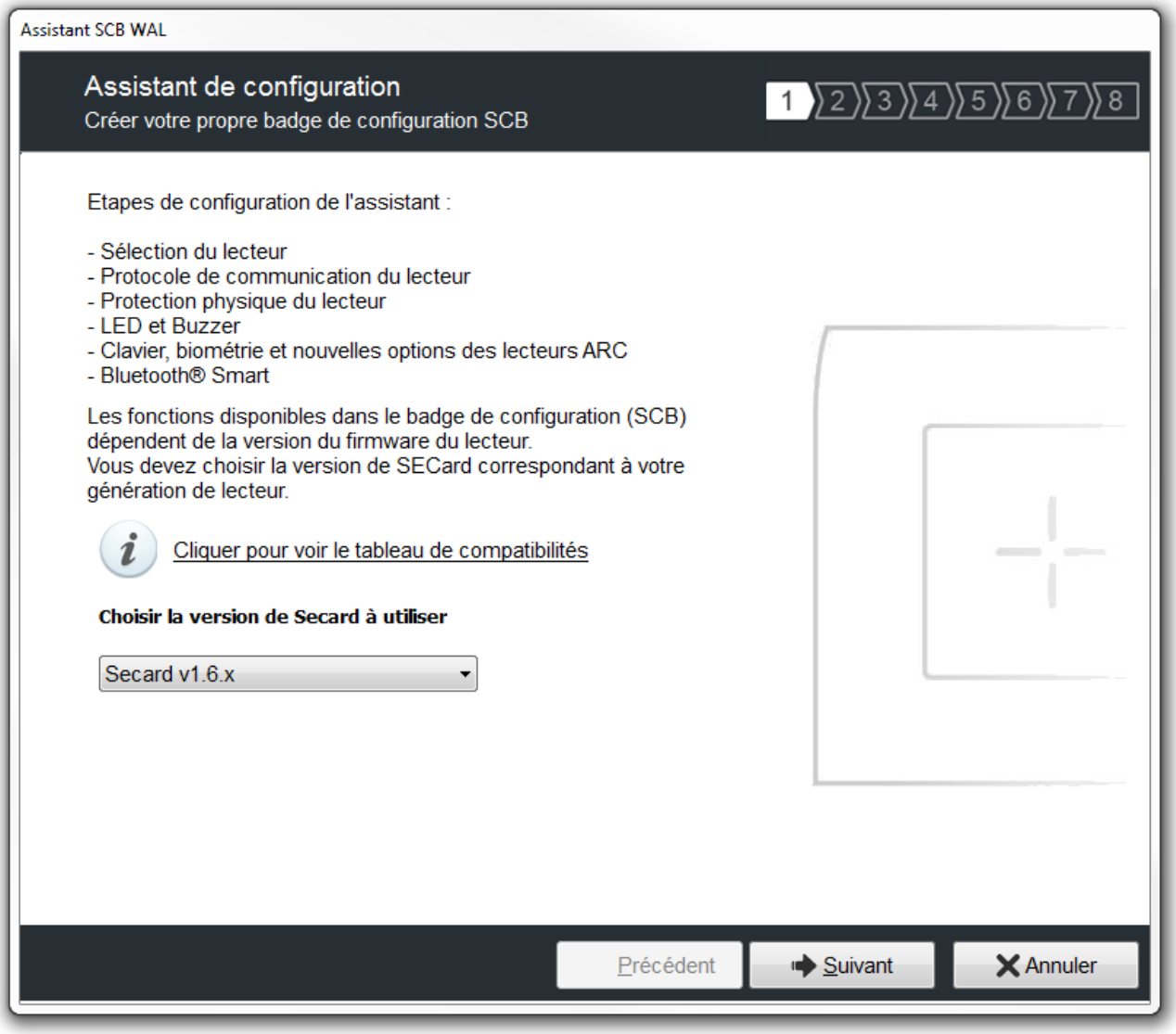
III. 5 - Assistant SCB WAL : paramètres lecteurs

Aucun Ajout de fonctionnalités lié à SECard V3.2.



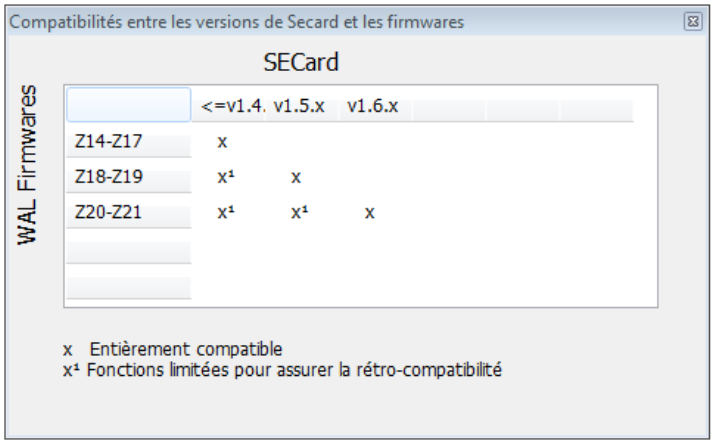
Lecteur « Paramètres » : la configuration du lecteur se fait en cinq étapes, pour passer d'une étape à l'autre il faut cliquer sur « Suivant ».

1 2 3 4 5 6 7 8 Cliquez-ici	Assistant de configuration / Choix de la version de SECard
1 2 3 4 5 6 7 8 Cliquez-ici	Sélection du lecteur
1 2 3 4 5 6 7 8 Cliquez-ici	Protocole de communication du lecteur
1 2 3 4 5 6 7 8 Cliquez-ici	Protections physiques du lecteur
1 2 3 4 5 6 7 8 Cliquez-ici	LED et Buzzer
1 2 3 4 5 6 7 8	Clavier, biométrie et options des lecteurs Non utilisé pour Lecteur WAL
1 2 3 4 5 6 7 8	Ecran tactile Non utilisé pour Lecteur WAL
1 2 3 4 5 6 7 8	Non utilisé pour Lecteur WAL

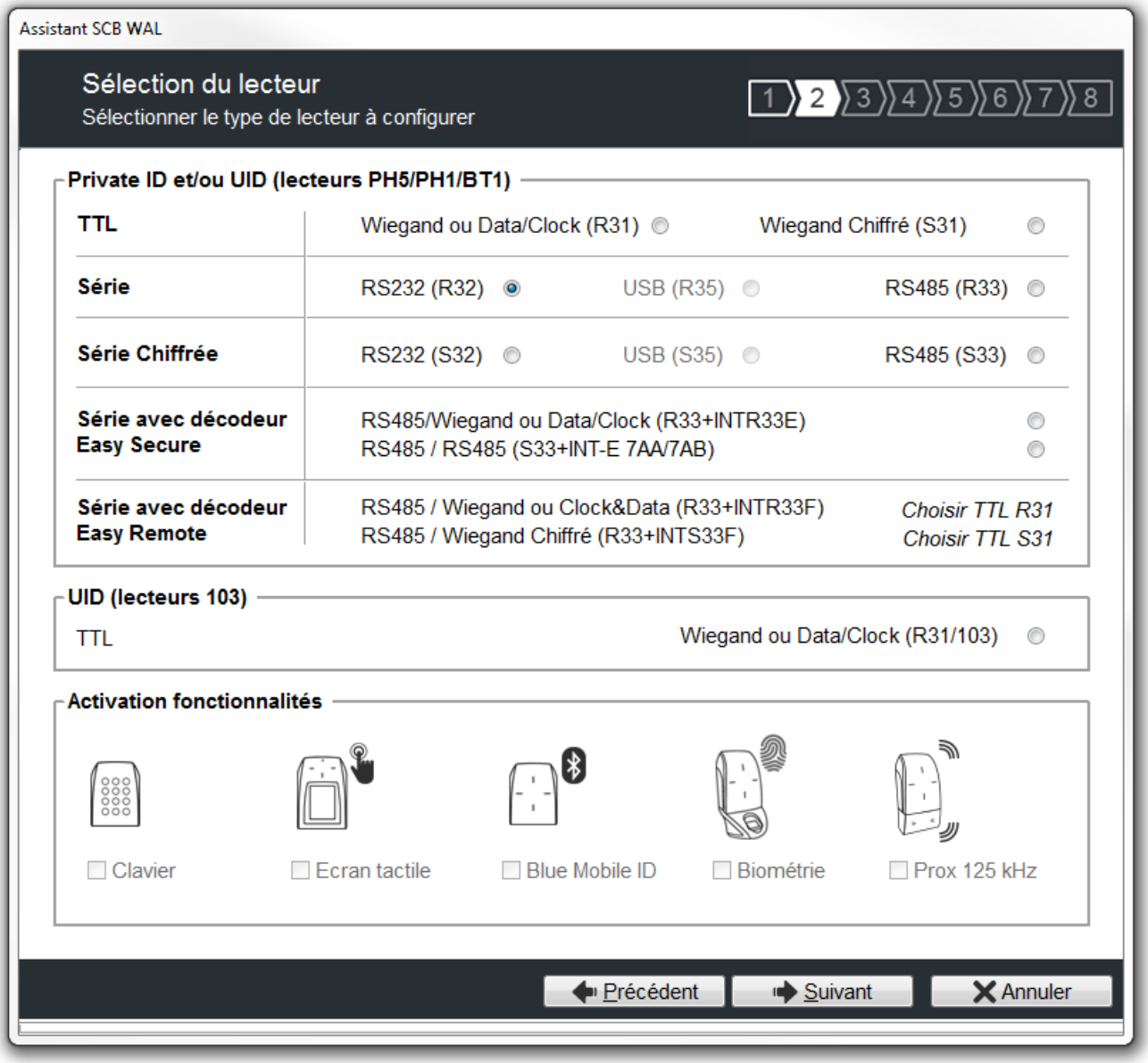


Les fonctionnalités disponibles et la compatibilité des badges SCB dépendent de la génération de firmware des lecteurs. Pour connaître la version du firmware, se reporter au paragraphe *T2.1 - Mise sous tension*.

Pour assurer la compatibilité entre les différentes versions de SCB et de firmware, SECard V2.1.x donne le choix à l'utilisateur de la version de SECard à utiliser si l'option a été validée dans l'onglet « *Fichiers* ».*cf. **II.** 3 - Fichiers*.



<u>Remarque</u> : pour les WAL dont le Firmware est inférieur ou égal à Z17 utiliser l'assistant « Configuration gamme LX ».

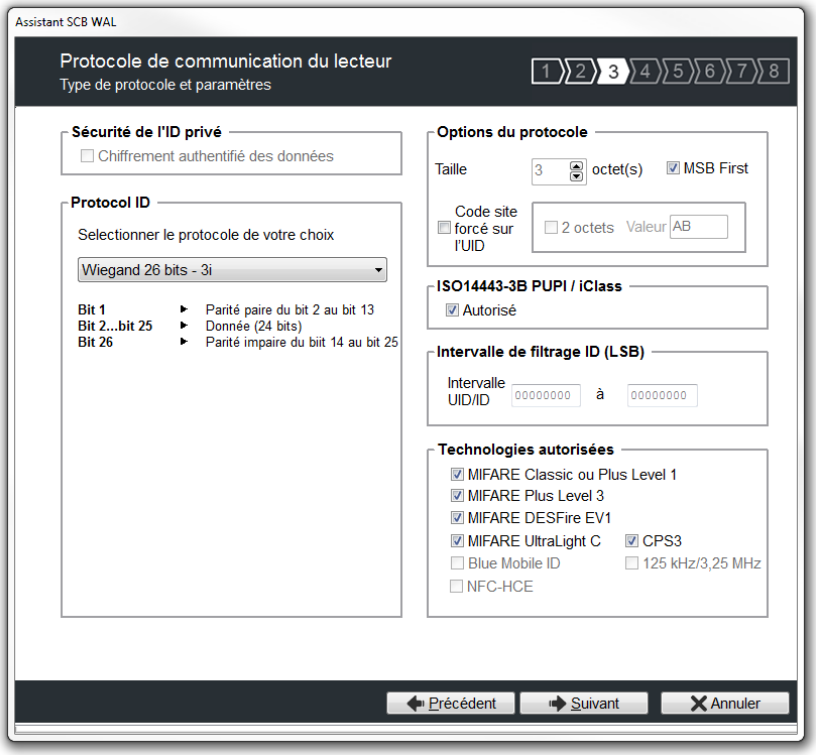


Cette étape permet :

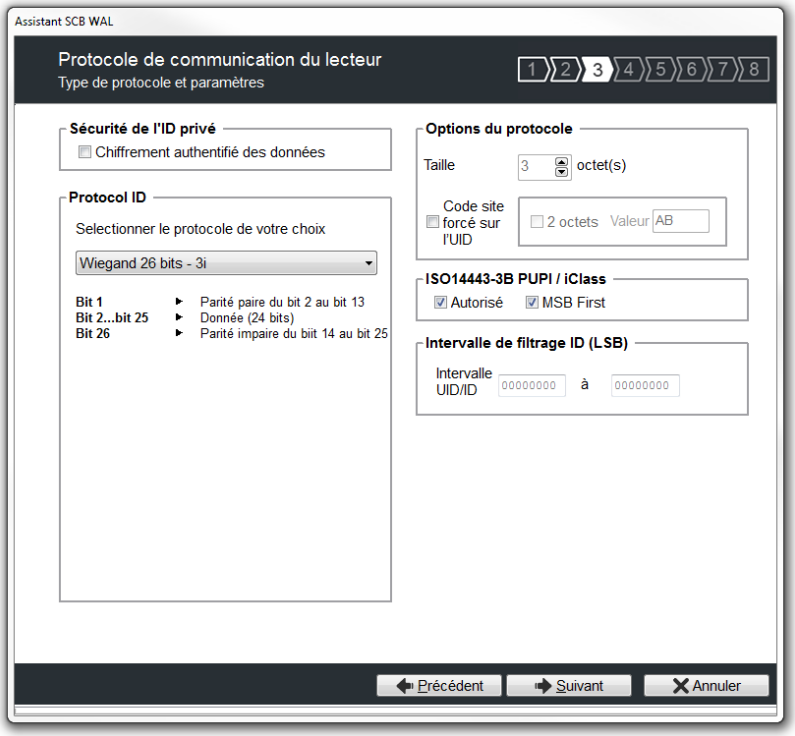
- De choisir le type de lecteur à configurer.

La gamme WAL n'a pas de fonctions externes et n'existe pas en sortie USB.

Cette fenêtre apparait lorsque le type de lecteur sélectionné à l'étape 2 est R31/103 :



Cette fenêtre apparait lorsque le type de lecteur sélectionné à l'étape 2 est en sorite TTL :



Protocole

Elle contient les différents protocoles de communication TTL supportés par le lecteur.
Pour plus d'information sur les protocoles se reporter au paragraphe *T4 - Au sujet des protocoles de communication TTL*.

Note : lors de l'encodage d'un identifiant, celui-ci est réalisé au format du protocole en cours (exemple : Décimal 13 caractères pour le protocole 2B – 10 caractères en hexadécimal pour le protocole 3Cb).

Options du protocole

- « *Taille* » permet d'ajuster la taille des protocoles personnalisables.

  Taille maximum en Wiegand : 48 octets
  Taille maximum en Data/Clock : 10 octets

- « *Code site forcé sur l'UID* » permet de forcer un code site quel que soit le protocole de communication. La valeur du code sera transmise en poids fort sur un ou deux octet(s). L'UID peut donc être tronqué selon le protocole utilisé. Cette option n'est pas disponible pour le Wiegand 64 bits - 3T.

ISO 14443-3B PUPI / iClass

Il est possible de gérer différemment les PUPI ISO14443-3B et 14443-2B exclusivement en calculant un code d'authentification de message utilisant une fonction de hachage cryptographique (SHA1) en combinaison avec une clé secrète. Les autres types de modulation (ISO14443-A) et fréquences (125 kHz /3.25 MHz) ne sont pas affectés par cette option.

Si la taille du protocole est inférieure à 20 octets, un troncage LSB sera effectué sur les 20 octets de signature obtenus.
Si la taille du protocole est supérieure à 20 octets, un padding à zéro sera effectué.

Intervalle de filtrage ID (LSB)

Il est possible de restituer un UID/ID uniquement si celui-ci est compris dans une plage spécifique bornée sur 4 octets.

Si la taille de l'UID/ID est supérieure à 4 octets, l'intervalle s'effectuera sur les 4 octets LSB (prise en compte de l'option MSB First au préalable). Les bornes sont incluses, limite basse ≤ UID/ID ≤ limite haute.

Si l'UID/ID est compris dans l'intervalle, le lecteur restituera le code suivant le protocole en cours et effectuera une action badge LED + Buzzer (SCB). Dans le cas contraire, le lecteur allumera la LED rouge + Buzzer durant 400ms (non paramétrable et non désactivable).

L'UID/ID comparé est la valeur hexadécimale après prise en compte du paramètre MSB First et avant mise en forme protocolaire.
Par exemple pour un protocole 2S, le code comparé sera le code sur 4oct avant codage au format 2S

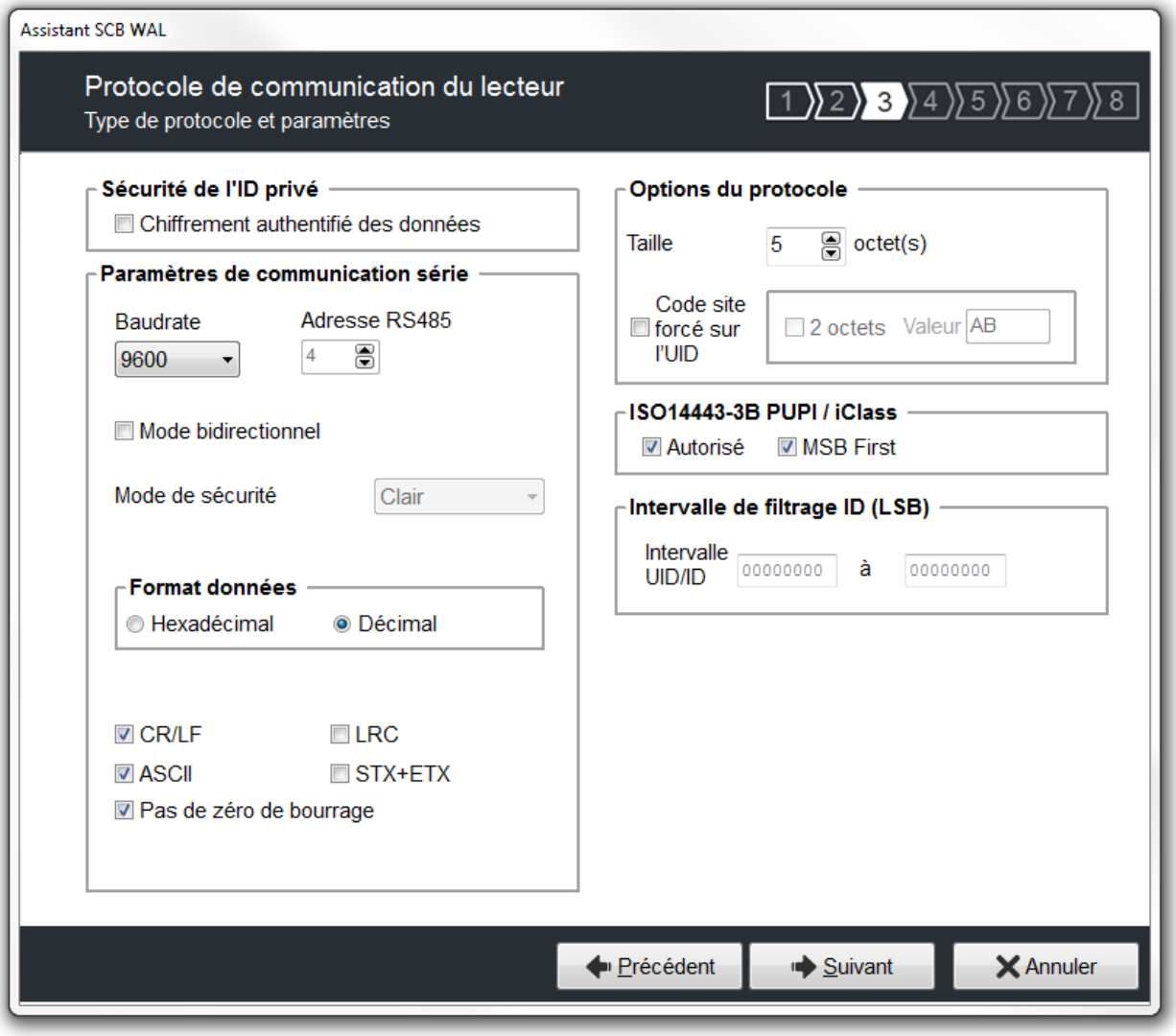
Technologies autorisées

Lorsque le lecteur sélectionné est de type UID seul, cette liste permet de sélectionner le type de technologies de puce pouvant être lues par le lecteur.

Sécurité de l'ID privé

Les identifiants privés peuvent être chiffrés ET signés avant d'être écrits dans le badge.
Le lecteur déchiffrera et authentifiera l'identifiant privé ainsi protégé avant de l'envoyer sur son média de sortie. Seul un identifiant correctement déchiffré et authentifié produira un code de sortie, sinon le lecteur restera muet.
Le chiffrement-authentification utilise le mode AtE (Authenticate Then Encrypt).
Le chiffrement, si activé, sera effectif pour tous les encodages des différentes puces.
Remarque : la taille de l'identifiant privé est limitée à 12 octets.

Cette fenêtre apparait lorsque le type de lecteur sélectionné à l'étape 2 est en sortie série :



Paramètres de communication série

Il contient les différents paramètres de communication série.

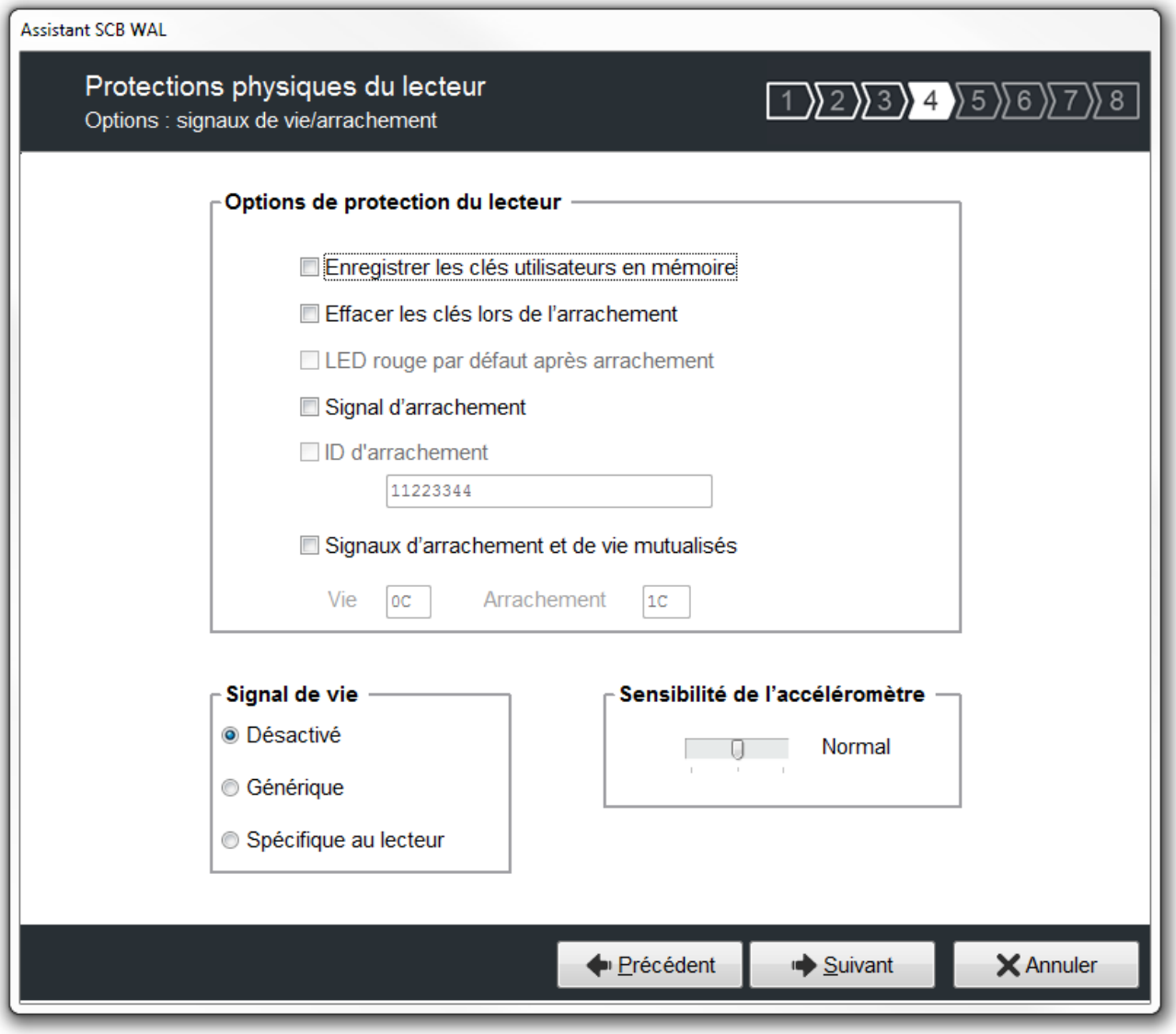
Pour plus d'information sur les protocoles se reporter au paragraphe *T5 - Au sujet des protocoles de communication Série*.

Options du protocole

« *Taille* » permet d'ajuster la taille des données.

Taille maximum en Hexadécimal : 48 octets
Taille maximum en Décimal : 10 octets

Note :
Il est possible d'augmenter la taille du champ au-delà des tailles maximum, pour cela, maintenir la touche CTRL enfoncée et cliquer dans le champ « *Taille données* », la valeur apparait alors soulignée. Cette manipulation ne fonctionne pas pour un encodage mais uniquement pour la relecture d'un identifiant. Uniquement disponible sur les lecteurs séries.



Options de protection du lecteur

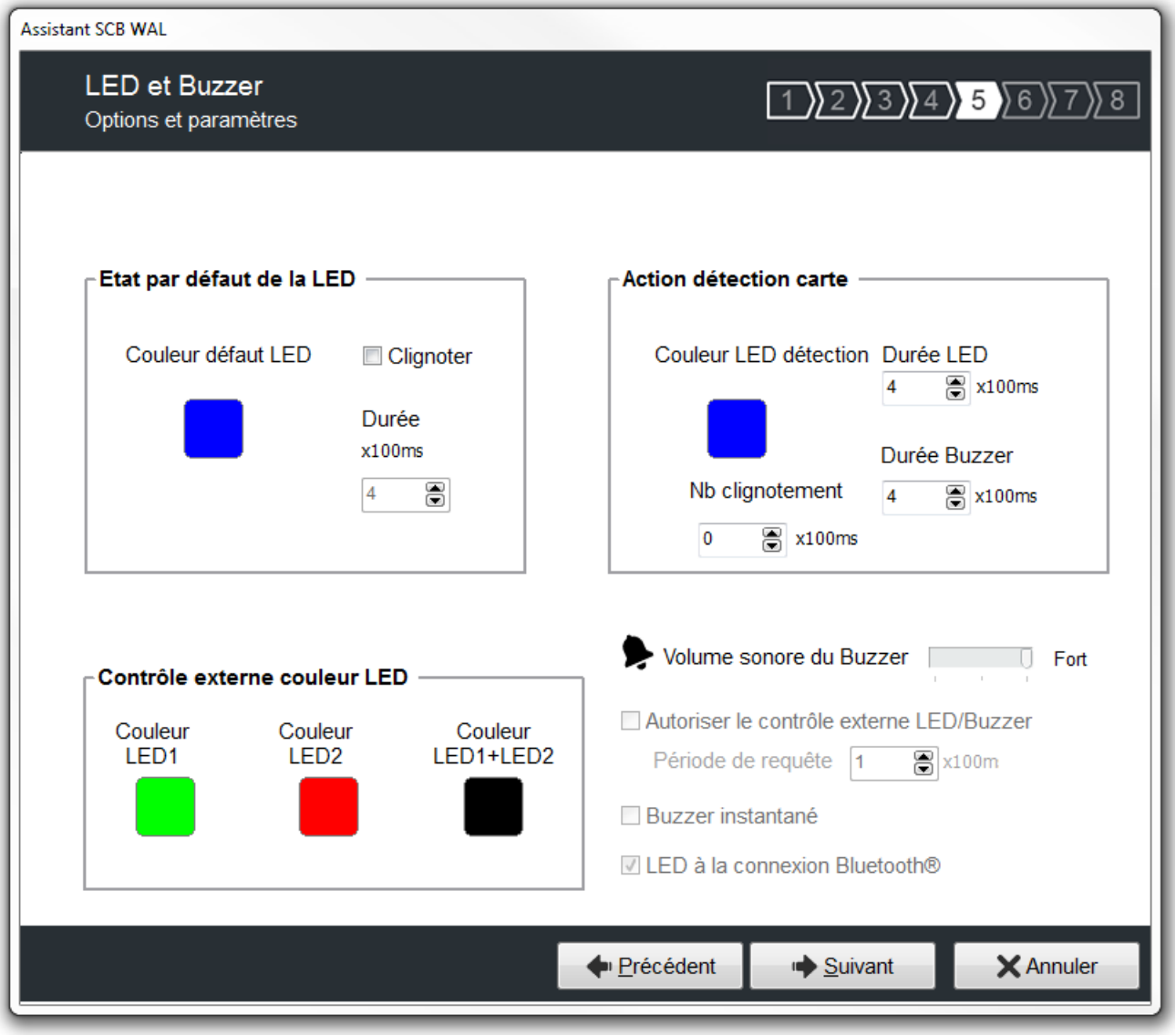
- Enregistrer les clés utilisateurs en mémoire : permet de sauvegarder les clés, de façon chiffrée, en cas de coupure d'alimentation. Les clés sont enregistrées en EEPROM mémoire non volatile.
- Effacer les clés lors de l'arrachement : permet d'effacer toutes les clés du lecteur si un changement d'état intervient sur l'accéléromètre du lecteur.
- LED rouge par défaut après arrachement : nécessite l'activation de l'arrachement.
  Si un changement d'état intervient sur l'accéléromètre du lecteur, la LED passe sur la couleur rouge indiquant que les clés ont été effacées.
- Signal d'arrachement : permet d'activer le signal d'arrachement. Se reporter au paragraphe *T11 - Signal d'arrachement.*
- ID signal d'arrachement : *paramètre non disponible pour les lecteurs standards, uniquement accessible depuis le Wizard des lecteurs ARC*.
- Signaux d'arrachement et de vie mutualisés : permet d'activer l'envoi dans une trame, d'un signal d'arrachement et de vie, disponible uniquement pour les lecteurs *R31*, *S31 et R33+INTR33E*. Se reporter au paragraphe *T13 - Signal de vie / arrachement mutualisés.*

Signal de vie

Permet d'activer / désactiver le signal et de choisir le type de signal « Générique » ou « Spécifique ».
Se reporter au paragraphe *T10 - Signal* de vie.

Sensibilité de l'accéléromètre

Les lecteurs de la gamme WAL sont équipés d'un accéléromètre pour détecter l'arrachement du lecteur.
En fonction du support / lieu d'installation du lecteur, il peut être nécessaire de régler la sensibilité du capteur afin que seul un arrachement effectif soit détecté.



Etat par défaut de la LED

Permet de définir l'état (couleur & clignotement) de la LED en fonctionnement normal.

Action détection carte

Permet de définir l'état (couleur & clignotement) de la LED et du buzzer lors de la détection d'un identifiant. Cette information est indépendante de l'acceptation de l'identifiant.

Volume sonore du Buzzer et LED à la connexion Bluetooth®

Paramètres non disponibles pour les lecteurs WAL, uniquement accessible depuis le Wizard des lecteurs ARCS.

Buzzer instantané

Permet au lecteur d'activer le buzzer à chaque détection d'identifiant sans attendre de commande du système. Disponible uniquement pour les lecteurs séries (R/S-32 et R/S-33) en mode bidirectionnel.

Autoriser le contrôle externe LED / Buzzer

Permet de contrôler la LED et le buzzer de façon externe. La période d'interrogation est réglable par pallier de 100ms. Disponible uniquement pour les lecteurs séries (R/S-32 et R/S-33) en mode bidirectionnel.

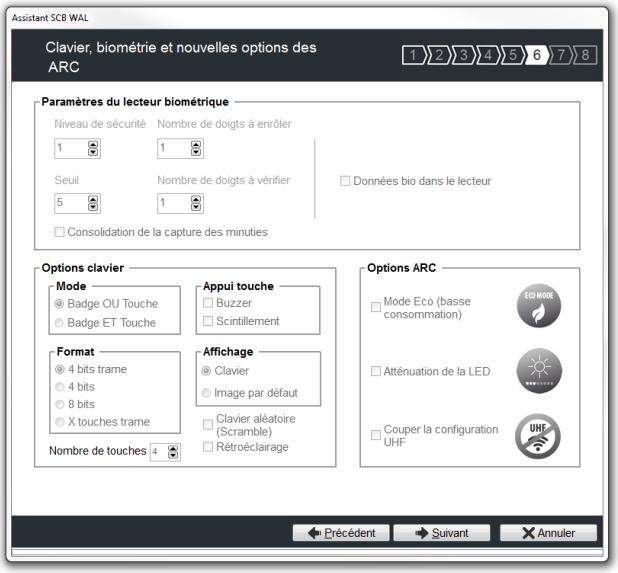
Contrôle externe couleur LED

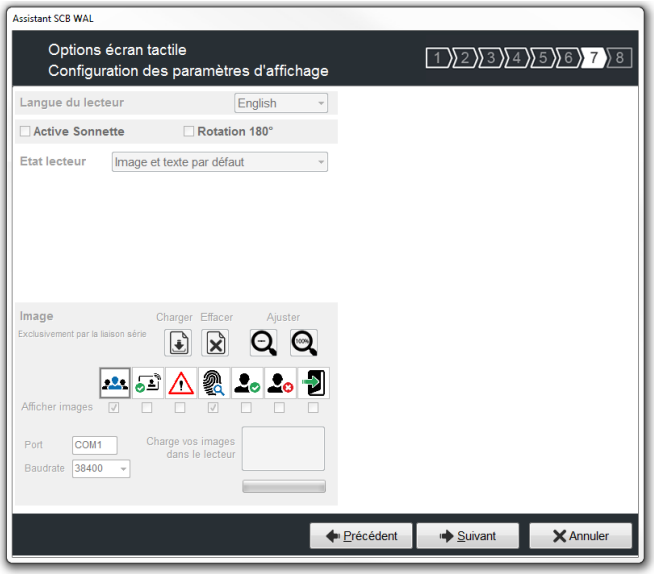
Permet de définir la couleur de l'entrée LED1, de l'entrée LED2 et des deux entrées LED si elles sont commandées simultanément.

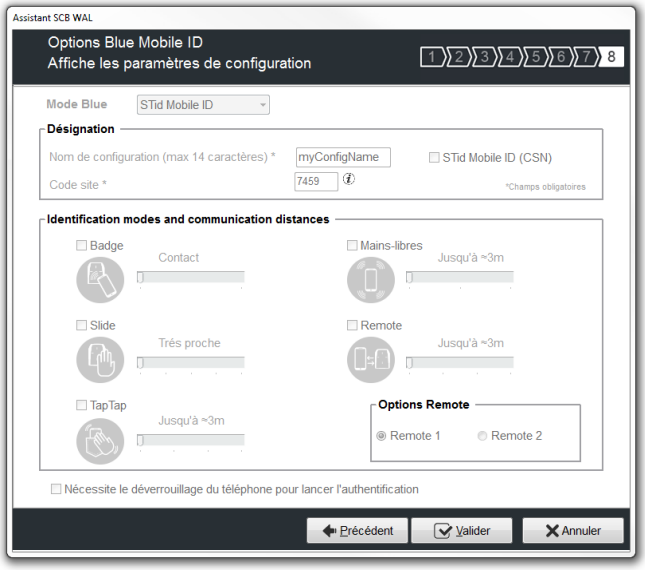
Pour modifier et sélectionner une couleur, cliquer sur les boutons de couleur, la fenêtre suivante s'ouvre :

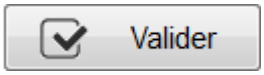
Pour sélectionner une couleur prédéfinie, cliquer sur un des carrés de couleur.

Options non disponibles pour les lecteurs WAL, uniquement accessibles depuis le Wizard des lecteurs standards et/ou ARC.



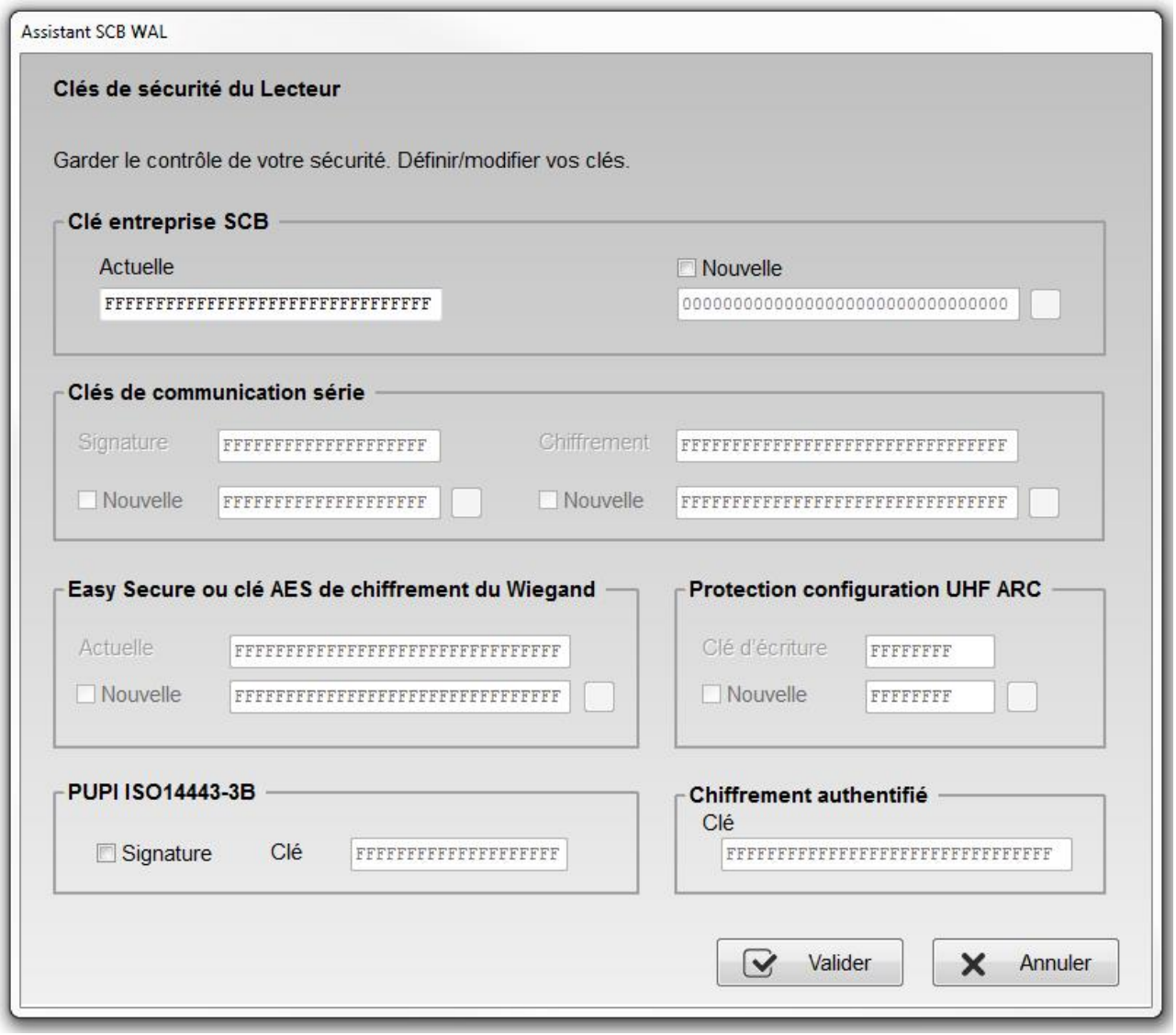




Cliquer sur le bouton 

pour terminer la configuration des paramètres lecteurs.

III. 6 - Assistant SCB WAL : clés de sécurité du lecteur



Clé entreprise SCB

Les lecteurs configurables par les badges « *SCB* » sont livrés initialement avec une configuration par défaut (clé usine 0XFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF).
Ceux-ci pourront donc être configurés par un SCB de clé courante 0xFF…FF vers une nouvelle clé entreprise.
Elle peut être saisie manuellement ou automatiquement en appuyant CTRL+R ou en effectuant un clic droit « *Remplir avec une valeur aléatoire* ».

Attention

Cette clé est importante et doit absolument être connue de l'administrateur. Elle protège les données du « *SCB* » et permet des modifications sur la configuration des lecteurs.

En cas de perte de cette clé, le lecteur ne pourra plus être reconfiguré par un autre « *SCB* » et devra obligatoirement être réinitialisé en usine.

Après la première configuration et afin de pouvoir reconfigurer le lecteur, il sera nécessaire de présenter au lecteur des badges « *SCB* » possédant une clé entreprise identique à celle enregistrée par le lecteur.

Note : la clé entreprise représente également lors de la création d'un badge utilisateur MIFARE Plus® les valeurs de la clé Maître Badge, de la clé configuration badge et de la clé de changement de niveau 3.

Clés de communication série

Permet de modifier la clé de signature et la clé de chiffrement utilisateur pour les lecteurs série chiffrés (S32 / S33).
Pour plus de détail sur la communication série sécurisée se reporter au paragraphe *T5.2 - Mode de communication bidirectionnel.*

Easy secure ou clés AES de chiffrement du Wiegand

Permet de modifier la clé de chiffrement utilisée pour sécuriser la liaison du lecteur S31 et du lecteur R33+INTR33E.

Note :
La valeur de la clé de chiffrement AES par défaut (sortie usine) est égale à «*FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF*».
Il est obligatoire de changer la valeur de cette clé afin que la sortie soit chiffrée.

PUPI ISO 14443-3B

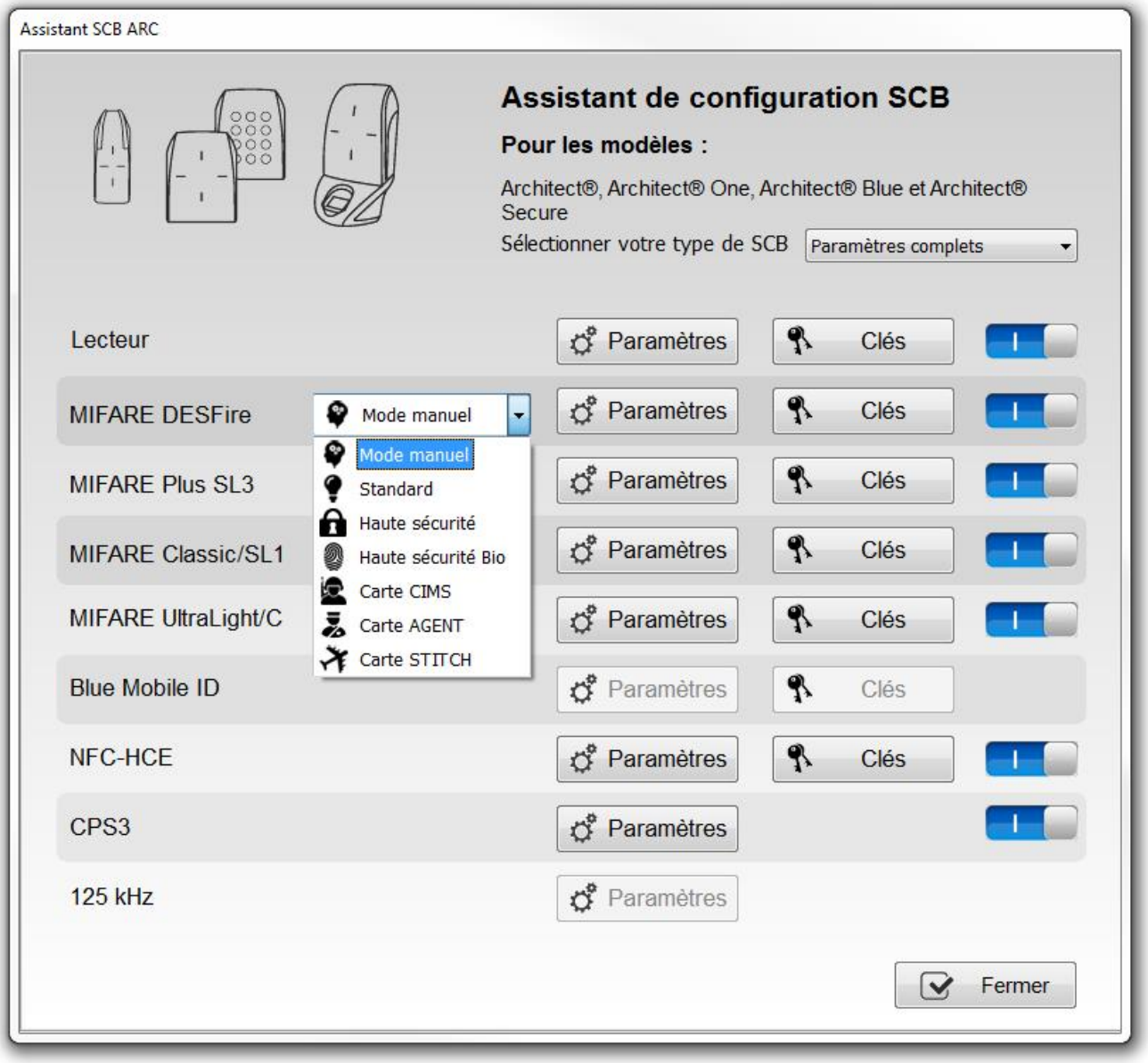
Permet de renseigner la clé utilisée pour le calcul de la signature dite « clé secrète » sur 10 octets.

Protection configuration UHF ARC : *non disponible pour les lecteurs WAL*.

Chiffrement authentifié :

Permet de renseigner la clé pour le chiffrement authentifié.

III. 7 - MIFARE® DESFire® : paramètres



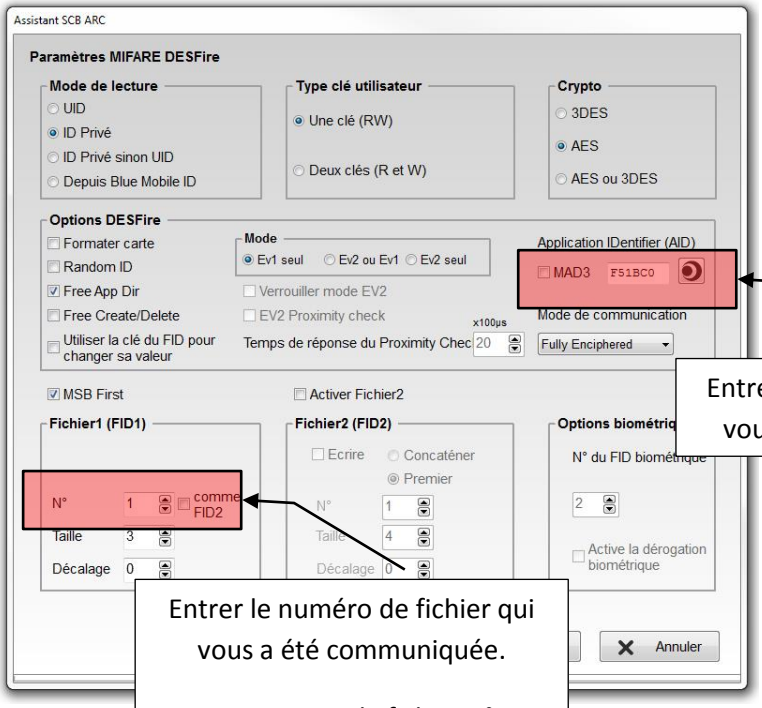
Pour faciliter le paramétrage de la puce DESFire, un menu déroulant propose des pré-configurations. En fonction de la configuration choisi les paramètres sont automatiquement sélectionnés et des valeurs de clés sont générées aléatoirement, il est toujours possible de visualiser et/ou apporter des modifications à l'aide des boutons Paramètres et Clés.

Mode Manuel : Tous les paramètres et les clés sont à renseigner manuellement.

Mode Standard : Correspond à une configuration sécurisé standard.
Mode Haute Sécurité : Correspond à une configuration haute sécurité avec Diversification des clés.
Mode Haute Sécurité Bio : Correspond à une configuration biométrie haute sécurité.

Dans les trois modes correspondants à des cartes spécifique (CIMS, AGENT et STITCH), les paramètres nécessaires à leur exploitation sont présélectionnés et les champs clés à utiliser pré remplies. Il faudra remplacer certaines valeurs par celle du site.

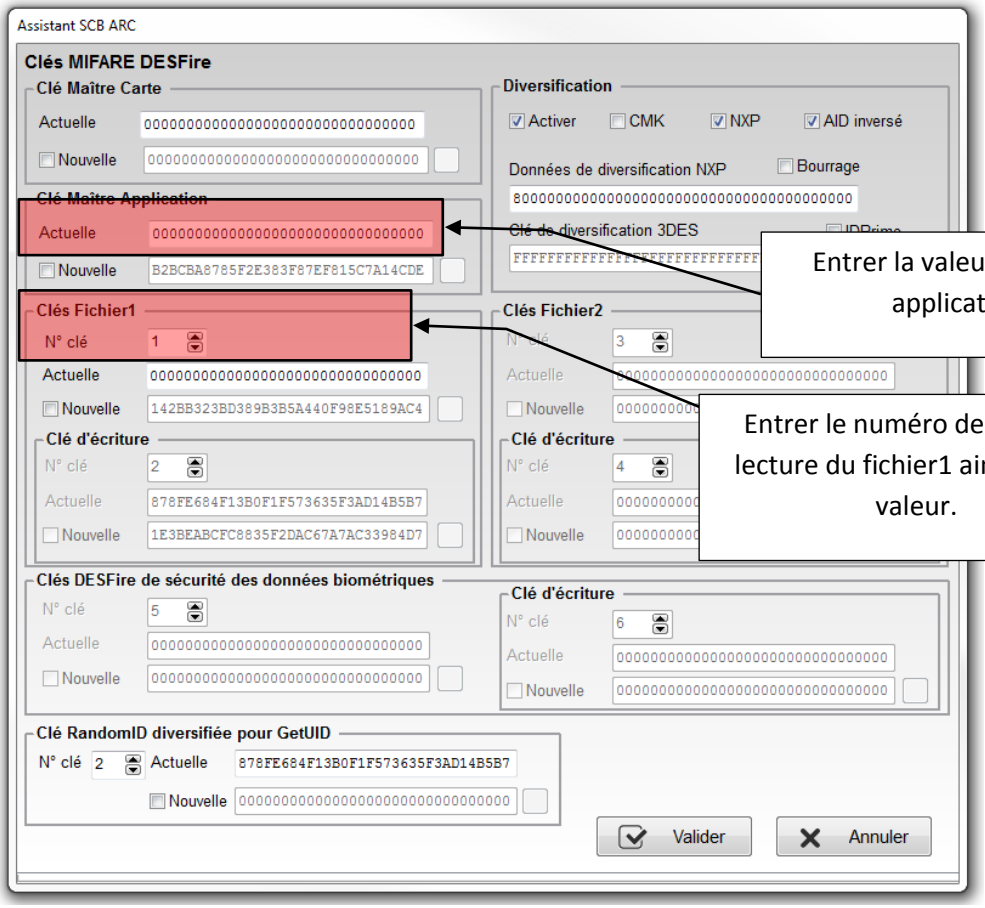
Carte CIMS :



Entrer la valeur de l'AID qui vous a été communiqué.

Entrer le numéro de fichier qui vous a été communiquée.

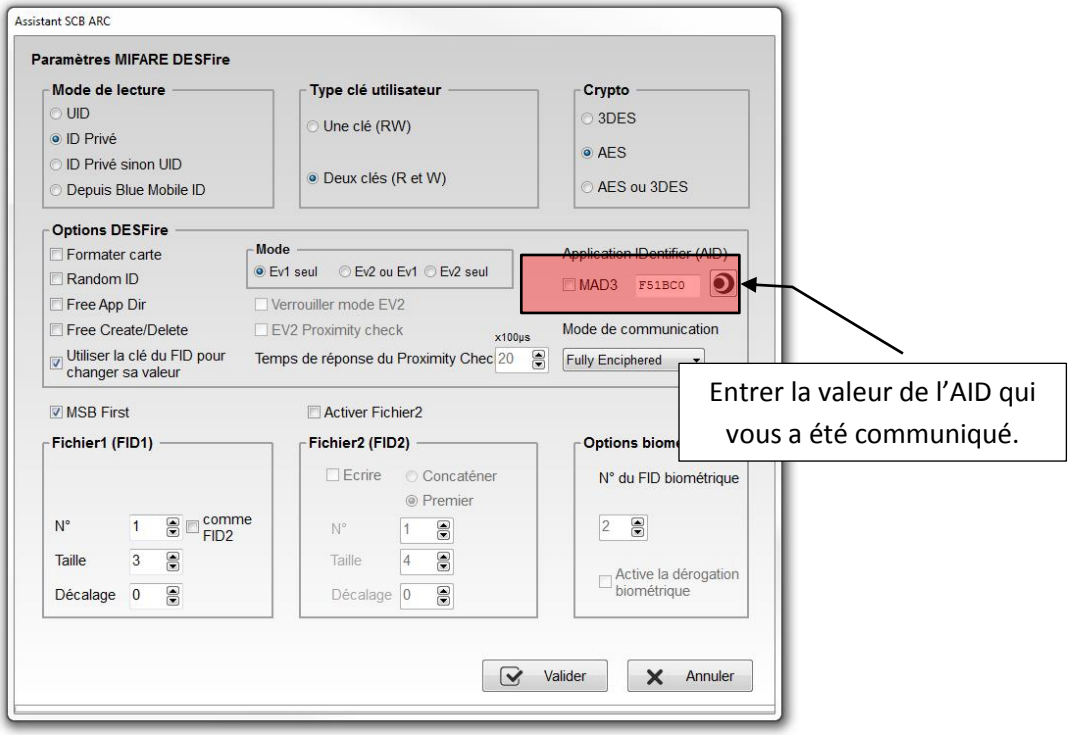
Couramment le fichier n°1



Entrer la valeur de la clé applicative

Entrer le numéro de la clé de lecture du fichier1 ainsi que sa valeur.

Carte Agent :



Entrer la valeur de l'AID qui vous a été communiqué.

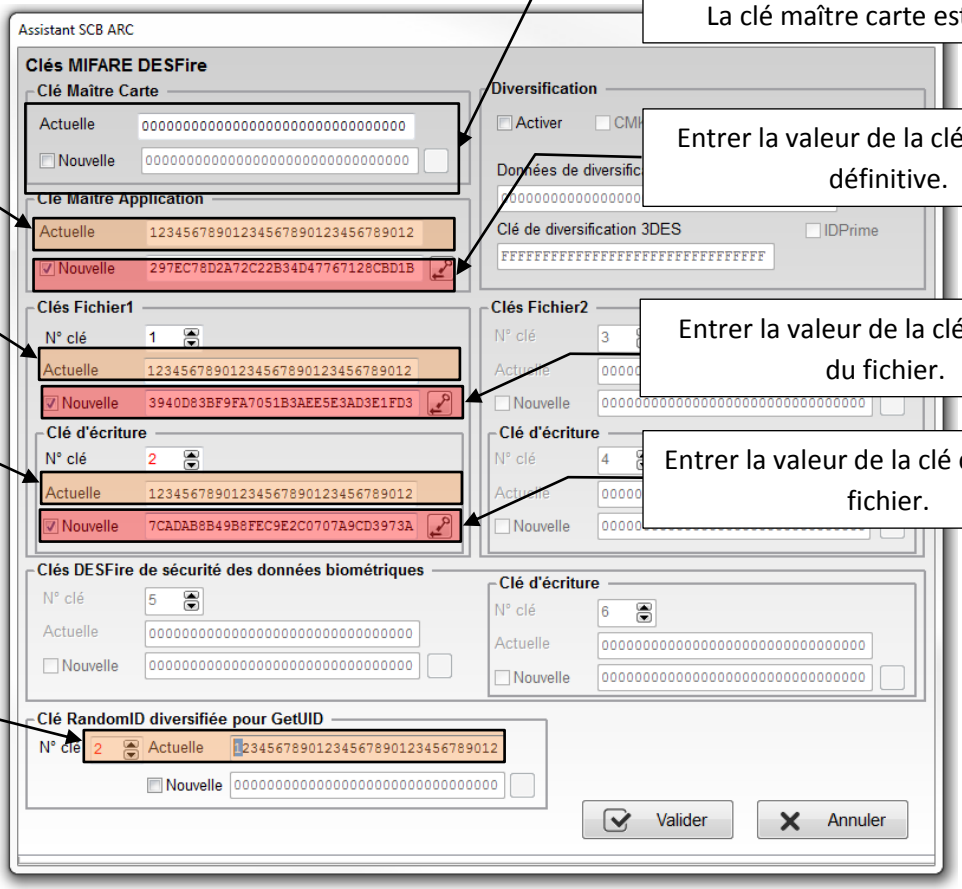
Entrer la valeur de la clé applicative partagée (clé de transport).

Ne rien inscrire dans ces champs. La clé maître carte est secrète.

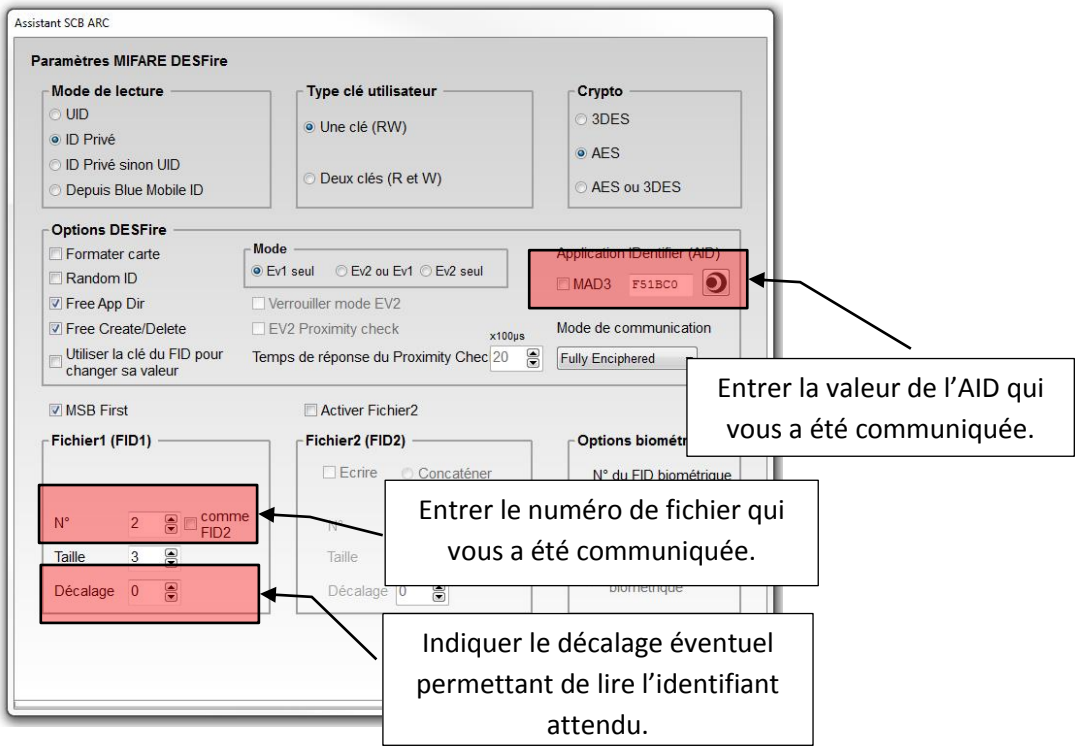
Entrer la valeur de la clé applicative définitive.

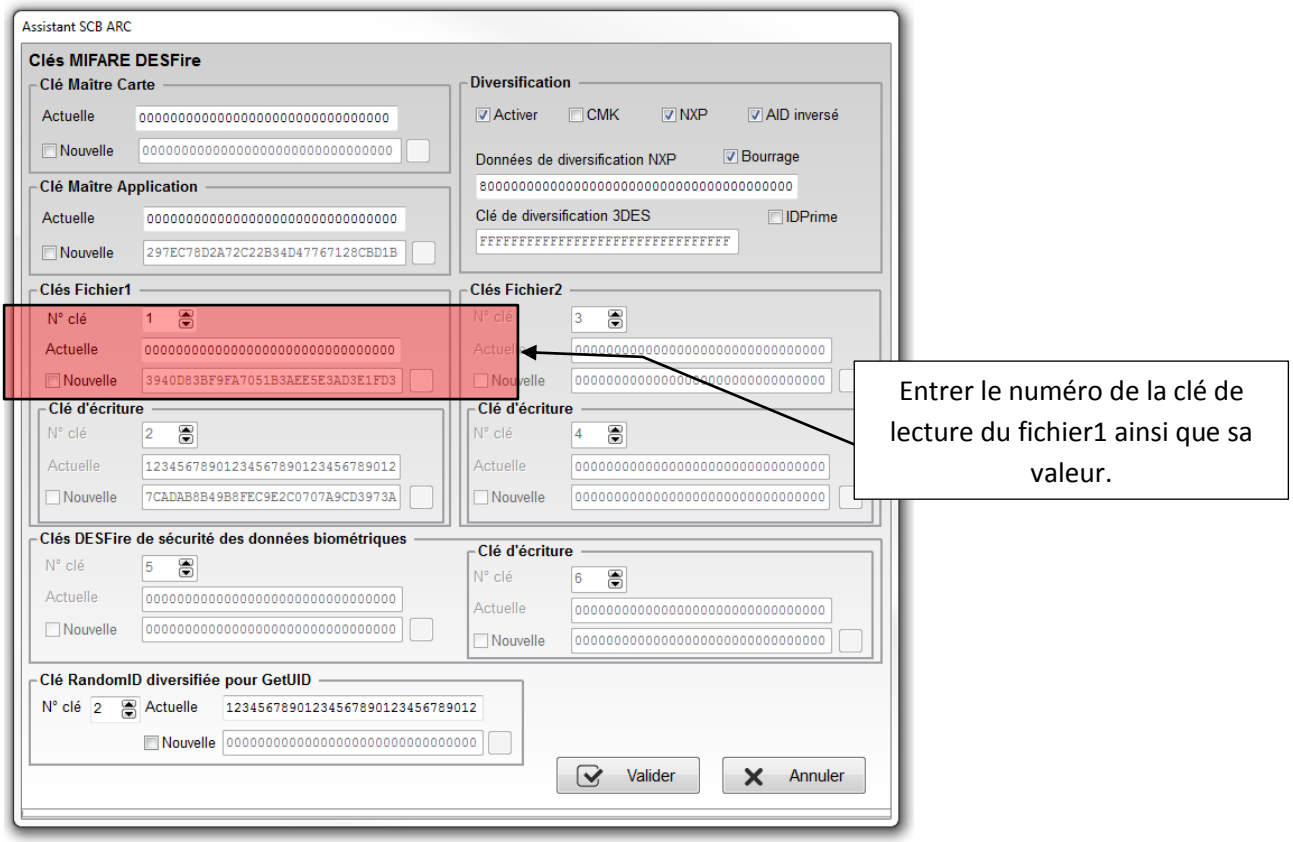
Entrer la valeur de la clé de lecture du fichier.

Entrer la valeur de la clé d'écriture du fichier.

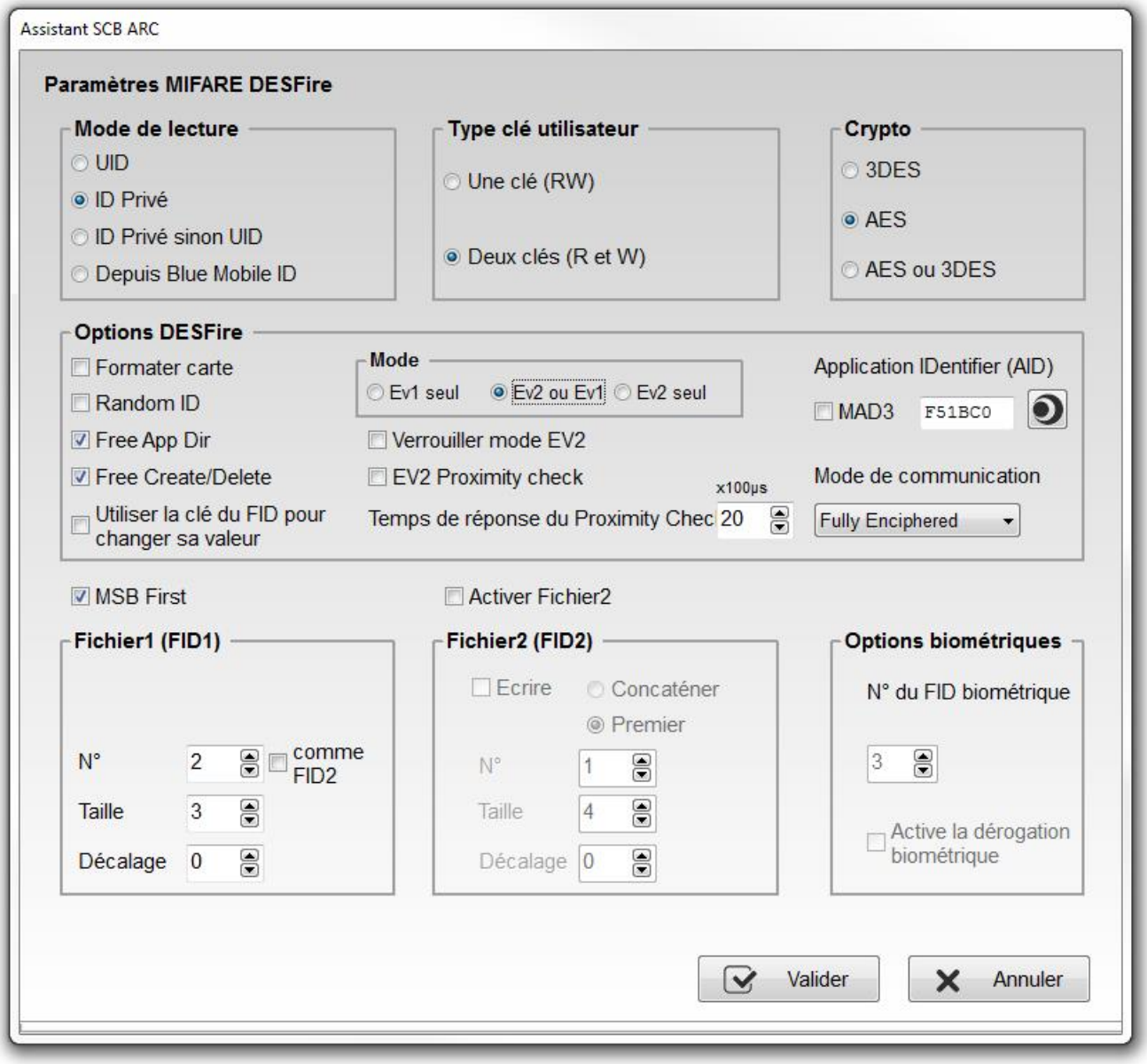


Carte STICTCH





Mode Manuel



Mode de lecture

- ❖ UID : Lecteur configuré uniquement en lecture de numéro de série.
- ❖ ID Privé : Lecteur configuré uniquement en lecture de code privé.
- ❖ ID Privé sinon UID : Lecteur configuré en lecture de code privé. Si celui-ci n'est pas trouvé ou si les paramètres de sécurité sont incorrects, alors le lecteur lira et retournera l'UID.
- ❖ Depuis Blue Mobile ID : Lecteur configuré uniquement pour lire une configuration héritée de la configuration BlueMobileID, nécessite qu'une configuration BlueMobileID soit active.

Type clé utilisateur

- ❖ Une clé (RW) : Utilisation d'une seule clé par fichier servant pour la lecture et l'écriture.
- ❖ Deux clés (R et W) : Utilisation de deux clés par fichier. Une clé servant pour la lecture, la seconde pour la lecture et l'écriture.

Crypto

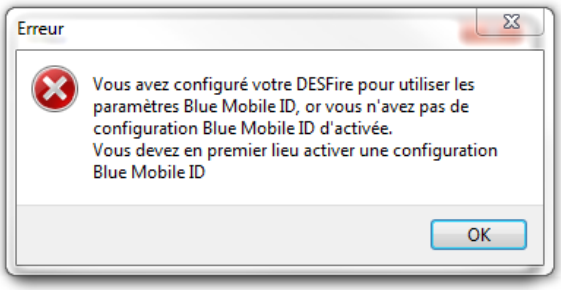
Permet de choisir la méthode d'authentification à utiliser.

- 3DES
- AES
- AES ou 3DES : Dans ce cas, le lecteur acceptera les deux méthodes d'authentification. Première authentification en AES, seconde en 3DES. La valeur de la clé doit être identique.

Pour modifier la méthode de crypto de la clé Maître, il faut cocher la case « *Nouvelle* », entrer la valeur de la clé dans le champ et choisir la méthode d'authentification.

*Depuis BlueMobileID

- Si « DepuisBlueMobileID » est sélectionné et que la configuration « BlueMobileID » n'est pas activée, le message suivant apparait :



- Dans ce mode, les paramètres DESFire sont automatiquement déterminés et hérités de la configuration Blue.

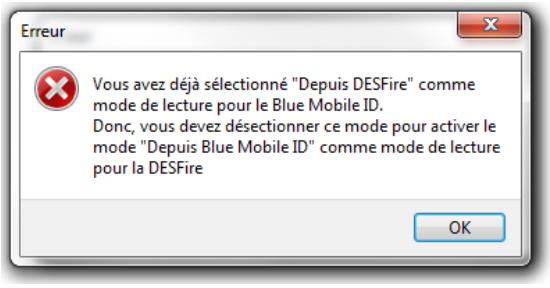
  Les paramètres fixés et non modifiables :

  - ✓ Méthode de Crypto : AES
  - ✓ AID : 0xF"code site de la configuration Blue"0
  - ✓ MSB First
  - ✓ RandomID : non
  - ✓ Activer Fichier 2 : non
  - ✓ Type de donnée : Brut
  - ✓ FID1 : 0
  - ✓ Taille et décalage identique à ceux de la configuration Blue.

  Les paramètres modifiables sont :

  - ✓ Formater carte
  - ✓ FreeAppDir
  - ✓ N° du FID des données biométriques

- Si DepuisBlueMobileID est sélectionné et que la configuration BlueMobileID est activée sur DepuisDESFire, le message suivant apparait :



Options DESFire®

❖ **Formater carte :**

Si cette option est activée, les puces DESFire® EV1/2 seront formatées avant encodage.
Pour cela, il est nécessaire d'entrer la valeur courante de la Clé Maître de la puce.

> **Attention**
>
> Cette option effacera complètement les données (applications et fichiers) de la puce mais pas la clé maître actuelle.

❖ **Random Id :**

Si cette option est activée, les puces DESFire® EV1/2 encodées seront configurées en mode Random Id. Cela signifie que le numéro de série remonté à chaque Scan sera différent et codé sur 32 bits maximum.

> **Attention**
>
> Cette option est irréversible. Le Random Id ne pourra plus être désactivé par la suite.

❖ **Free App dir :**

Si cette option est activée la lecture de la liste des applications présentes dans la puce sera possible sans authentification.
Cette option est activée par défaut sur la puce DESFire® EV1/2.

❖ **Utiliser la clé du FID pour changer sa valeur :**

Par défaut dans SECard, un changement de valeur de clé de fichier nécessite une authentification préalable avec la Clé Maître de l'application (AMK). Et un changement de Clé Maître de l'application avec la Clé Maître du badge (CMK).
Si cette option est activée SECard s'authentifiera avec la clé à changer.
Pour utiliser cette option avec une puce qui a été déjà encodée mais pas avec SECard, il faut que l'application ait été créée avec les droits d'accès le permettant : « Configuration Changeable OK » sinon il faudra formater la puce ou effacer l'application.
Dans le cas de l'encodage des Cartes Agents cette option doit être activée.

❖ **Free C/D :**

Par défaut dans SECard, les applications sont créées avec le paramètre Free Create/Delete : la création / suppression de fichier ne nécessite pas d'authentification avec la clé Maître de l'Application.

Si la case est cochée, elles seront créées sans Free Create/Delete: la création / suppression de fichier nécessite une authentification avec la clé Maître de l'Application.

❖ **Communication mode :**

Dans une puce DESFire® EV1/2 le fichier peut être créé avec un niveau de sécurité de la communication, entre la puce et le lecteur, paramétrable suivant trois modes :

- **Plain** : communication en clair.
- **MACed** : communication en clair protégée par signature DES/3DES ou AES.
- **Fully Enciphered** : communication entièrement chiffrée en DES/3DES ou AES.

Le choix du mode de communication dans SECard s'effectue donc en fonction du mode de communication choisi lors de l'encodage.

> **Attention**
>
> Par défaut dans SECard, le mode de communication choisi lors de la création des fichiers a toujours été Fully Enciphered jusqu'aux versions de SECard < 3.0.0

❖ **Application IDentifier (AID)** :

Si la case « *MAD3* » est cochée, alors la valeur de l'identifiant de l'application à créer sera sur quatre caractères. La valeur finale de celui-ci sera sur six, SECard forçant le premier caractère à la valeur « F » et le dernier à la valeur « 0 ».
Exemple : pour un Identifiant Application « 51BC », l'identifiant de l'application créée sera « F51BC0 ».

Si la case « *MAD3* » n'est pas cochée, le champ de l'*AID* ne sera plus bridé et complètement personnalisable par l'utilisateur. Il sera donc possible de le définir sur 6 caractères.

❖ **Mode pour le paramétrage en lecture du lecteur**

La DESFire Ev2 offre des fonctionnalités de sécurité (Secure messaging Ev2) que nous appellerons ici Mode Ev2 : comprenant l'interdiction de dialoguer en Ev1 et en 3DES.

Ev1 seul :	Lecteur configuré pour lire les Ev1 et les Ev2 en mode Ev1. Une Ev2 non verrouillée en mode Ev2 (Lock Ev2) sera lue comme une Ev1. Une Ev2 verrouillée en mode Ev2 (Lock Ev2) ne pas sera lue.
Ev2 ou Ev1 :	Lecteur configuré pour lire les Ev2 (Lock Ev2 ou non) et les Ev1. Le lecteur va essayer de communiquer en Ev2, si échec il essai en Ev1.
Ev2 seul :	Lecteur configuré pour lire uniquement les Ev2. Une Ev1 ne sera pas lu.

❖ **Mode pour le paramétrage à l'encodage**

Ev1 uniquement :	Encode uniquement en mode Ev1. Une Ev2 non verrouillée en mode Ev2 (Lock Ev2) sera encodée. Une Ev2 verrouillée en mode Ev2 (Lock Ev2) ne pas sera encodée.
Ev2 ou Ev1 :	Encode une carte EV1 en mode EV1 AES et une EV2 en mode verrouillée ou non en mode Ev2.
Ev2 uniquement :	Encode uniquement des Ev2. Une Ev1 ne sera pas encodée.

❖ **Mode Lock Ev2 (Secure messaging)**

Uniquement disponible pour des Ev2. Lors de l'encodage la puce sera configurée pour dialoguer uniquement en Secure Messaging Ev2.
Elle ne pourra plus dialoguer en Ev1 ou 3 DES.
Attention : Cette action est définitive, aucun retour possible

❖ **Ev2 Proximity check / Temps de réponse Proximity check**

Active la protection contre les attaques relais**.**
Impose des contraintes de synchronisation plus strictes sur le délai aller-retour autorisé lors de l'authentification, afin de rendre plus difficile la transmission de messages à des cartes éloignées ou à des lecteurs via des réseaux informatiques.

Le temps maximum acceptable pour l'échange du Proximity Check est réglage par l'utilisateur (multiple de 100 micro secondes).

MSB First

Si la case est cochée, le lecteur lira l'identifiant Most Significant Byte First.
Si la case est décochée, le lecteur lira l'identifiant Least Significant Byte First.

Le sens de lecture usuel sur les lecteurs STid est MSB First.

SECard permet à l'utilisateur d'encoder deux fichiers en lui laissant deux possibilités :

- ❖ Soit réserver la place pour le deuxième fichier sans l'encoder.
- ❖ Soit écrire le second fichier en même temps que le premier.

Activer Fichier2

Permet d'activer le paramétrage d'un second fichier.

Fichier1 (FID1)

Permet de paramétrer le premier fichier de données :

- ❖ Type de donnée : permet de choisir le type de format de donnée à lire
  - Raw : donnée brute, si les données à lire ont été encodées en hexadécimal.
  - ASCII décimal : si les données à lire ont été encodées en ASCII décimal – max 17 caractères (8 octets) (par ex : 0x313131 écrit dans le badge sera lu 111 ou 0x6F selon le protocole choisi). ***Disponible que pour les lecteurs ARC et ARC1.***
- ❖ N° : permet de choisir le numéro (entre 0 et 31) du fichier à créer dans l'application.
- ❖ Taille : permet de définir la taille de l'identifiant à encoder.
- ❖ Décalage : permet de définir un décalage dans l'encodage de l'identifiant.
- ❖ comme FID2 : permet d'encoder le second fichier lors d'un futur encodage.
  Il faut alors reporter les données (clés, taille, numéro de fichier…) du second fichier dans les champs de l'encadré Fichier1 (FID1).
  Après cette manipulation, le FID2 sera prêt à être encodé et lu par le lecteur sans reconfiguration d'un badge « *SCB* ».

Fichier2 (FID2)

Permet de paramétrer le second fichier de données si la case Activer Fichier2 est cochée :

- ❖ Ecrire : permet d'encoder le second fichier en même temps que le premier. Si la case n'est pas cochée, le second fichier ne sera pas encodé mais les paramètres seront connus du lecteur.
- ❖ N° : permet de choisir le numéro (entre 0 et 31) du fichier à créer dans l'application.
- ❖ Taille : permet de définir la taille de l'identifiant à encoder.
- ❖ Décalage : permet de définir un décalage dans l'encodage de l'identifiant.
- ❖ Concaténer : cette fonction permet d'indiquer au lecteur qu'il doit lire les fichiers FileID1 et FileID2. Les informations remontées par celui-ci seront alors concaténées (premier fichier puis second fichier). Dans ce cas de configuration, il est nécessaire que la taille des données totales encodées (FileID1 & FileID2) correspondent au format du protocole de sortie défini dans la configuration du lecteur. (exemple : pour un Wiegand 3CB sur 5 octets, la taille totale des deux fichiers devra être 5 octets). Dans le cas inverse, le lecteur tronquera les données du FID2. Dans ce mode, le fichier FID2 est aussi automatiquement écrit au premier encodage si la case « *Ecrire* » est cochée.
- ❖ Premier : dans ce mode, le lecteur lit automatiquement le premier fichier trouvé en fonction des paramètres de sécurité. Si l'authentification avec le fichier FID1 n'est pas possible (mauvaises valeurs de clé par exemple), le lecteur tentera alors de lire le second fichier.

Note :
Les fichiers 1 et 2 sont des fichiers Standards de données (StandardDataFile) de 48 octets chacun.
La communication RF est effectuée selon le choix de l'utilisateur.

Les numéros des deux fichiers doivent être différents l'un de l'autre et du numéro de fichier biométrique, sinon les numéros de fichier apparaitront en rouge.

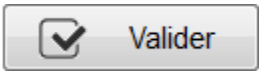
Attention

Dans le cas d'une utilisation de deux fichiers et lorsque l'option « Ecrire » est activée (Concaténer ou Premier), il est important que les tailles définies dans les champs « Taille » des fichiers 1 et 2 **correspondent à celles à encoder.**

Pour cela, l'ajout de 0 non significatifs peut s'avérer nécessaire.
Exemple : pour un ID 0x11 0x22, si la taille définie est sur 3 octets, il faudra alors renseigner 0x00 0x11 0x22.

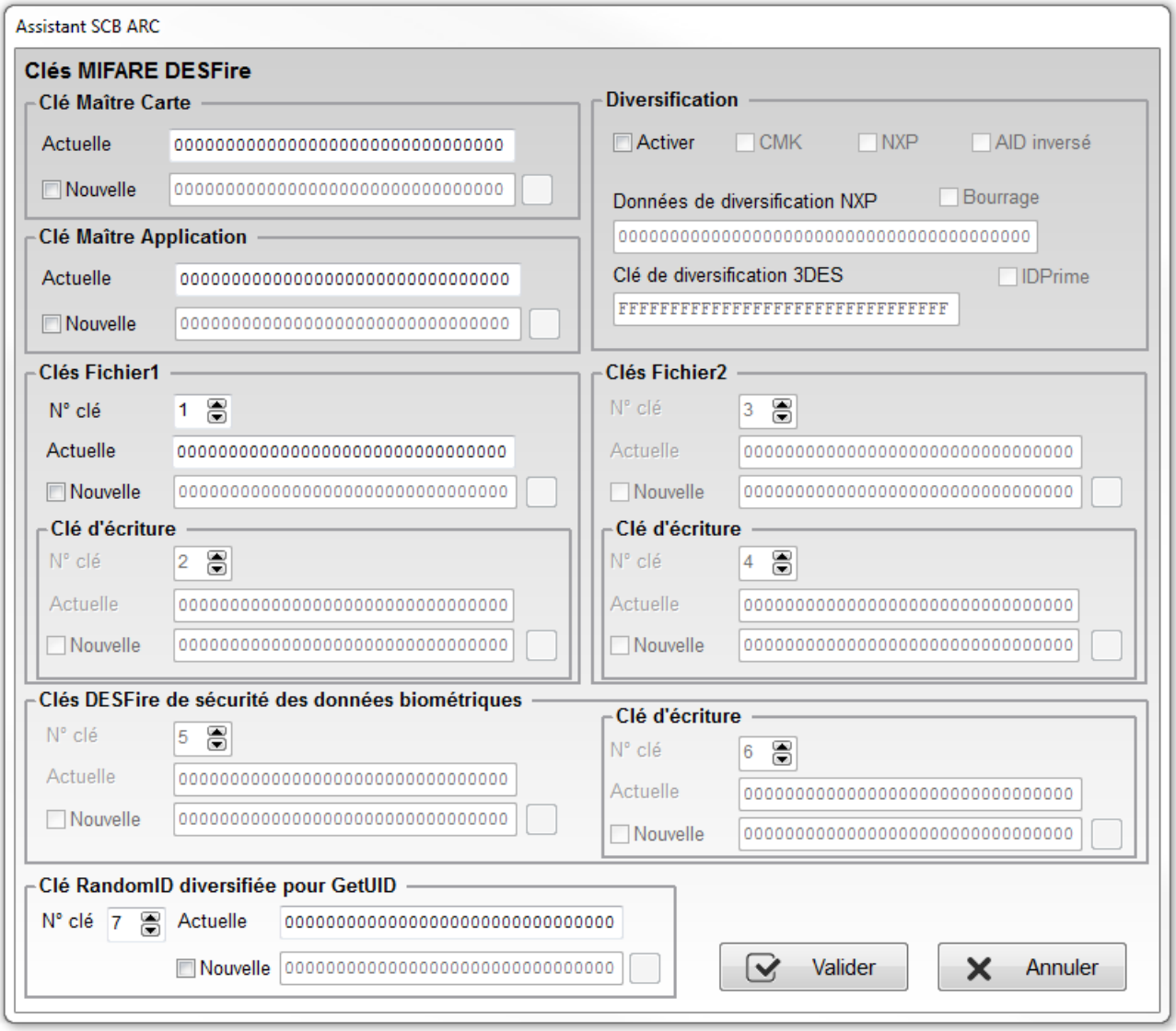
Options biométriques

- ❖ N° du FID biométrique : Permet de choisir le numéro (entre 0 et 31) du fichier dans lequel seront encodées les empreintes. Attention, doit être différent de FID1/2.
- ❖ Active la dérogation biométrique. Se reporter au paragraphe *T7.2 - Dérogation biométrique*

Cliquer sur le bouton 

pour terminer la configuration des paramètres DESFire®.

III. 8 - MIFARE® DESFire® : clés



Permet de définir toutes les clés relatives à la puce MIFARE® DESFire® EV1.
Pour plus d'information sur l'organisation mémoire de la puce se reporter à *T3.2 - Organisation de la mémoire des puces MIFARE® DESFire® et MIFARE® DESFire® EV1/2*.

Clé Maître Carte

La *Clé Maître Carte* est la valeur de la clé maître de la puce MIFARE® DESFire® et MIFARE® DESFire® EV1/2.

Par défaut sa valeur est « 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 » (16 octets à 00h) en crypto 3DES.
Il est recommandé de modifier sa valeur pour optimiser la sécurité.

Clé Maître Application

La *Clé Maître Application* est la valeur de la clé de l'application qui a été définie dans les paramètres de la puce MIFARE® DESFire® et MIFARE® DESFire® EV1/2.

Par défaut sa valeur est « 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 » (16 octets à 00h).
Il est recommandé de modifier sa valeur pour optimiser la sécurité.

Diversification

- ☑ Activer

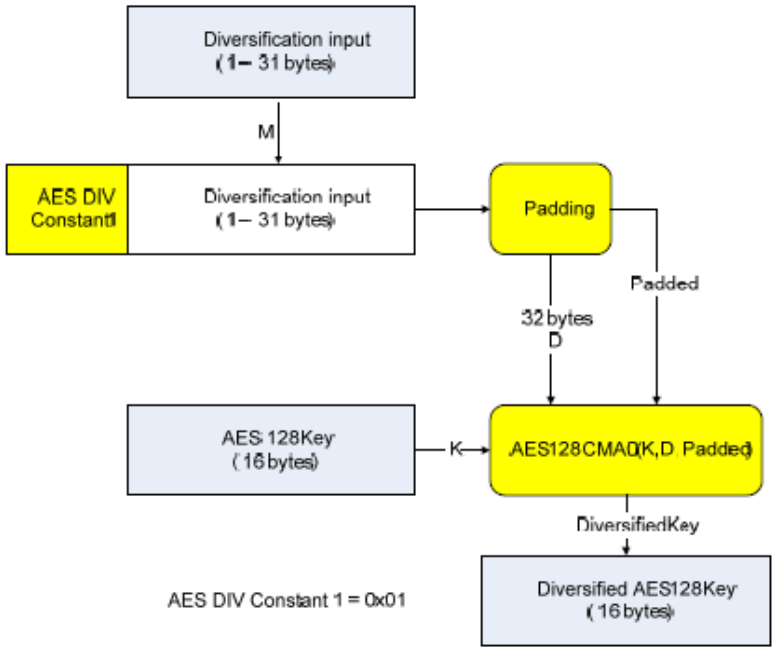
Cette fonction permet d'utiliser une clé différente de celle connue par l'utilisateur. Pour cela, l'encodeur utilise l'algorithme de diversification en fonction de l'encadré « *Crypto* » des paramètres DESFire, afin de pouvoir générer une autre clé.

- Si l'algorithme en cours est le *3DES,* la clé générée sera fonction d'une clé de chiffrement *3DES* de 16 octets définie dans le champ « *Clé de diversification 3DES* ». Il est nécessaire que les 8 premiers octets de celle-ci soit différents des 8 derniers.
- Si l'algorithme en cours est *l'AES*, la clé générée sera fonction de la clé utilisateur ainsi que d'autres paramètres. Dans ce cas, le champ « *Clé de diversification 3DES* » est grisé.

- ☑ CMK permet de diversifier la Card Master Key, c'est-à-dire la Clé Maître Carte.

Afin de désactiver la diversification des clés appliquée sur la *Card Master Key*, il est nécessaire de décocher l'option "*CMK*" et de formater la puce via la case "*Formate la carte*". De plus un changement de clés est nécessaire.

- ☐ NXP clé diversifiée selon la méthode NXP-AN-165310.
- ☑ NXP clé diversifiée selon la méthode NXP-AN10922.

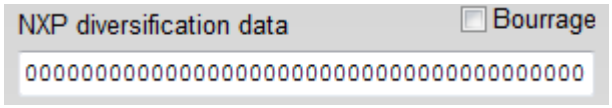


Le « diversification input » correspond à : UID I AID I KeyNum.

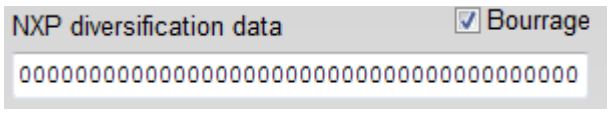
- Pour être compatible avec les différentes interprétations des recommandations de NXP, deux paramètres sont laissés accessibles à l'utilisateur : le sens de l'AID et le padding/data.

: permet d'inverser l'AID (LSB / MSB) avant le calcul de la clé diversifiée.

Ex.: AID = FB C5 10 ou AID = 10 C5 FB.

- 

Avec la case Bourrage non cochée la valeur du champ sera considérée en tant qu'entrée de diversification et le calcul de la diversification sera effectué selon CMAC K1*.

- 

Avec la case Bourrage cochée, la valeur du champ sera considérée en tant que Padding et le calcul de la diversification sera effectué selon CMAC K2*.

* Note pour les sous clés K1 et K2 : se référer à la RFC4493

> **Subkey Generation Algorithm**
>
> The subkey generation algorithm, Generate_Subkey(), takes a secret key, K, which is just the key for AES-128.
>
> The outputs of the subkey generation algorithm are two subkeys, K1 and K2. We write (K1,K2) := Generate_Subkey(K).
>
> Subkeys K1 and K2 are used in both MAC generation and MAC verification algorithms. K1 is used for the case where the length of the last block is equal to the block length. K2 is used for the case where the length of the last block is less than the block length.

Remarque : afin de s'authentifier avec la carte CIMS (Carte d'identité Multi-Services du gouvernement français), utiliser AID inversé coché et padding à 0x 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00.

Note :

* Pour que la diversification soit effective, il est nécessaire de cocher également les cases « *Nouvelle* » des clés à diversifier et de renseigner la valeur de la clé.

* Il est possible d'utiliser l'option de diversification des clés en utilisant l'option « Random ID ». En revanche, la Clé Maître Carte ne sera pas diversifiée.

- 

diversification spécifique Gemalto MD3811 (1 I UID I Padding & Card UID Len=4)

Clés Fichier1 / Clés Fichier2

Permet de paramétrer le numéro de clé et la valeur de la clé des fichiers de données.
Attention, la clé numéro 0 correspond à la Clé Maître Application.

Si utilisation d'une seule clé par fichier la partie « Clé d'écriture » est grisée.

Pour modifier une valeur de clé, dans le champ « Actuelle » renseigner la clé actuelle puis cocher la case « Nouvelle » et remplir le champ avec la valeur de la clé voulue.

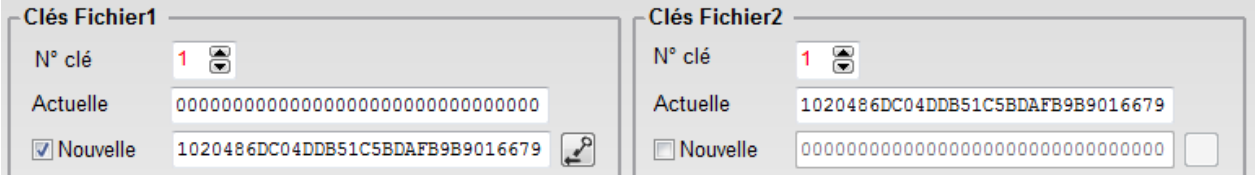
Par défaut, les valeurs de clé sont 0x 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00.

Note :

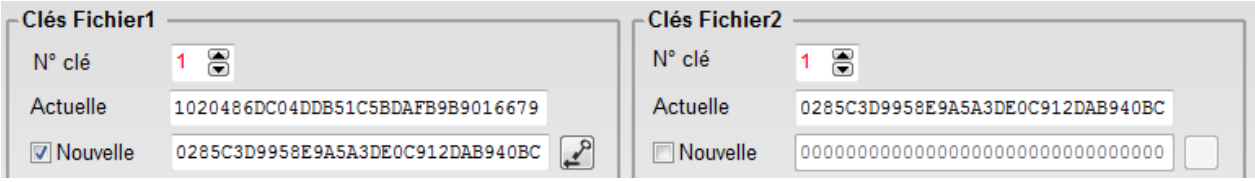
A partir de la version 3.0.0 de SECard, il n'est plus nécessaire de réinscrire la clé Nouvelle dans le champ Actuelle pour ré-encoder le badge.

- **Cas particulier** : il est possible d'utiliser la même clé pour les fichiers 1 et 2.

Dans ce cas les champs clés doivent être renseignés comme ci-dessous :



Et pour effectuer un changement de clé, renseigner les champs clés comme ci-dessous :



- **Free Read**

Pour relire un fichier encodé en Free Read utiliser la clé de lecture numéro 14.

Cette clé est une clé particulière de la DESFire qui ne nécessite pas d'authentification.

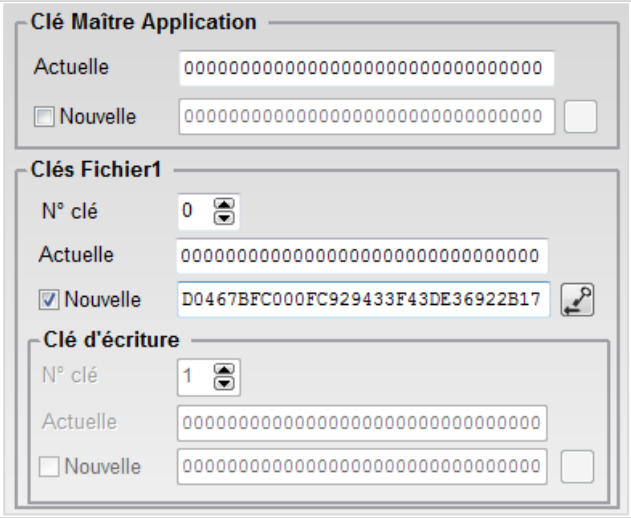
- **Utilisation d'une seule clé pour gérer la sécurité de l'application et du fichier**

A partir de la version 3.0.0 de SECard, il est possible d'utiliser la Clé Maître Application (n°0) pour gérer la sécurité de l'application **et** du fichier 1. Le fichier 2 ne doit pas être activé.

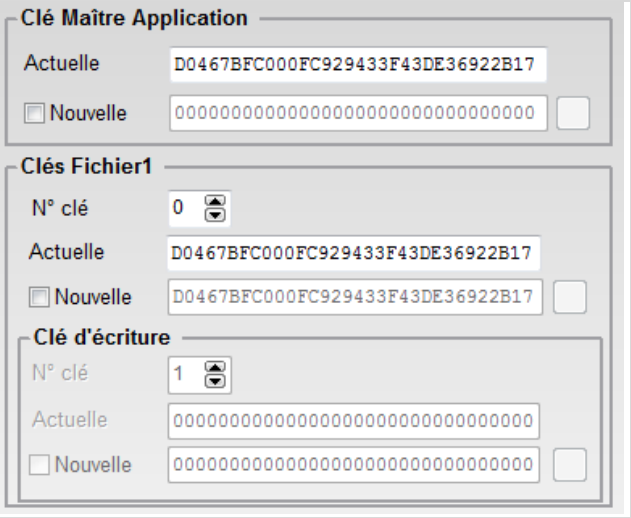
Dans ce cas le changement de la valeur de la clé numéro 0 s'effectue dans le champ de la clé de lecture/écriture du fichier 1.

Cas d'une seule clé (RW) :

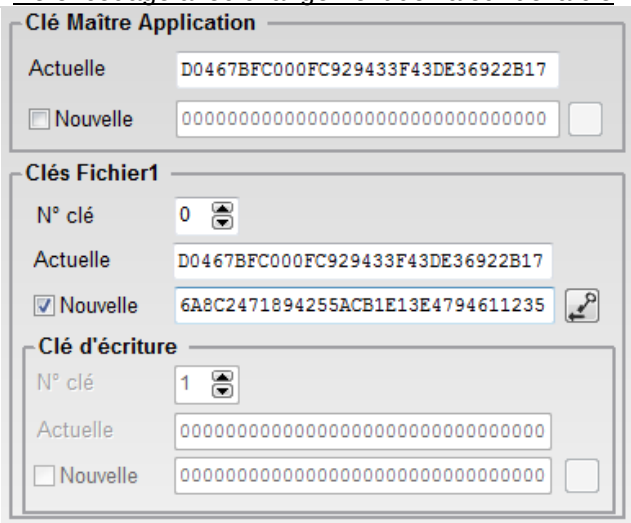
Premier encodage sur badge vierge



Ré encodage sans changement de valeur de la clé

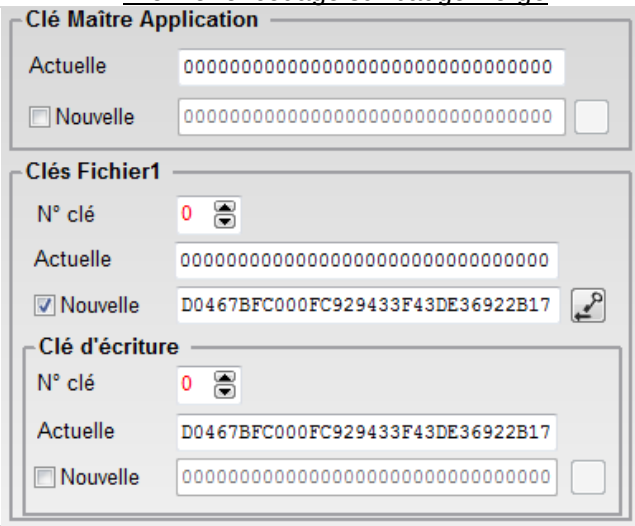


Ré encodage avec changement de valeur de la clé

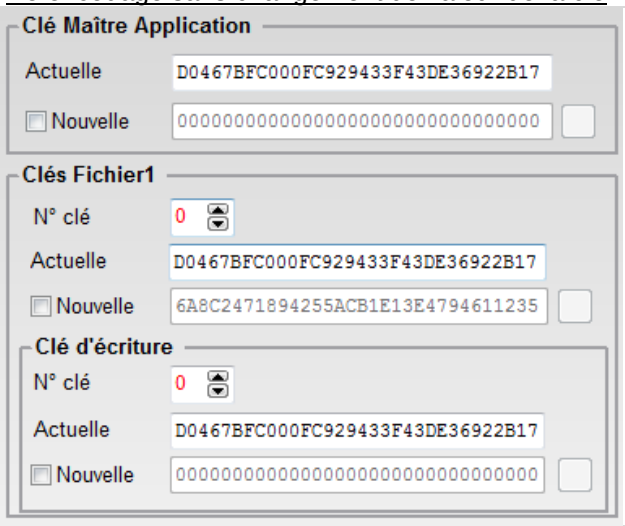


Cas de deux clés :

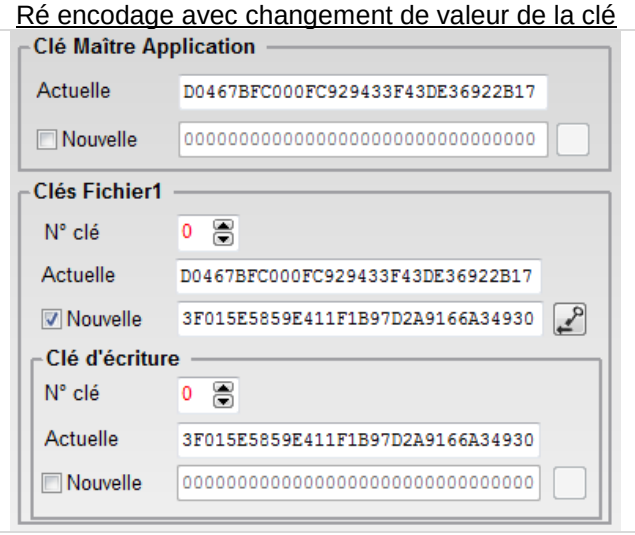
Premier encodage sur badge vierge



Ré encodage sans changement de valeur de la clé



Ré encodage avec changement de valeur de la clé



Clés DESFire de sécurité des données biométriques

Permet de paramétrer le numéro de clé et la valeur de la clé du fichier biométrique.

Si utilisation d'une seule clé par fichier la partie « Clé d'écriture » est grisée.

Pour modifier une valeur de clé, dans le champ « Actuelle » renseigner la clé actuelle puis cocher la case « Nouvelle » et remplir le champ avec la valeur de la clé voulue.

Par défaut, les valeurs de clé sont 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00.

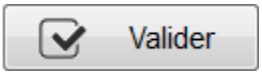
Clé utilisée pour GetUID d'une carte diversifiée et RandomID

Dans le cas d'une puce DESFire® en RandomID et diversifiée, il est nécessaire de s'authentifier pour récupérer l'UID.

Par défaut la clé utilisée pour l'authentification est la clé maître carte (CMK), si elle n'est pas connue il faut définir et utiliser une autre clé connue pour s'authentifier et récupérer ainsi l'UID.

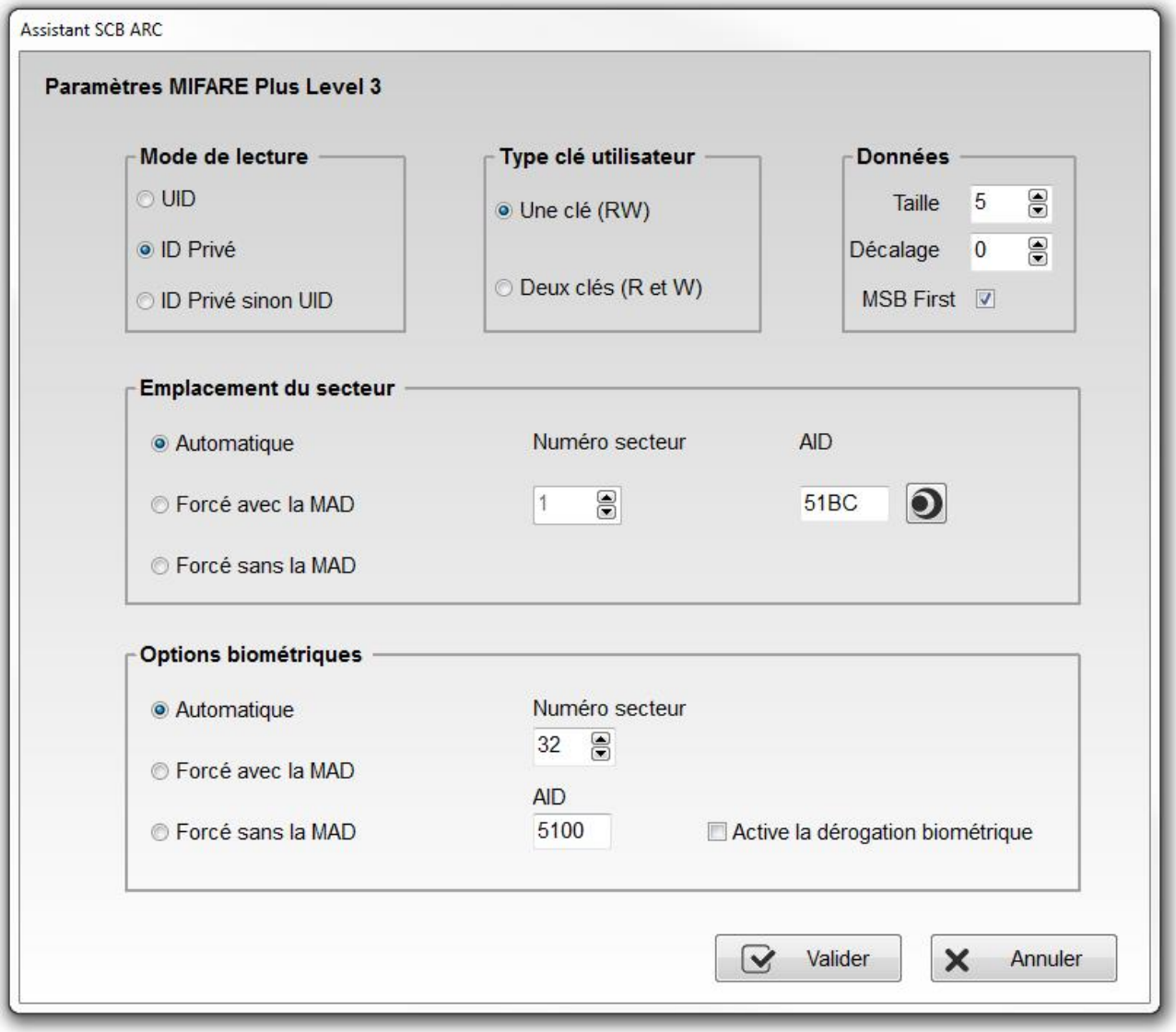
Cette nouvelle clé est utilisée pour l'encodage uniquement si RandomID est activée ET que l'utilisateur saisie une nouvelle valeur pour cette clé. Dans le cas inverse c'est la CMK qui sera toujours utilisée.

Attention implique toujours que la carte passe/soit passée en RandomID.

Cliquer sur le bouton 

pour terminer la configuration des clés DESFire® EV1.

III. 9 - MIFARE Plus® SL3 : paramètres



Mode de lecture

- ❖ UID : Lecteur configuré uniquement en lecture de numéro de série.
- ❖ ID Privé : Lecteur configuré uniquement en lecture de code privé.
- ❖ ID Privé sinon UID : Lecteur configuré en lecture de code privé. Si celui-ci n'est pas trouvé ou si les paramètres de sécurité sont incorrects, alors le lecteur lira l'UID.

Type clé utilisateur

- ❖ Une clé (RW) : Utilisation d'une seule clé par secteur servant pour la lecture et l'écriture.
- ❖ Deux clés (R et W) : Utilisation de deux clés par secteur. Une clé servant pour la lecture, la seconde pour la lecture et l'écriture.

Données

- ❖ Taille : Détermine la longueur de l'ID lu dans le secteur. La valeur correspond au protocole choisi lors de la configuration du lecteur. Cependant, il est possible de choisir une taille différente en entrant une autre valeur. Dans ce cas, le lecteur lira l'ID à la taille définie dans ce champ et le restituera au format défini par le protocole.
- ❖ Décalage : Permet de décaler le numéro privé à encoder/lire par rapport à l'octet « 0 ».
- ❖ MSB First : Si la case est cochée, le lecteur lira l'identifiant Most Significant Byte First.
  Si la case est décochée, le lecteur lira l'identifiant Least Significant Byte First.

Emplacement du secteur

Permet de définir le secteur dans lequel les données seront encodées et/ou lues par le lecteur.

La MAD (*MIFARE® Application Directory*) est une table des matières qui a pour but de référencer les applications (informations) écrites dans les secteurs des badges utilisateurs par l'intermédiaire d'un *AID* (*Application IDentifier*).
Ce dernier est complètement personnalisable et se décompose en deux parties : le c*luster code* et l'*application code*.

La puce MIFARE Plus® 2ko dispose de 32 secteurs (0 à 31). Celle-ci est utilisable en MAD1 (secteur 0 gérant les secteurs 1 à 15) et MAD2 (secteur 16 gérant 17 à 31).

La puce MIFARE Plus® 4ko dispose de 40 secteurs (0 à 39). Celle-ci est utilisable en MAD1 (secteur 0 gérant les secteurs 1 à 15) et MAD2 (secteur 16 gérant les secteurs 17 à 39). Seuls les 31 premiers secteurs sont gérés par SECard pour un identifiant.

La MAD est protégée par une clé de lecture (Clé A) et une clé d'écriture (Clé B). Par défaut, celles-ci sont positionnées à :

- ✓ « A0 A1 A2 A3 A4 A5 A6 A7 A0 A1 A2 A3 A4 A5 A6 A7 » pour la clé A
- ✓ « FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF » pour la clé B

Ces valeurs de clés sont celles préconisées par la note d'application *NXP* permettant à tous les utilisateurs d'accéder à la MAD.

Grâce à ce dispositif, MAD et AID, un lecteur peut retrouver un code personnel dans des badges qui ont été programmés différemment avec les données personnelles à des endroits différents.

- ❖ Automatique + AID :
  Dans ce mode, l'utilisateur n'a pas à se préoccuper de l'emplacement des données.
  Le « SCB » et les badges utilisateurs sont créés avec les paramètres suivants :
  - Le premier secteur disponible dans le badge utilisateur est choisi par SECard via le scan de la MAD.
  - L'AID inscrit dans le champ « AID » est communiqué au lecteur par l'intermédiaire du « *SCB* ».
  - La MAD du badge utilisateur est programmée avec l'AID à l'emplacement correspondant au premier secteur disponible en utilisant les valeurs par défaut des clés :
    - Clé A de lecture « A0 A1 A2 A3 A4 A5 A6 A7 A0 A1 A2 A3 A4 A5 A6 A7 » non modifiable.
    - Clé B d'écriture « FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF » modifiable.
  - Le lecteur identifie le secteur à lire du badge utilisateur par la recherche de l'AID dans la MAD.

- ❖ Forcé avec MAD + Numéro secteur + AID :
  Dans ce mode, le logiciel forcera l'encodage du badge utilisateur au secteur défini dans le champ « Numéro secteur » ainsi qu'avec l'AID inscrit dans le champ « AID ». Le lecteur configuré par le « SCB » lira les informations en fonction de ces paramètres.

- ❖ Forcé sans la MAD +Numéro secteur :
  Dans ce mode, aucune gestion de la MAD n'est effectuée. Seul le paramètre « Numéro secteur » est pris en compte pour définir l'emplacement des données dans la puce. Le lecteur configuré par le « SCB » lira les informations dans ce secteur.

Note : l'AID *51BC* affiché par défaut dans le champ « *AID* » est la valeur de *l'Application IDentifier* STid.

Options biométriques

Les empreintes à encoder seront inscrites dans les secteurs 32 à 39 de la puces MIFARE Plus® Level 3. Automatique, Forcé avec la MAD et Forcé sans la MAD même principe que ci-dessus.

Dans le cas de l'utilisation de la MAD avec AID, la valeur de l'AID doit être différente de celle utilisée pour l'ID privé.

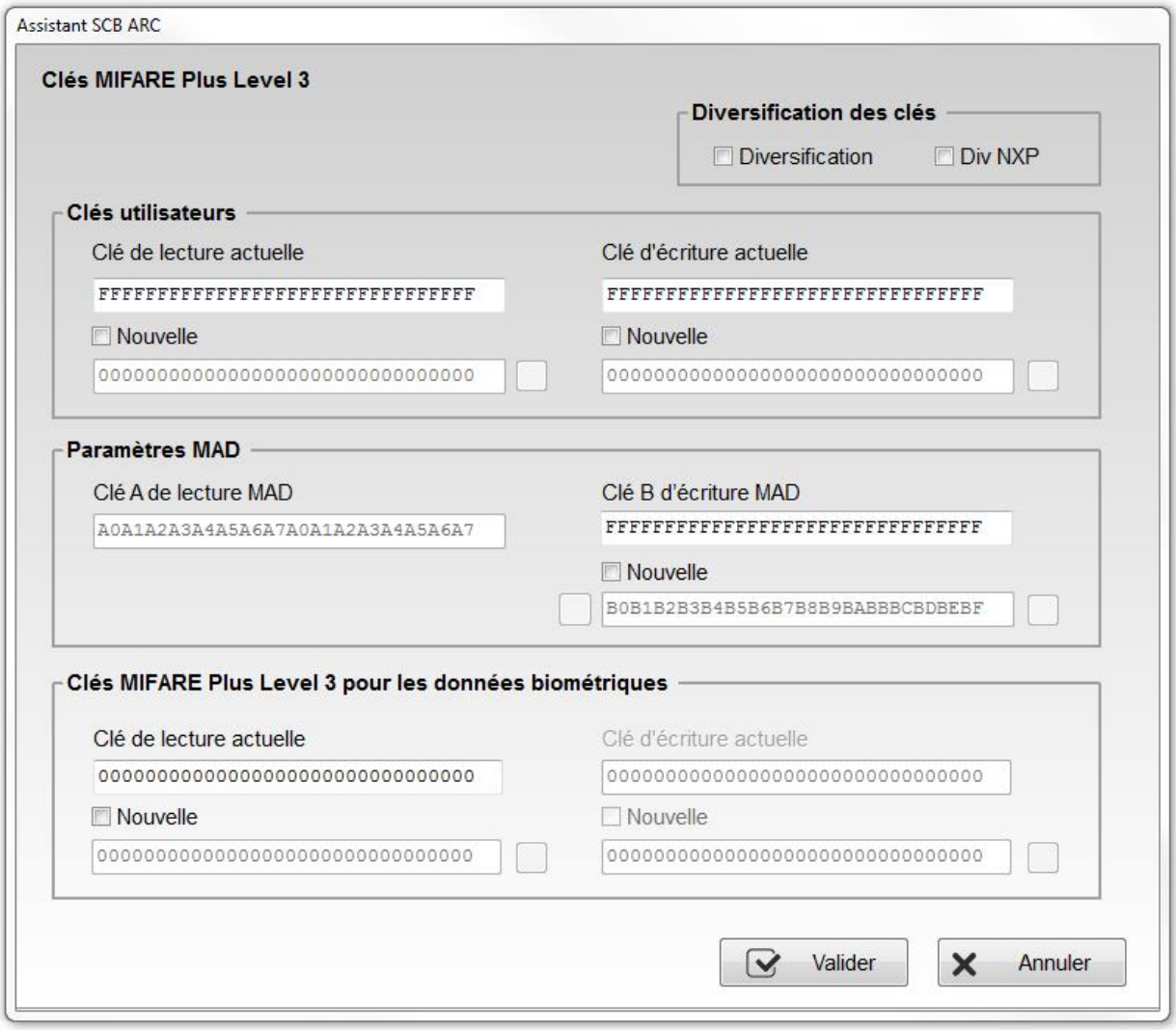
Note : l'encodage de la biométrie n'est réalisable que sur des puces MIFARE Plus® Level 3 de 4KO de mémoire.

- Active la dérogation biométrique. Se reporter au paragraphe *T7.2 - Dérogation biométrique*

Cliquer sur le bouton 

pour terminer la configuration des paramètres MIFARE Plus® Level 3.

III. 10 - MIFARE Plus® SL3 : clés



Diversification des clés

- Permet d'activer la diversification des clés. Cette fonction permet d'utiliser une clé différente de celle connue par l'utilisateur, pour cela l'encodeur utilise l'algorithme AES afin de pouvoir générer une autre clé. Pour que la diversification soit effective, il est nécessaire de cocher les cases « *Nouvelle* » des clés à diversifier et de renseigner la valeur de la clé.

- La case « Div NXP » indique que la diversification sera effectuée selon la préconisation NXP, c'est-à-dire avec un bourrage de 0 permettant d'arriver à une longueur de 32 octets. Si cette option n'est pas cochée, la longueur sera de 16 octets.

Clés utilisateurs

Clés protégeant le secteur contenant l'ID privé.
Permet de renseigner la valeur des clés actuelles et de les modifier.

Remarque : A partir de la version 3.0.0 de SECard lors d'un ré-encodage, il n'est plus nécessaire de passer la valeur du champ Nouvelle au champ Actuel

Paramètres MAD

Cet encadré n'est disponible que si l'emplacement du secteur a été paramétré en mode « Automatique » ou « Forcé avec la MAD ».

La Clé A de lecture MAD est forcée automatiquement à la valeur « A0 A1 A2 A3 A4 A5 A6 A7 A0 A1 A2 A3 A4 A5 A6 A7».

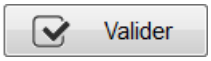
La clé B d'écriture MAD est par défaut FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF, il est possible de la changer en remplissant le champ Nouvelle clé B MAD.

Lors d'une gestion de MAD, les clés des secteurs « 0 » et « « 16 » changent. Les conditions d'accès sont :

- Une clé de lecture Clé A ayant pour valeur « A0 A1 A2 A3 A4 A5 A6 A7 A0 A1 A2 A3 A4 A5 A6 A7».
- Une clé d'écriture Clé B ayant pour valeur « FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF »

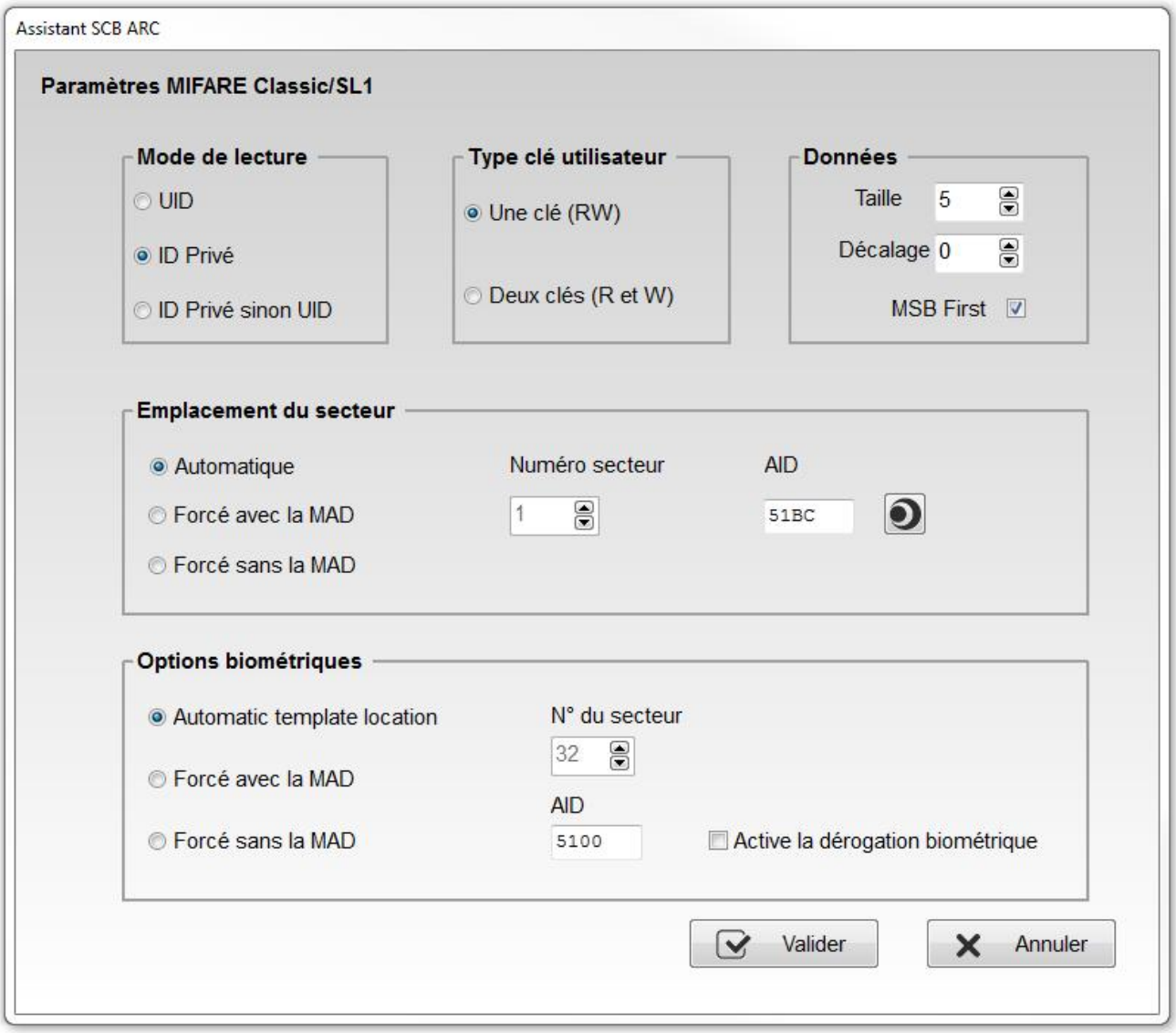
Clés MIFARE Plus® Level 3 pour les données biométriques

Clés protégeant le secteur contenant les informations biométriques.
Permet de renseigner la valeur des clés actuelles et le les modifier.

Cliquer sur le bouton 

pour terminer la configuration des clés MIFARE Plus® Level 3.

III. 11 - MIFARE® Classic/SL1 : paramètres



Mode de lecture

- ❖ UID : Lecteur configuré uniquement en lecture de numéro de série.
- ❖ ID Privé : Lecteur configuré uniquement en lecture de code privé.
- ❖ ID Privé sinon UID : Lecteur configuré en lecture de code privé. Si celui-ci n'est pas trouvé ou si les paramètres de sécurité sont incorrects, alors le lecteur lira l'UID.

Type clé utilisateur

- ❖ Une clé (RW) : Utilisation d'une seule clé par secteur servant pour la lecture et l'écriture.
- ❖ Deux clés (R et W) : Utilisation de deux clés par secteur. Une clé servant pour la lecture, la seconde pour la lecture et l'écriture.

Données

- ❖ Taille : Détermine la longueur de l'ID lu dans le secteur. La valeur correspond au protocole choisi lors de la configuration du lecteur. Cependant, il est possible de choisir une taille différente en entrant une autre valeur. Dans ce cas le lecteur lira l'ID à la taille définie dans ce champ et le restituera au format défini par le protocole.
- ❖ Décalage : Permet de décaler le numéro privé à encoder/lire par rapport à l'octet « 0 ».
- ❖ MSB First : Si la case est cochée, le lecteur lira l'identifiant Most Significant Byte First. Si la case est décochée, le lecteur lira l'identifiant Least Significant Byte First.

Emplacement du secteur

Permet de définir le secteur dans lequel les données seront encodées et/ou lues par le lecteur.

La MAD (*MIFARE® Application Directory*) est une table des matières qui a pour but de référencer les applications (informations) écrites dans les secteurs des badges utilisateurs par l'intermédiaire d'un *AID* (*Application IDentifier*). Cf AN103787.
Ce dernier est complètement personnalisable et se décompose en deux parties : le c*luster code* et l'*application code*.

La puce MIFARE® Classic 1ko utilisable en MAD1 dispose de 16 secteurs (secteur 0 à 15). Les secteurs 1 à 15 sont disponibles pour les données, le secteur 0 étant occupé par la MAD.

La puce MIFARE Plus® 2ko dispose de 32 secteurs (0 à 31). Celle-ci est utilisable en MAD1 (secteur 0 gérant les secteurs 1 à 15) et MAD2 (secteur 16 gérant 17 à 31).

La puce MIFARE® Classic 4ko / MIFARE Plus® 4ko dispose de 40 secteurs (0 à 39). Celle-ci est utilisable en MAD1 (secteur 0 gérant les secteurs 1 à 15) et MAD2 (secteur 16 gérant les secteurs 17 à 39). Seuls les 31 premiers secteurs sont gérés par SECard.

La MAD est protégée par une clé de lecture (Clé A) et une clé d'écriture (Clé B). Par défaut, celles-ci sont positionnées à :

- ✓ « A0 A1 A2 A3 A4 A5 » pour la clé A
- ✓ « FF FF FF FF FF FF » pour la clé B

Ces valeurs de clés sont celles préconisées par la note d'application *NXP* permettant à tous les utilisateurs d'accéder à la MAD.

Grâce à ce dispositif, MAD et AID, un lecteur peut retrouver un code personnel dans des badges qui ont été programmés différemment avec les données personnelles à des endroits différents.

- ❖ Automatique + AID :
  Dans ce mode, l'utilisateur n'a pas à se préoccuper de l'emplacement des données.
  Le « SCB » et les badges utilisateurs sont créés avec les paramètres suivants :
  - Le premier secteur disponible dans le badge utilisateur est choisi par SECard via le scan de la MAD.
  - L'AID inscrit dans le champ « AID » est communiqué au lecteur par l'intermédiaire du « *SCB* ».
  - La MAD du badge utilisateur est programmée avec l'AID à l'emplacement correspondant au premier secteur disponible en utilisant les valeurs par défaut des clés :
    - Clé A de lecture « A0 A1 A2 A3 A4 A5 », modifiable.
    - Clé B d'écriture « FF FF FF FF FF FF », modifiable.
  - Le lecteur identifie le secteur à lire du badge utilisateur par la recherche de l'AID dans la MAD.

- ❖ Forcé avec MAD + Numéro secteur + AID :
  Dans ce mode, le logiciel forcera l'encodage du badge utilisateur au secteur défini dans le champ « Numéro secteur » ainsi qu'avec l'AID inscrit dans le champ « AID ». Le lecteur configuré par le « SCB » lira les informations en fonction de ces paramètres.

- ❖ Forcé sans la MAD +Numéro secteur :
  Dans ce mode, aucune gestion de la MAD n'est effectuée. Seul le paramètre « Numéro secteur » est pris en compte pour définir l'emplacement des données dans la puce. Le lecteur configuré par le « SCB » lira les informations dans ce secteur.

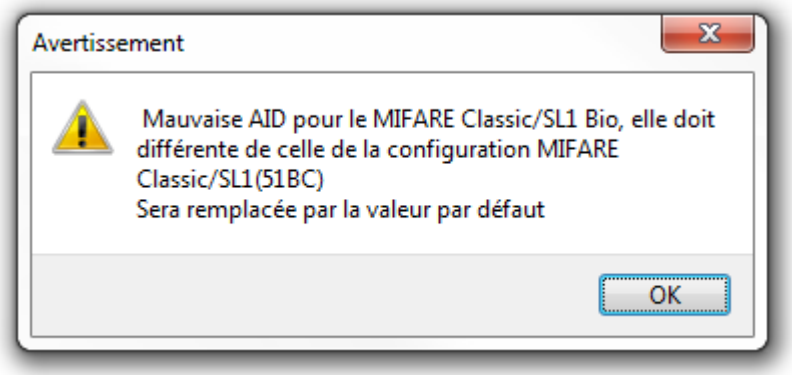
Note : L'AID *51BC* affiché par défaut dans le champ « *AID* » est la valeur de *l'Application IDentifier* STid.

Options biométriques

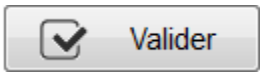
Uniquement disponible pour des puces MIFARE® Classic 4ko.

Définir le secteur (>=32) dans lequel seront encodées les données biométriques.

Si la MAD est utilisée, elle doit être différente de la MAD utilisée pour les données.

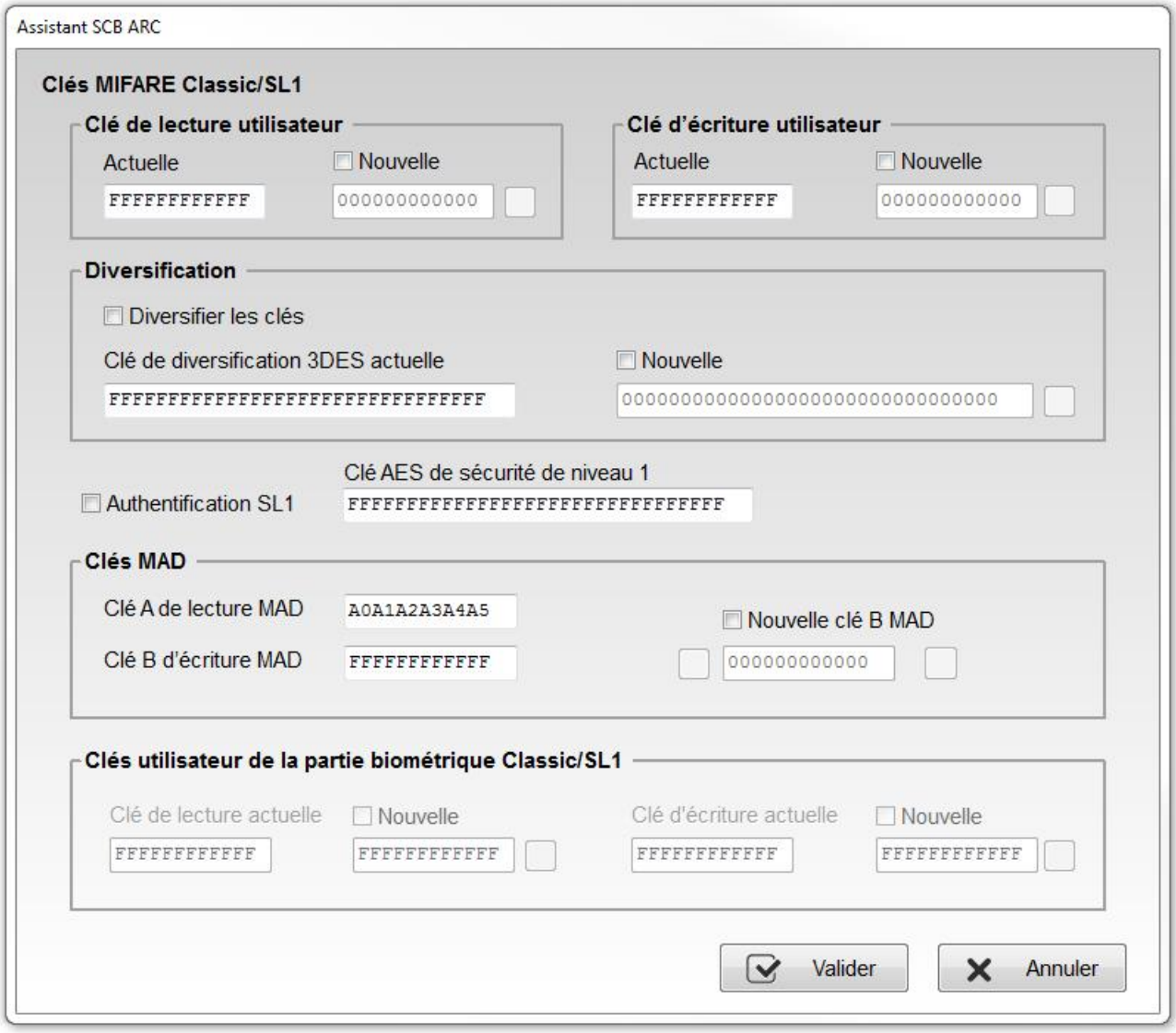


- Active la dérogation biométrique. Se reporter au paragraphe *T7.2 - Dérogation biométrique*

Cliquer sur le bouton 

pour terminer la configuration des paramètres MIFARE® Classic/SL1.

III. 12 - MIFARE® Classic /SL1 : clés



Clé de lecture utilisateur / Clé d'écriture utilisateur

Clés protégeant le secteur contenant l'ID privé.
Permet de renseigner la valeur des clés actuelles et de les modifier.

Note : Les clés par défaut pour un badge vierge sont soit à « FF FF FF FF FF FF » soit à « A0 A1 A2 A3 A4 A5 » selon l'origine fournisseur du badge.

Diversification

- Permet d'activer la diversification des clés. Cette fonction permet d'utiliser une clé différente de celle connue par l'utilisateur. Pour cela, l'encodeur utilise l'algorithme de diversification afin de pouvoir générer une autre clé qui sera fonction du numéro de bloc, du numéro de série, de la clé utilisateur et d'une clé de chiffrement 3DES de 16 octets. Pour que la diversification soit effective, il est nécessaire de cocher les cases « *Nouvelle* » des clés à diversifier et de renseigner la valeur de la clé.

Note : il est possible de ne plus utiliser l'option de diversification des clés. Pour cela, il faut recréer le « *SCB* » en décochant la case « *Diversification* » et en indiquant dans le premier champ la valeur de la clé de chiffrement *3DES*. Il sera nécessaire par la suite d'encoder le badge utilisateur à nouveau sans cette option.

Authentification SL1

Permet d'activer l'authentification *AES* pour les puces MIFARE Plus® Level 1. Celle-ci permet de sécuriser l'authentification puce/lecteur par un algorithme de chiffrement.

Disponible uniquement en mode « *ID Privé* » et « *ID Privé ou UID* » (l'UID sera remonté dans ce mode si le lecteur n'arrive pas à s'authentifier)

Attention

Cette clé est importante et doit absolument être connue de l'Administrateur.
Une puce MIFARE Plus® Level 1ayant une autre valeur de clé *AES* ne pourra s'authentifier avec le lecteur.

Si cette option est utilisée, le lecteur ne pourra plus lire de code privé de MIFARE® Classic

Pour désactiver cette option, il est nécessaire de récréer / reconfigurer le badge « *SCB* » en décochant l'option « *Authentification SL1* »

Il est nécessaire de décocher la case « *Type carte auto* » et de cocher le mode « *Classic/Plus L1* » pour un encodage d'une puce MIFARE® Classic possédant un numéro de série sur 7 octets.

Clés MAD

Cet encadré n'est disponible que si l'emplacement du secteur a été paramétré en mode « Automatique » ou « Forcé avec la MAD ».

La Clé A de lecture MAD est par défaut à la valeur « A0 A1 A2 A3 A4 A5 ». Il est possible d'utiliser une autre valeur en la modifiant dans le champ.
La clé B d'écriture MAD est par défaut à la valeur FF FF FF FF FF FF, il est possible de la changer en remplissant le champ « Nouvelle clé B MAD ».

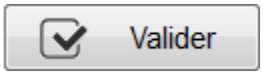
Lors d'une gestion de MAD, les clés des secteurs « 0 » et «16 » changent. Les conditions d'accès sont :

- Une clé de lecture Clé A ayant pour valeur « A0 A1 A2 A3 A4 A5 ».
- Une clé d'écriture Clé B ayant pour valeur par défaut « FF FF FF FF FF FF »

ATTENTION,
Depuis le document de NXP AN-10787 Rev07 7 July 2010, la CléA de la MAD est fixée à A0A1A2A3A4A5A6A7. La cléB reste inchangée (FF…FF par défaut).

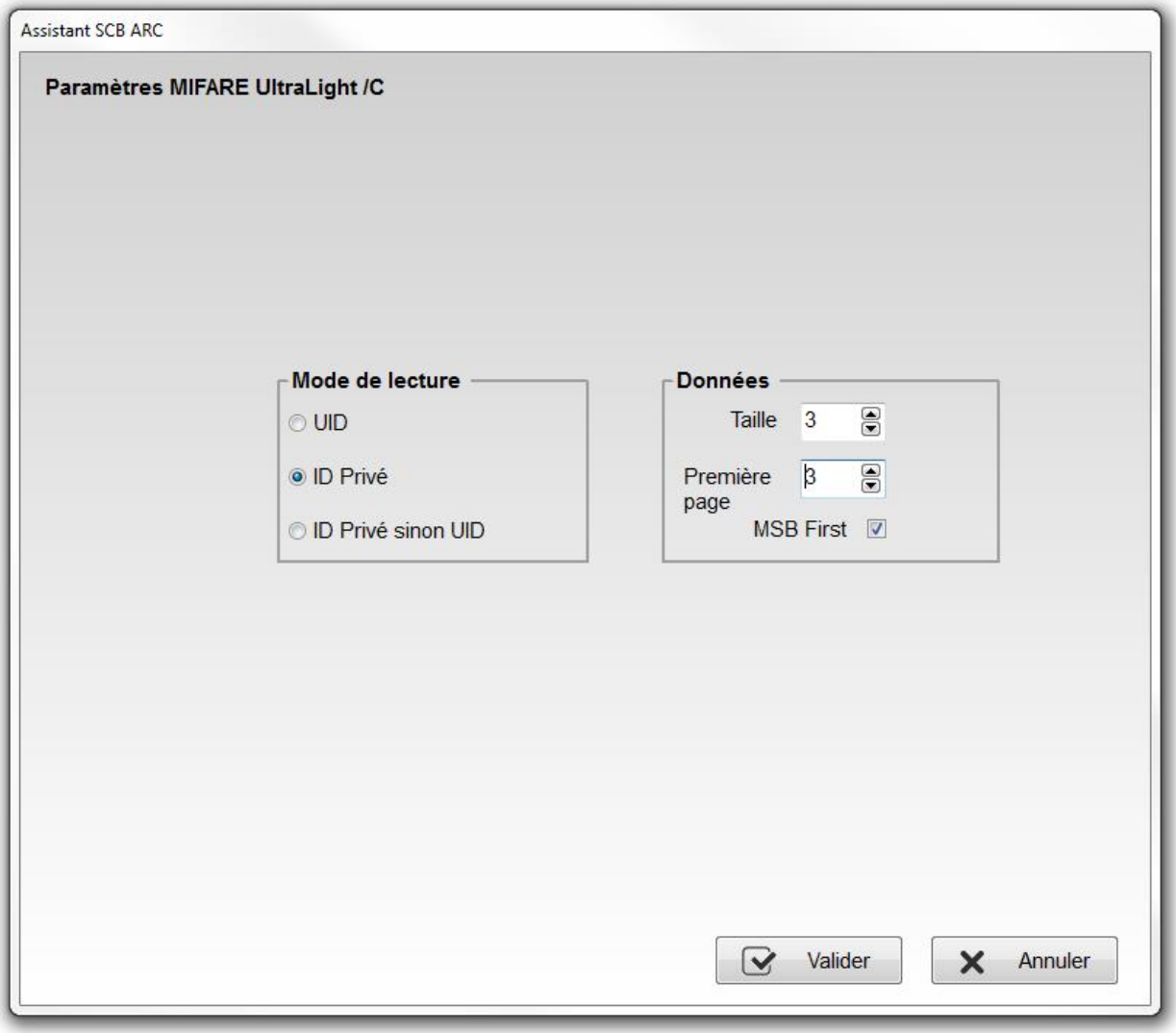
Clé utilisateur de protection des données biométriques

Clé protégeant le secteur contenant les données biométriques.

Cliquer sur le bouton 

pour terminer la configuration des clés MIFARE® Classic/SL1.

III. 13 - MIFARE Ultralight® C : paramètres



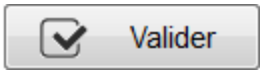
Mode de lecture

- ❖ UID : Lecteur configuré uniquement en lecture de numéro de série.
- ❖ ID Privé : Lecteur configuré uniquement en lecture de code privé.
- ❖ ID Privé sinon UID : Lecteur configuré en lecture de code privé. Si celui-ci n'est pas trouvé ou si les paramètres de sécurité sont incorrects, alors le lecteur lira l'UID.

Données

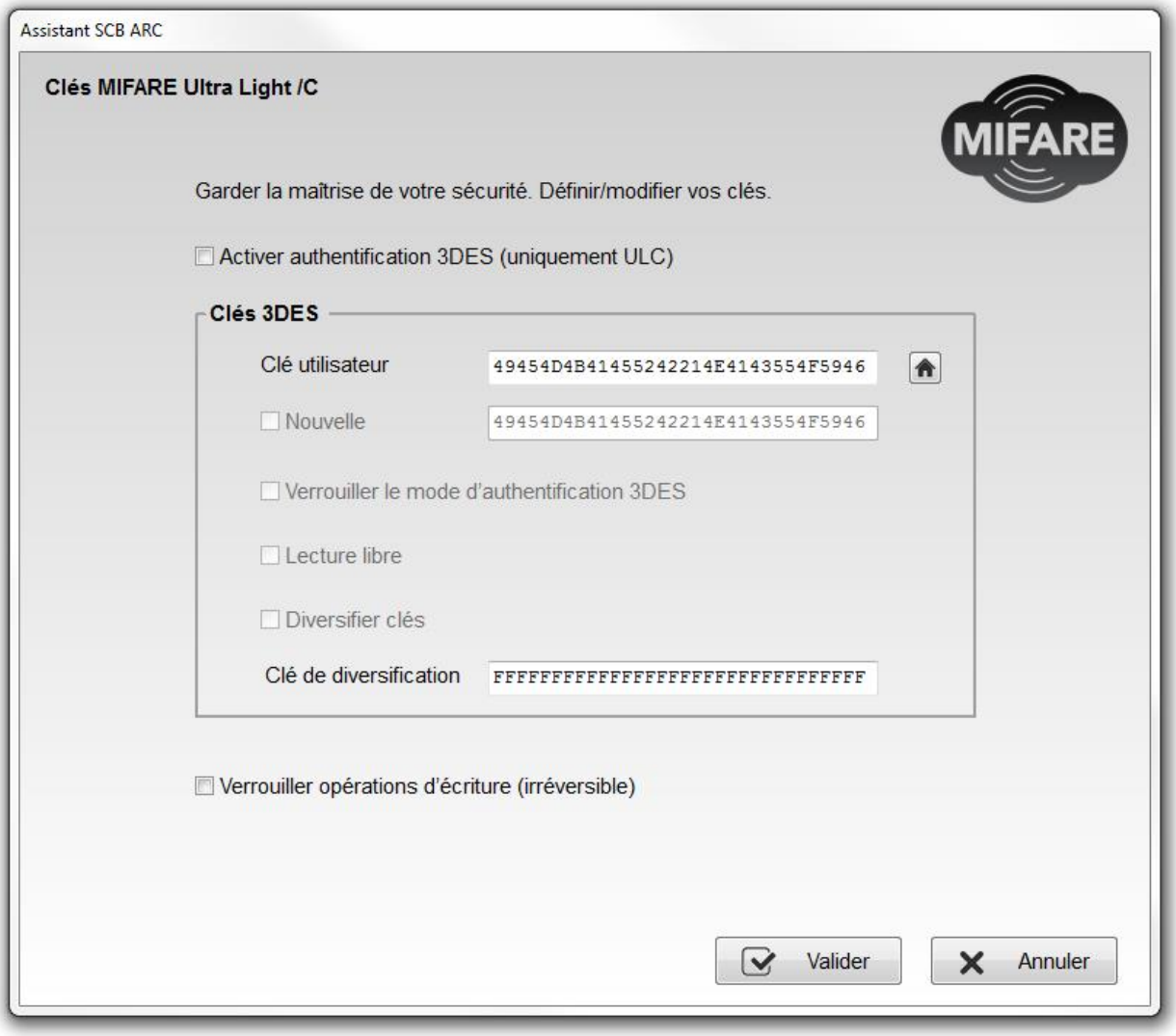
- ❖ Taille : Détermine la longueur de l'ID lu. La valeur correspond au protocole choisi lors de la configuration du lecteur. Cependant il est possible de choisir une taille différente en entrant une autre valeur, dans ce cas le lecteur lira l'ID à la taille définie dans ce champ et le restituera au format défini par le protocole.
- ❖ Décalage : Permet de déterminer la première page dans laquelle va être lu/encodé le code privé.
- ❖ MSB First : Si la case est cochée, le lecteur lira l'identifiant Most Significant Byte First.
  Si la case est décochée, le lecteur lira l'identifiant Least Significant Byte First

A partir de SECARD V3.0.0 la première page accessible devient la page 3. **Attention il s'agit d'une page OTP. Le ré-encodage n'est pas possible dans ce cas-là.**

Cliquer sur le bouton 

pour terminer la configuration des paramètres MIFARE Ultralight®/C.

III. 14 - MIFARE Ultralight® C : Clés



Activer authentification 3DES (uniquement ULC)

Permet d'activer/désactiver l'authentification 3DES entre la puce MIFARE Ultralight® C et le lecteur.

Clé utilisateur

Champs réservés aux valeurs de clés 3DES courantes et à modifier.
La valeur par défaut de la clé utilisateur est : *49454D4B41455242214E4143554F5946*

Verrouiller le mode d'authentification 3DES

Si cette case est cochée, il sera nécessaire de s'authentifier en mode *3DES* avec la puce MIFARE Ultralight® C (cette action est irréversible).

Lecture Libre

Si cette case est cochée et si la case « *Verrouiller le mode d'authentification 3DES* » est décochée, il ne sera pas nécessaire de s'authentifier en mode *3DES* avec la puce MIFARE Ultralight® C afin de lire les données encodées.

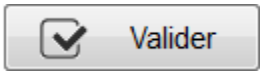
Diversifier clés

Permet d'activer la diversification des clés.

Cette fonction permet d'utiliser une clé différente de celle connue par l'utilisateur. Pour cela, l'encodeur utilise un algorithme de diversification afin de pouvoir générer une clé en fonction du numéro de série, de la clé utilisateur et d'une clé de chiffrement *3DES.*

Verrouiller opérations d'écriture (irréversible)

Permet d'interdire toutes les opérations d'écriture sur la puce. Celle-ci ne sera plus exploitable qu'en lecture. (Cette action est irréversible)

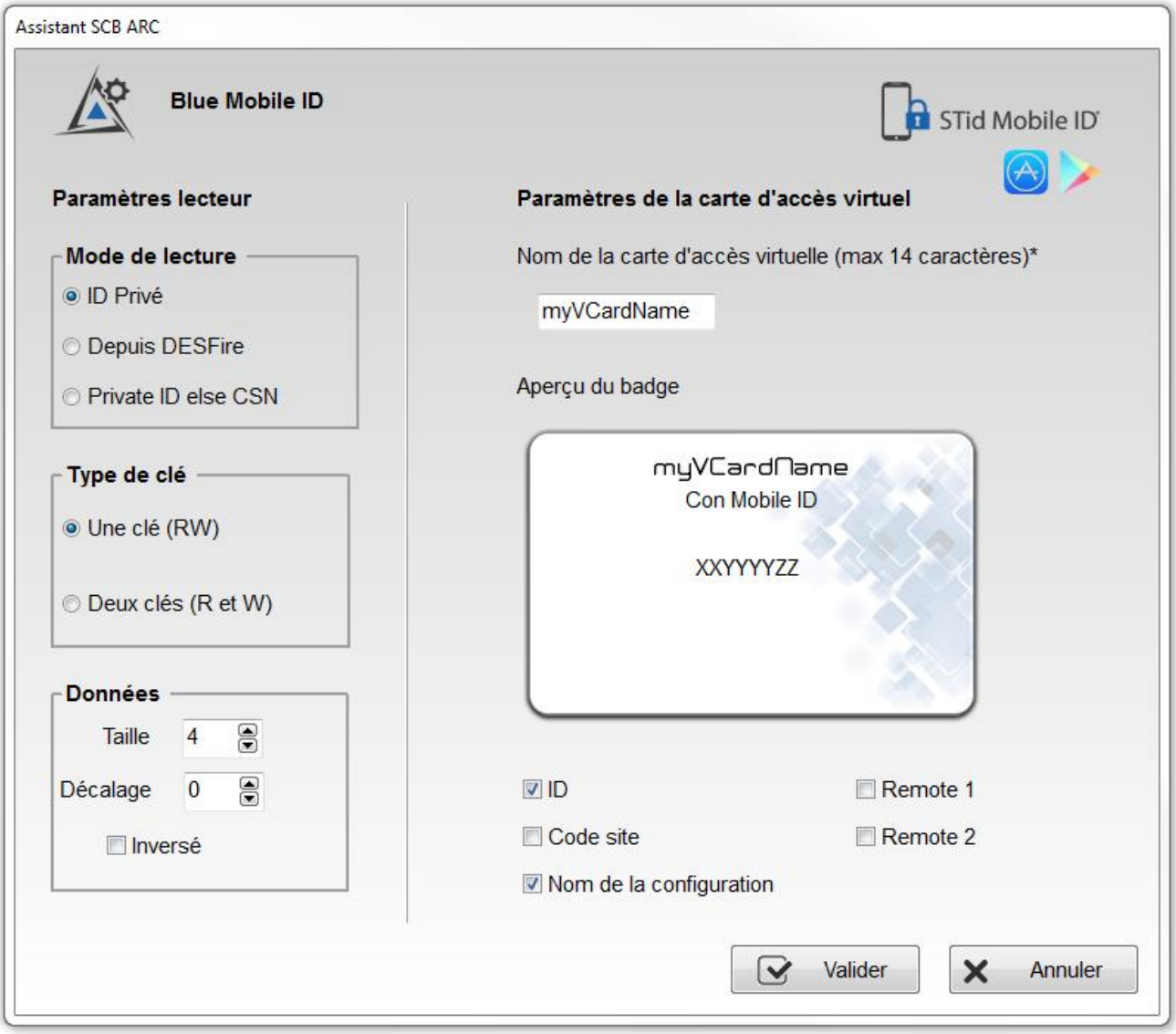
Cliquer sur le bouton 

pour terminer la configuration des clés MIFARE Ultralight®/C.

III. 15 - Blue Mobile ID : paramètres

III.15.1 - STid Mobile ID

❖ Mode de lecture : ID privé



Lecteur configuré en lecture de l'identifiant privé uniquement

Type de clé

- ❖ Une clé (RW) : Utilise une clé pour lire et écrire.
- ❖ Deux clés (R et W) : Utilise une clé pour lire et une clé pour lire/écrire.

Data

- ❖ 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 du badge d'accès virtuel

Personnalisation de l'affichage du badge virtuel.

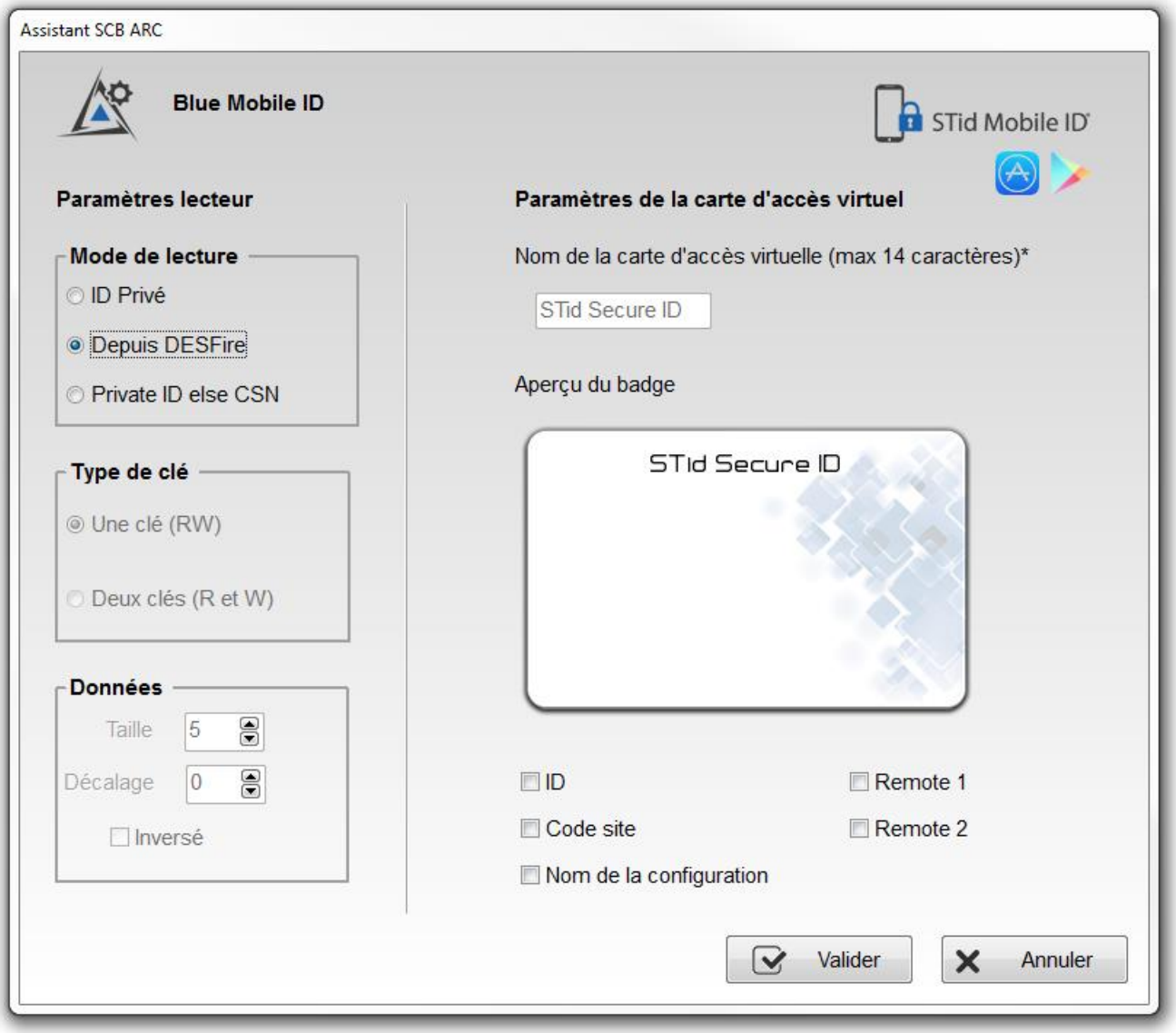
Nom de la carte d'accès : Nom qui apparaitra sur le badge virtuel à l'écran du smartphone.

Note : choisir un nom significatif permettant à l'utilisateur d'identifier rapidement le badge virtuel à utiliser.

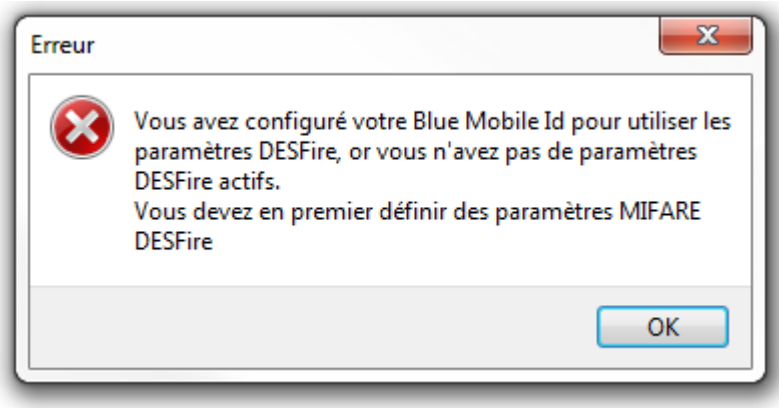
Image non-contractuelle

Exemples :

❖ **Mode de lecture : Depuis DESFire**



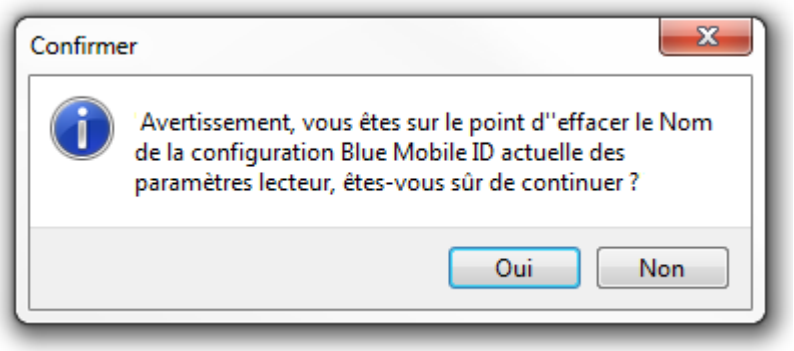
Si ce mode est activé une configuration DESFire doit être active sinon le message d'erreur suivant apparaitra :



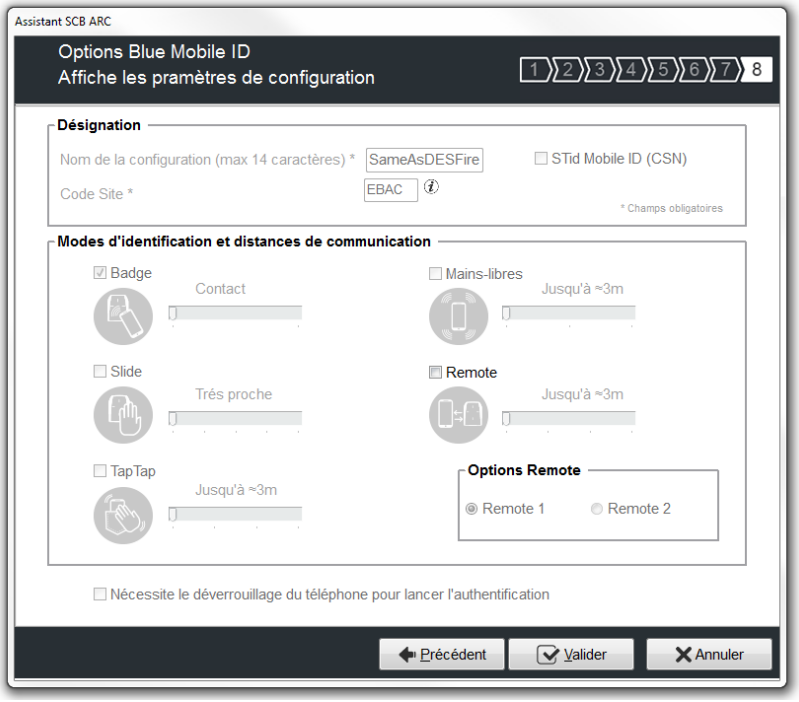
Dans ce mode, tous les paramètres BlueMobile ID sont automatiquement déterminés et hérités des paramètres définis pour la DESFire®.

- ✓ Inversé : MSB First
- ✓ Type de clé, taille et décalage hérités de la partie DESFire.

Attention



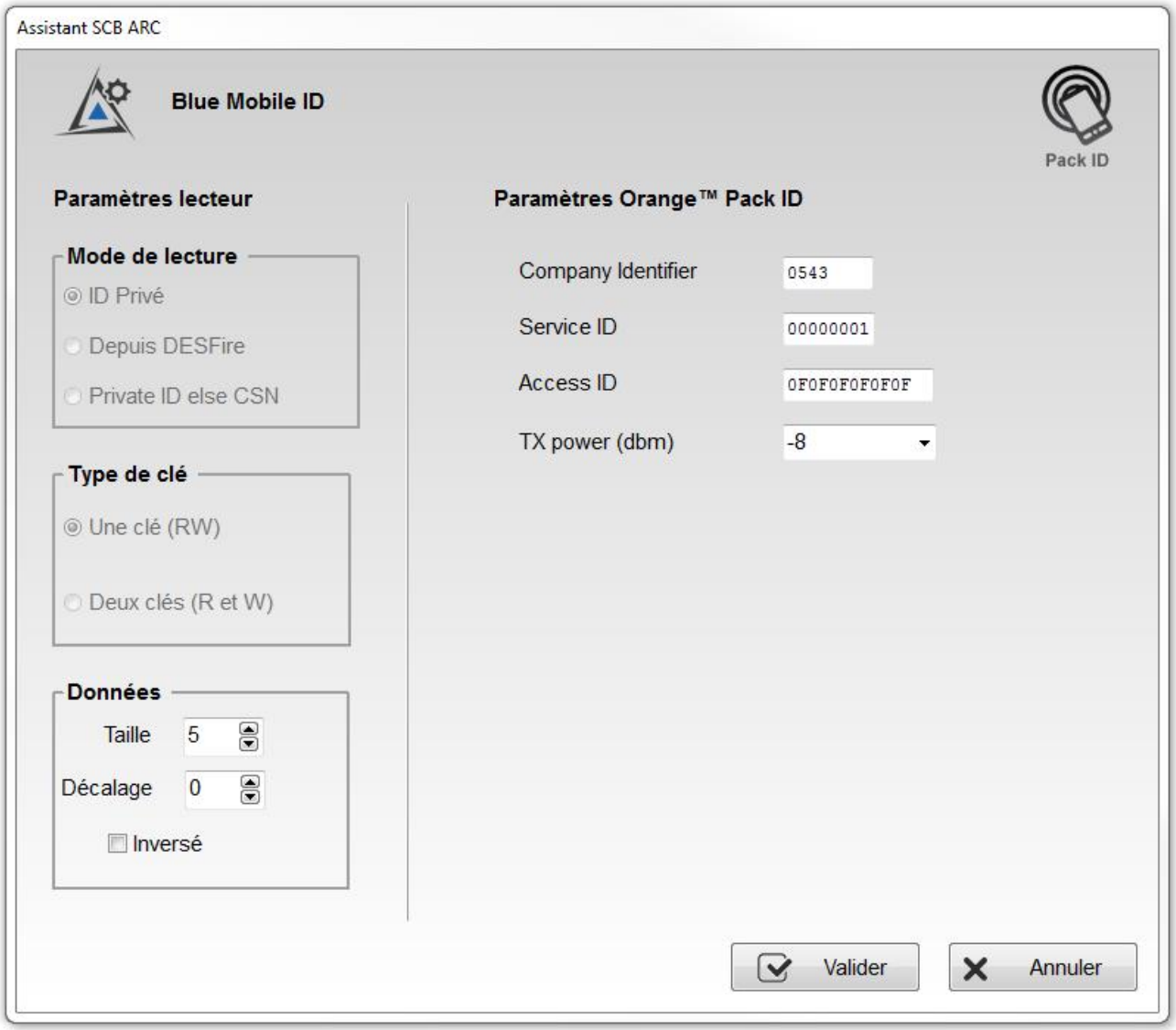
Remarque : les paramètres lecteurs sont donc modifiés et passe sur la configuration SameAsDESFire.



❖ **Mode de lecture : ID privé sinon UID**

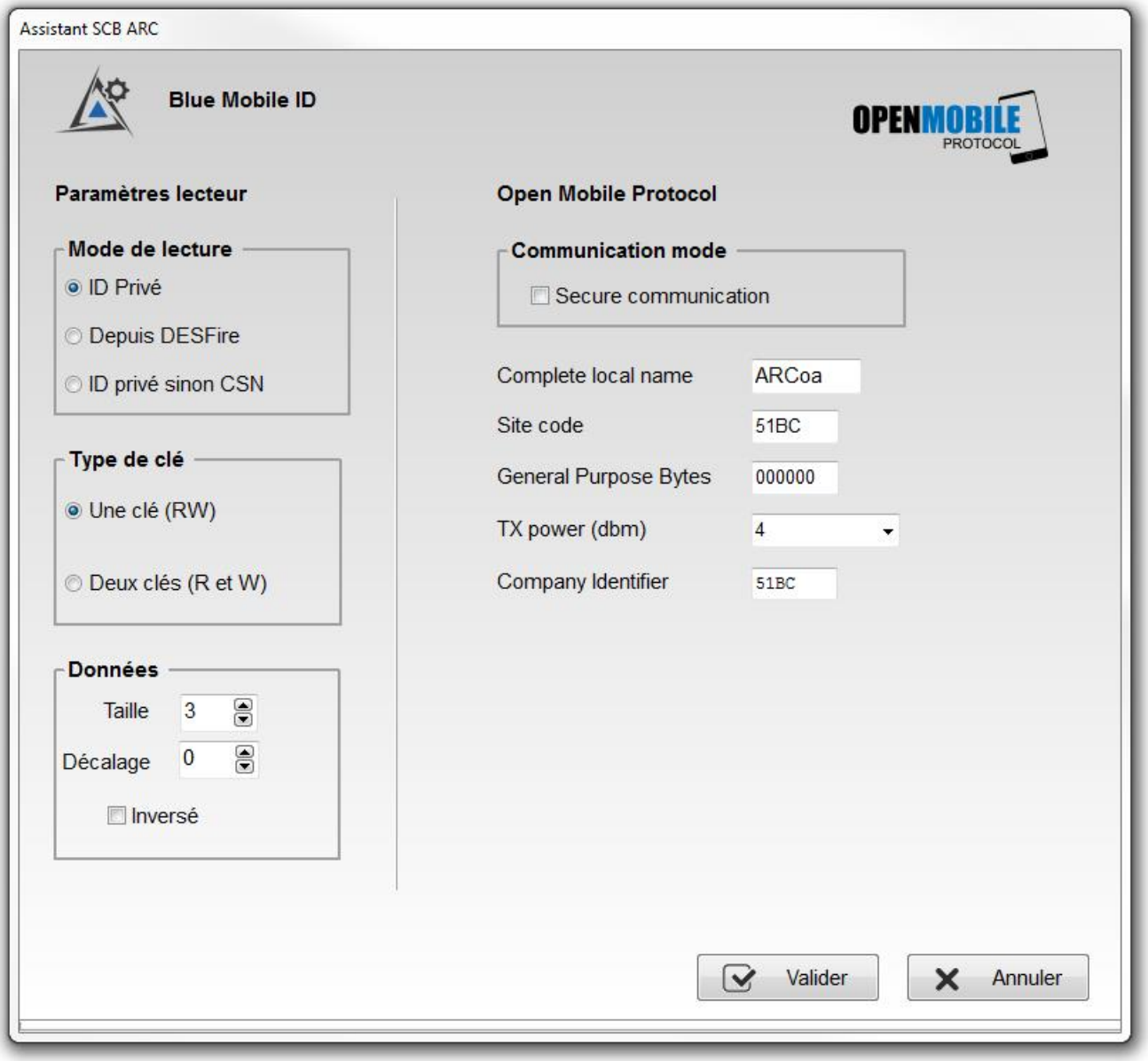
Le lecteur sera configuré en lecture de badge virtuel sécurisé. Si celui-ci n'est pas trouvé ou si les paramètres de sécurité sont incorrects, alors le lecteur lira et retournera le STid Mobile ID CSN.

III.15.2 - Orange Pack ID

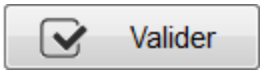


❖ Company Identifier : donnée constructeur sur 2 octets.
❖ Service ID : donnée constructeur sur 4 octets pour différencier les clients de Pack ID.
❖ Access ID : donnée constructeur sur 6 octets pour identifier la zone contrôlée par le lecteur.
❖ Tx power : Permet de changer le niveau de puissance du lecteur. (défault 4 dbm).
Valeurs possibles : -16, -12, -8, -4, 0 and 4 dbm.

III.15.3 - Open Mobile Protocol



Pour toutes informations sur le « Open Mobile Protocol » merci de contacter votre commercial STid.

Cliquer sur le bouton 

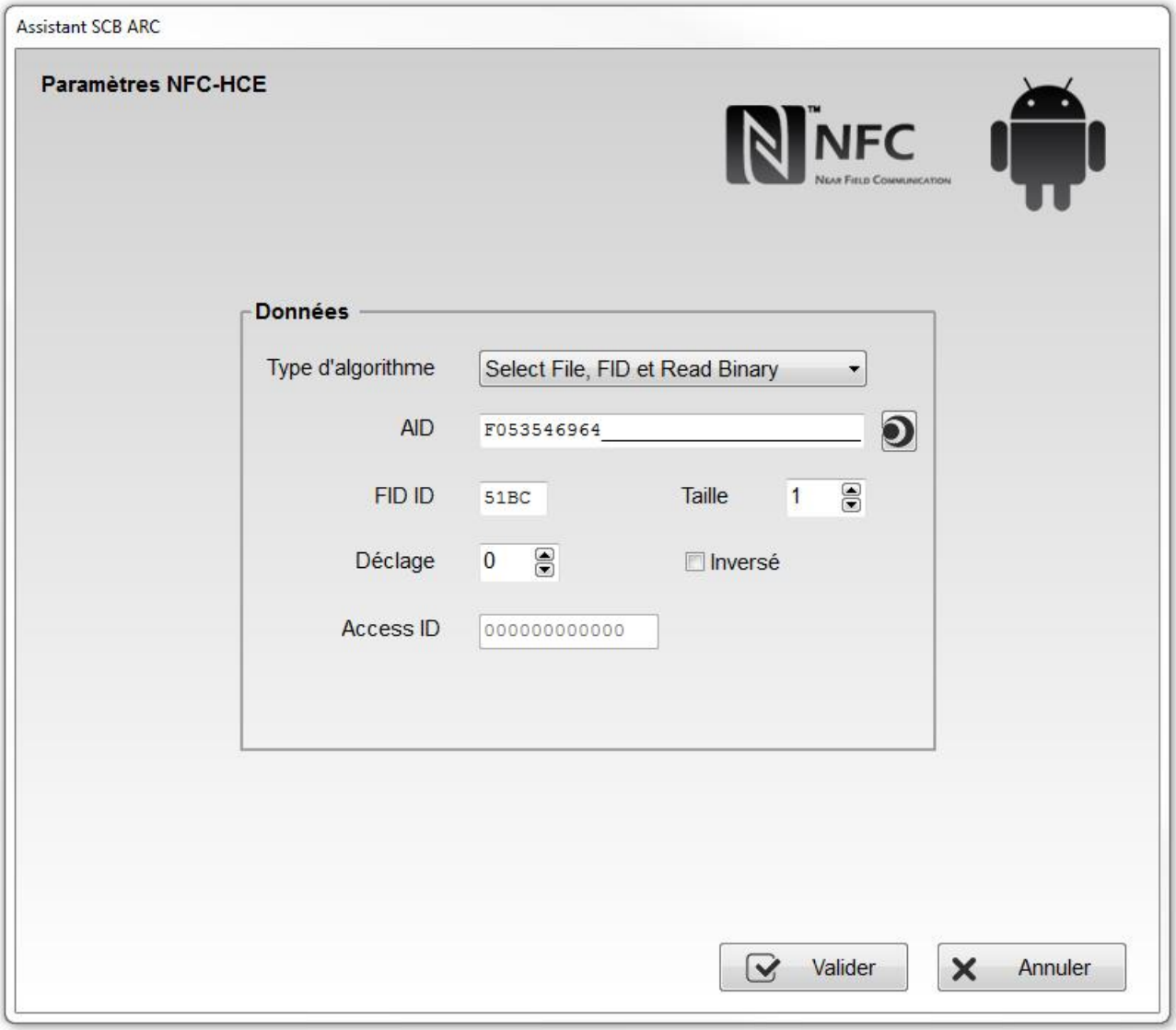
pour terminer la configuration

III. 16 - Blue Mobile ID : clés

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.

III. 17 - NFC-HCE : paramètres



Nécessite une APK (application mobile) et un smartphone Android qui supportent l'HCE (version OS ≥4.4.x).

Exemples de smartphones testés compatibles : Samsung S4, S5 & S6, LG G3, Nexus 6, Sony Xperia Z1 et Huawei P8 Lite.

Vous devez développer une APK selon un des deux algorithmes ou utiliser l'application Orange Pack ID.

Attention

Désactivé la lecture du PUPI dans l'assistant de configuration.

❖ **Type d'algorithme :** Select File, FID et Read Binary

Les échanges entre le lecteur RFID et le téléphone sont basés sur l'ISO07816. Le mode opératoire est "Select File AID + Select File FID ID + Read binary (size + offset)".

Les commandes à implémenter dans l'application sont :

- SELECT FILE 0xAID (DESFIRE ISO FILE) : un AID dont la taille est comprise entre 5 et maximum 16 octets.

  command APDU : 00A4040005AID

  response APDU : 9000

- SELECT FILE 0xFID ID (DESFIRE ISO FILE ID) : ID du fichier à lire sur 2 octets.

  command APDU : 00A4000002FIDID

  response APDU : 9000

- READ BINARY xx bytes

  command APDU : 00B000000Size

  response APDU : xxxxxxxxxx9000 avec xx = ID sur « size » octets

Paramètres SECard :

- **AID** — AID de 5 octets minimum et 16 octets maximum.
  Par défaut = 0xF053546964
- **FID ID** — ID du fichier à lire sur 2 octets. Par défaut = 0x51BC.
- **Size** — Nombre d'octets de l'ID (max 48octets) :
  - TTL Wiegand et Hexadécimal série : 1 à 48 octets
  - TTL Iso et Décimal Série : 1 à 10 octets
- **Décalage** — Position du premier octet de l'ID (0 à 48-Size). Par défaut = 0.
- **Inversé** — ☐ Inversé : ID envoyé non inversé (Default)
  ☑ Inversé : ID envoyé inversé

❖ **Type d'algorithme:** Select File seulement

La commande à implémenter dans l'application est :

- SELECT FILE 0xAID (DESFIRE ISO FILE):

command APDU : 00A40400**Size**$_{AID}$AID

Size$_{AID}$*: 1 octet (0x05 à 0x10)*

AID dont la taille est comprise entre 5 et maximum 16 octets

response APDU : ID9000

Paramètres SECard :

- ➢ **AID** AID de 5 octets minimum et 16 octets maximum
  Par défaut = 0xF053546964
- ➢ **Size** Nombre d'octets de l'ID (max 48octets) :
  - TTL Wiegand et Hexadécimal série : 1 à 48 octets
  - TTL Iso et Décimal Série : 1 à 10 octets
- ➢ **Inversé**
  ☐ Inversé ID envoyé non inversé (Default)
  ☑ Inversé ID envoyé inversé

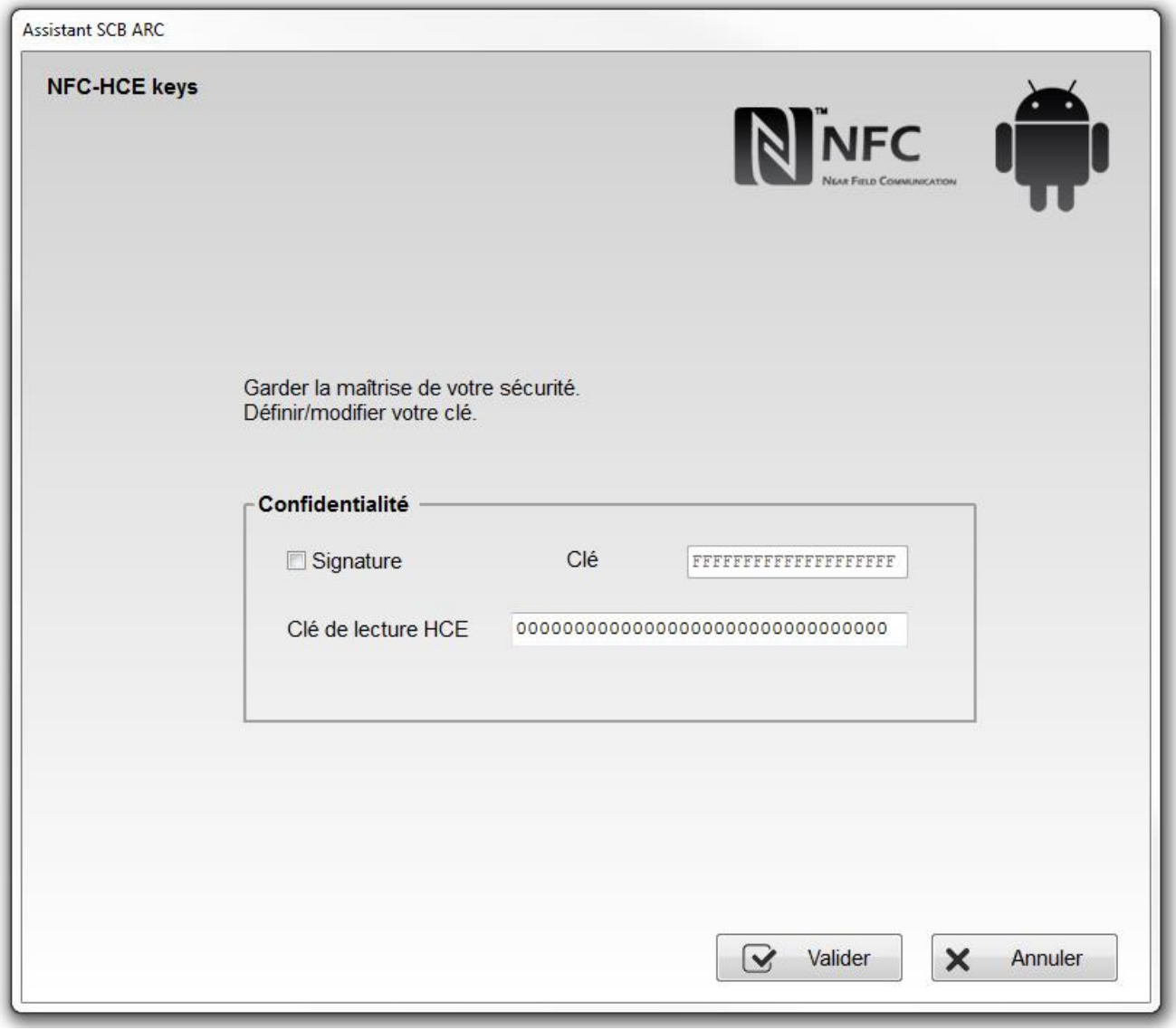
Remarque : le paramètre "Size" est utilisé pour vérifier la taille de l'ID reçu avec celle sélectionné dans SECard.

❖ **Type d'algorithme:** Orange PackID

Paramètres SECard :

- ➢ **AID** AID de 16 octets
- ➢ **Size** Nombre d'octets de l'ID (max 48octets) :
  - TTL Wiegand et Hexadécimal série : 1 à 48 octets
  - TTL Iso et Décimal Série : 1 à 10 octets
- ➢ **Inversé**
  ☐ Inversé ID envoyé non inversé (Default)
  ☑ Inversé ID envoyé inversé
- ➢ **Access ID** Valeur sur 6 octets identifiant la zone d'accès contrôlée par le lecteur.

III. 18 - NFC-HCE : Clés



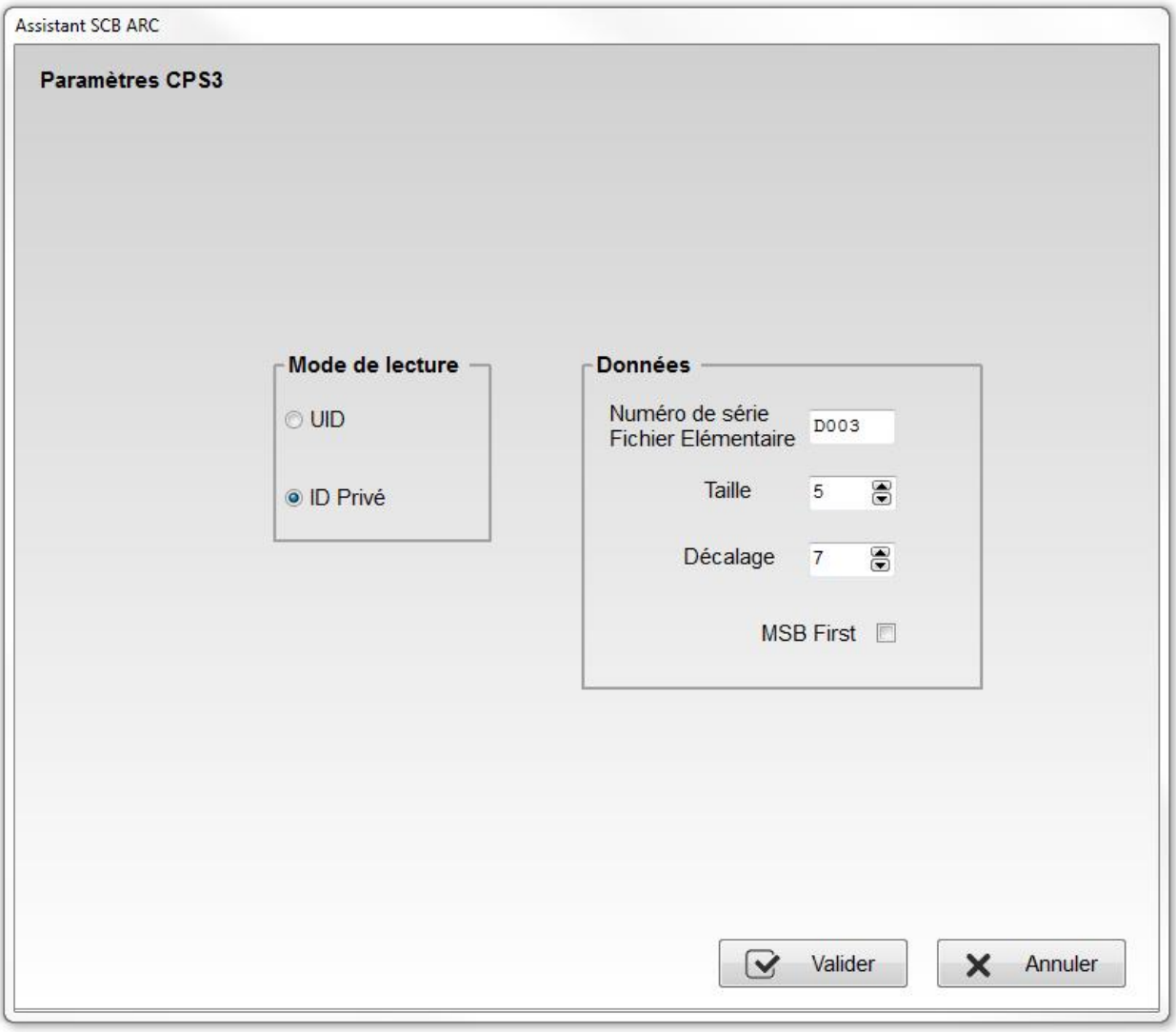
- **Signature**

  Signature l'ID HCE est envoyé en mode clair (défault)

  Signature une clé HMAC-SHA1 sur 10 octets est utilisée pour signer l'ID HCE.

- **Clé** — Permet de renseigner la clé utilisée pour le calcul de la signature sur 10 octets.
- **Clé de lecture HCE** — Uniquement disponible pour l'algortihme Orange Pack ID
  Clé secrète de la zone Access ID définie dans paramètres.

III. 19 - CPS3 : paramètres



Mode de lecture

- UID : Lecteur configuré uniquement en lecture de numéro de série
- ID Privé : Lecteur configuré uniquement en lecture de code privé

Dans le cas de la CPS3, l'UID correspond à l'Identifiant protocolaire, qui est le numéro de série de la puce.

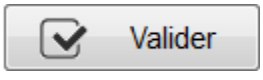
L'Id privé correspond à l'Identifiant Technique (N° de série IAS), c'est un numéro sur 19 digits constitué comme suit :

[Identifiant ASIP (10)][N°unique de la carte (8)][clé(1)]

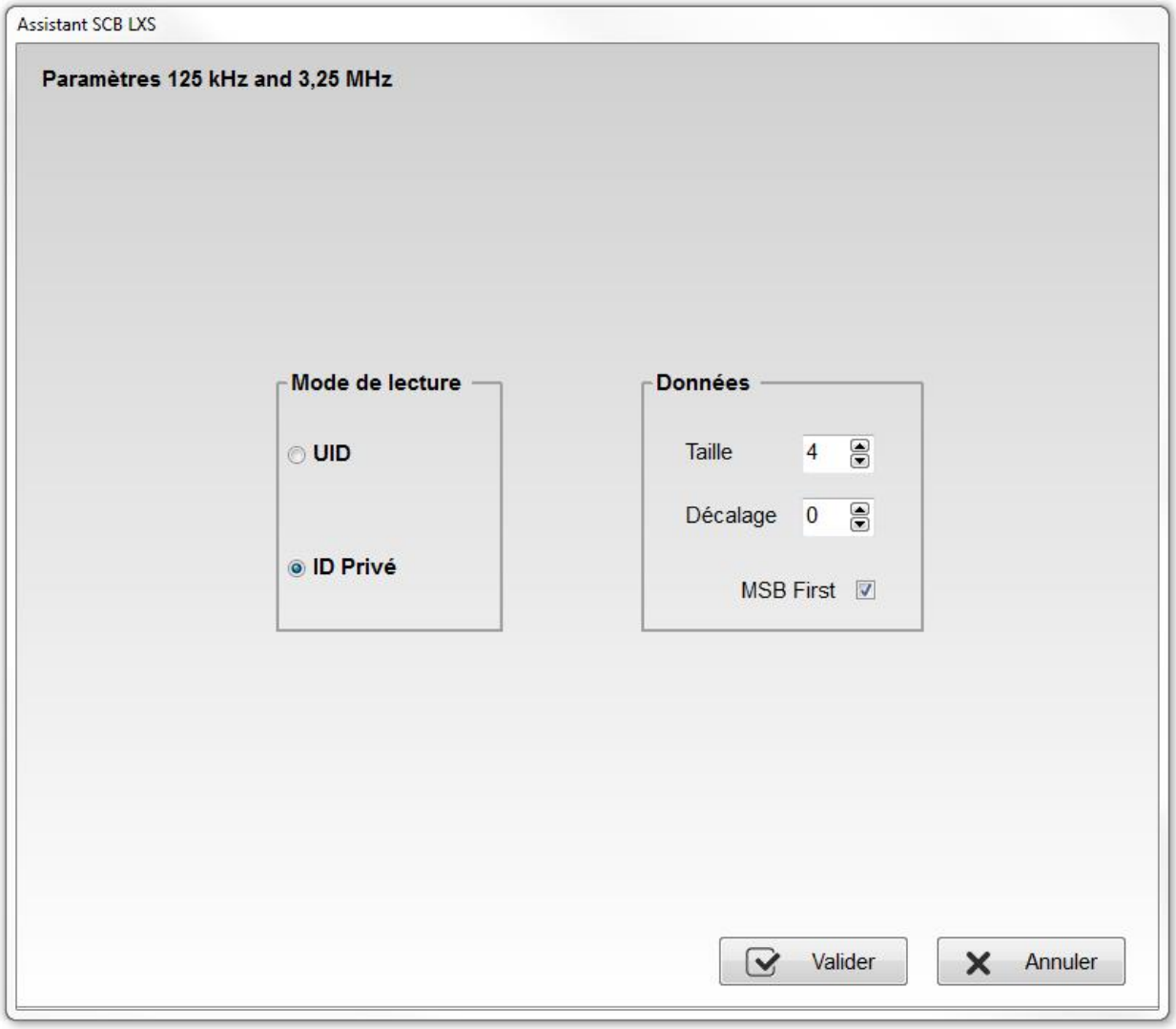
Sa valeur est présente dans le Fichier Elémentaire D003.

Afin de récupérer le code unique de la carte, il faut lire 5 octets de l'IAS avec un décalage de 7 octets pour ne pas lire l'Identifiant ASIP.

Pour lire cet ID, il n'y a pas d'authentification entre le lecteur et la puce.

Cliquer sur le bouton  **pour terminer la configuration des paramètres CPS3.**

III. 20 - 125kHz / 3.25MHz : paramètres



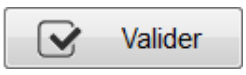
Le 3.25 Mhz n'est accessible qu'à partir du Wizard « Configuration gamme LXS ».
Permet de configurer les paramètres de lecture liés aux puces EM4102, EM4x50, HID, Nedap 125 kHz et 3.25 MHz.

Mode de lecture

- UID : Lecteur configuré uniquement en lecture du numéro de série.
- ID Privé : Lecteur configuré pour remonter l'identifiant avec une taille et un décalage possible. Permet de gérer le fonctionnement particulier du 2H.

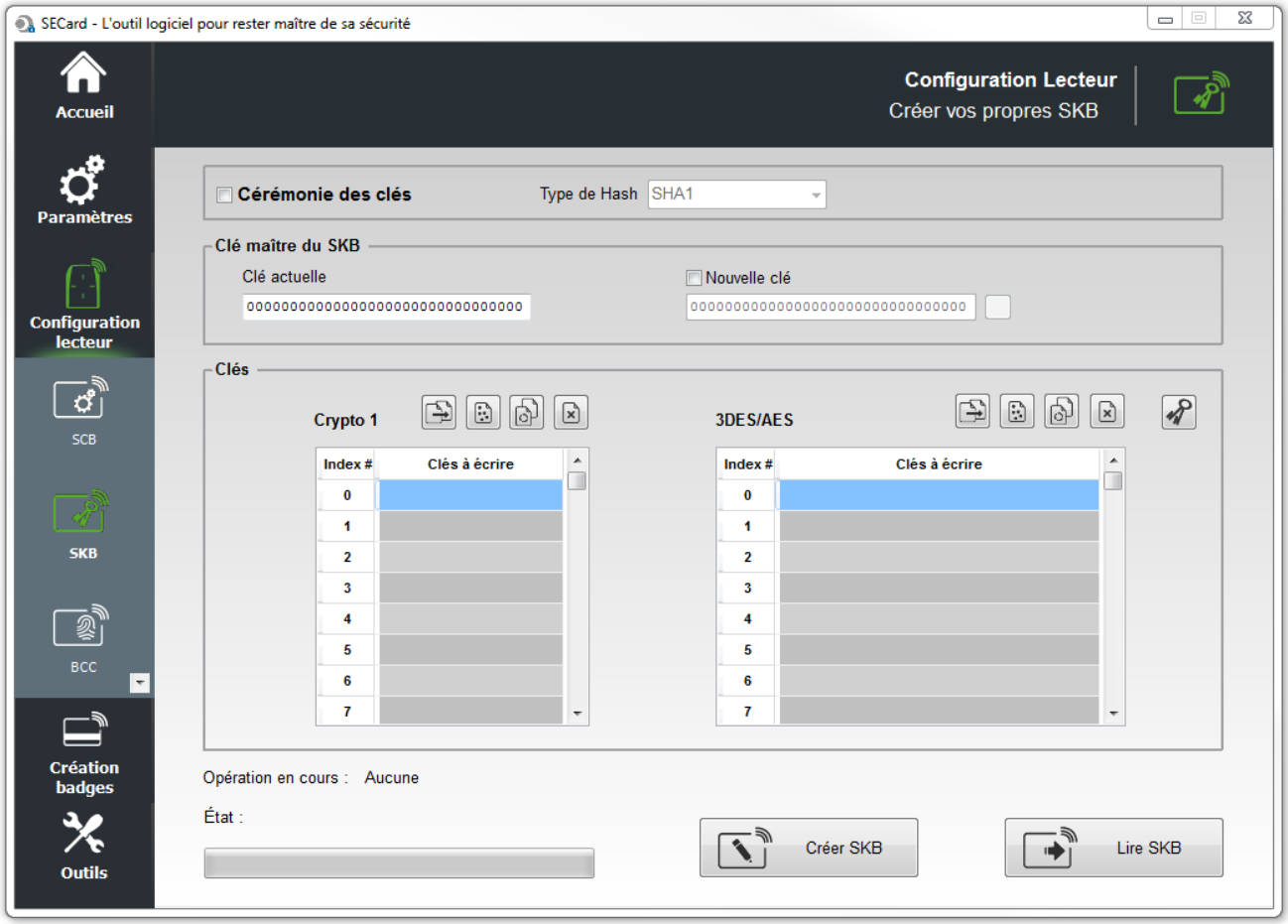
Données

- Taille : Détermine la longueur de l'ID lu. Il est défini par le protocole choisi lors de la configuration du lecteur. Cependant, il est possible de choisir une taille différente en déterminant une autre valeur. Dans ce cas, le lecteur lira l'identifiant à la taille déterminée dans le champ « *Taille* » et le restituera au format défini dans la configuration du lecteur.
- Décalage : Permet de décaler le numéro privé à encoder/lire par rapport à l'octet « 0 ».
- MSB First : Si la case est cochée, le lecteur lira l'identifiant Most Significant Byte First.
  Si la case est décochée, le lecteur lira l'identifiant Least Significant Byte First

Cliquer sur le bouton 

pour terminer la configuration des paramètres 125 kHz/3.25 MHz.

IV. Configuration lecteur - SKB



Le logiciel SECard dispose d'un module de création de badges de clés, appelés *SKB* (Secured Key Bundle). Ceux-ci renferment 32 clés *Crypto1* et 32 clés *3DES/AES* protégées par une clé « *SKB Master Key* ».

Ces badges sont utilisés sur les lecteurs suivants via une commande *Load_SKB* (*voir protocole de communication 5AA-7AA*) :

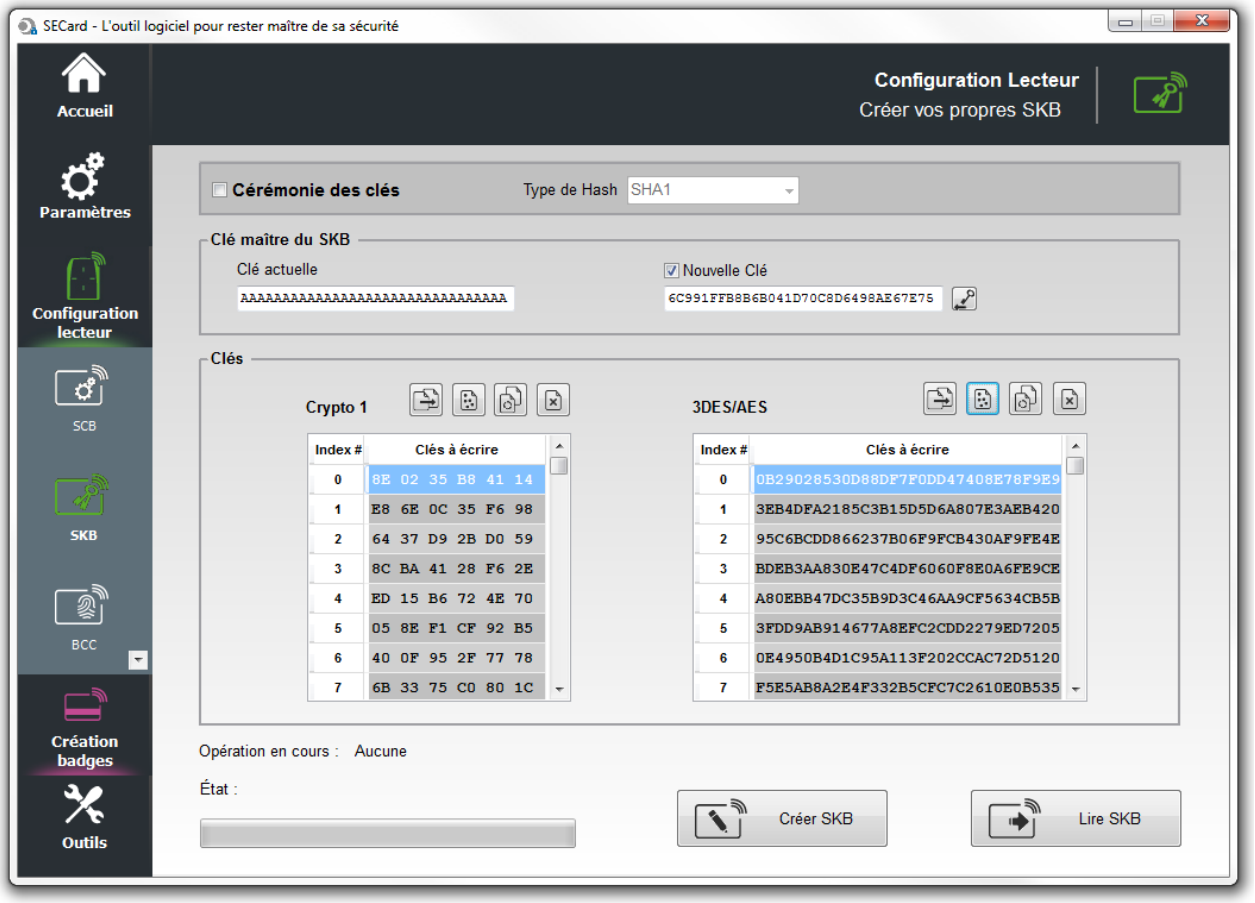
- ARC-W32-X-PH5-5AA-x — *Lecteur Evolutif – RS232 – Lecture/Ecriture*
- ARC-W33-X-PH5-7AA-x — *Lecteur Evolutif – RS485 – Lecture/Ecriture*
- WAL-W32-X-PH5-5AA-x — *Lecteur – RS232 – Lecture/Ecriture*
- WAL-W33-X-PH5-5AA-x — *Lecteur – RS485 – Lecture/Ecriture*
- ARCS-W33-X-PH5-7AA-x — *Lecteur Evolutif Sécurisé – RS485– Lecture/Ecriture*
- ARC1S-W33-X-PH5-7AA-x — *Lecteur Sécurisé – RS485– Lecture/Ecriture*
- STR-W35-E-PH5-5AA-1 — *Lecteur de table – USB – Lecture/Ecriture*
- STR-W32-E-PH5-5AA-1 — *Lecteur de table – RS232 – Lecture/Ecriture*
- LXS/ ATX/ MXS / LXC / LXE-W32-E-PH5-5AA-x — *Lecteur Prox– RS232 – Lecture/Ecriture*
- LXS/ ATX/ MXS / LXC / LXE-W33-E-PH5-5AA-x — *Lecteur Prox– RS485 – Lecture/Ecriture*
- MS-W31-E-PH5-5AA-x — *Lecteur OEM – RS232/TTL – Lecture/Ecriture*

Leur fonction est de fournir un portefeuille de clés indexées (de 0 à 31 *Crypto1* et *3DES/AES*). Une fois sauvegardées en EEPROM par le lecteur, il sera possible de les utiliser en les appelants dans les commandes *SSCP* par leur numéro d'index. Le but étant de ne plus faire transiter les valeurs de clés via la liaison.
Remarque : le temps de chargement du SKB est de 6 secondes.

Attention

Il est nécessaire de créer ces badges avec des MIFARE Plus® Level 0, MIFARE® DESFire® EV1/2 ou un badge « *SKB* » existant.

IV.1 - Création en mode classique



Clé maître du SKB

Sur un badge MIFARE® DESFire® EV1/2 vierge, la clé par défaut est « 00000000000000000000000000000000».

Sur un badge MIFARE Plus® Level 0 vierge, la clé par défaut est soit FFFF…FFFF soit A0A1A2….A15.

Il est recommandé de changer cette valeur pour plus de sécurité.

Clés

	Permet de recopier les valeurs du tableau de clés lues vers le tableau de clés à écrire.
	Permet de remplir le tableau de clés à écrire avec des valeurs de clés aléatoires. Ces valeurs seront celles écrites dans le badge SKB.
	Permet de passer du tableau de clés à écrire au tableau de clés à lire et inversement.
	Permet d'effacer les valeurs du tableau de clés à écrire.
	Tableau de clés indexées pour l'Encodage.

Crypto 1
Tableau de clés réservé aux 32 valeurs de clés en Crypto 1.

3DES/AES
Tableau de clés réservé aux 32 valeurs de clés en 3DES/AES.

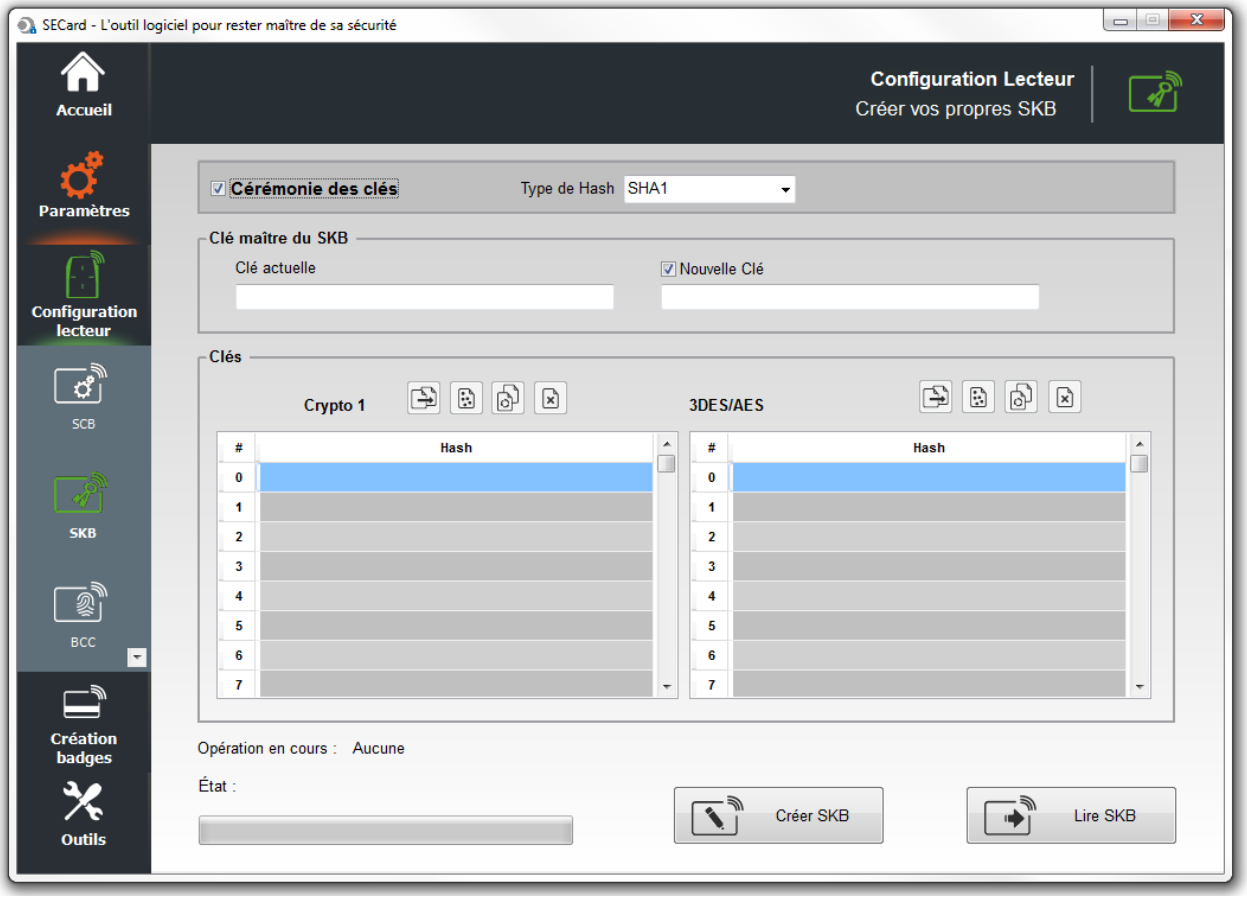
IV.2 - Création en mode « Cérémonie des clés »

Avec la cérémonie des clés, trois détenteurs sont requis pour la création du badge SKB.

Les champs clés ne sont pas accessibles en écriture, tous les champs seront automatiquement remplis par le procédé de Cérémonie des clés.

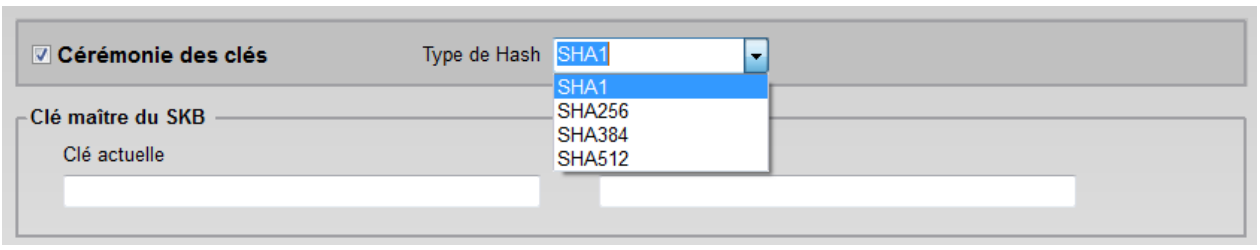
Chaque clé sera le résultat d'un XOR sur les trois clés saisies par les détenteurs. Les valeurs apparaissant dans les champs sont le Hash de ce résultat.

Il faut effectuer la Cérémonie des clés pour toutes les clés nécessaire. Si une clé n'est pas utilisée elle sera forcée à zéro.

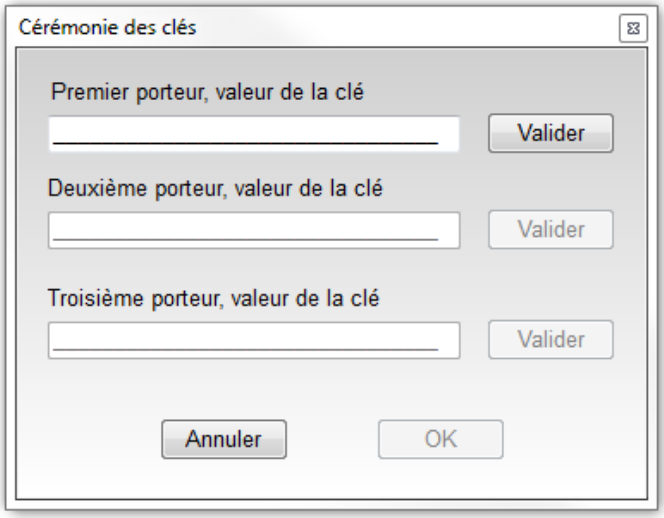


Exemple de la Cérémonie des Clés pour la clé maître du SKB

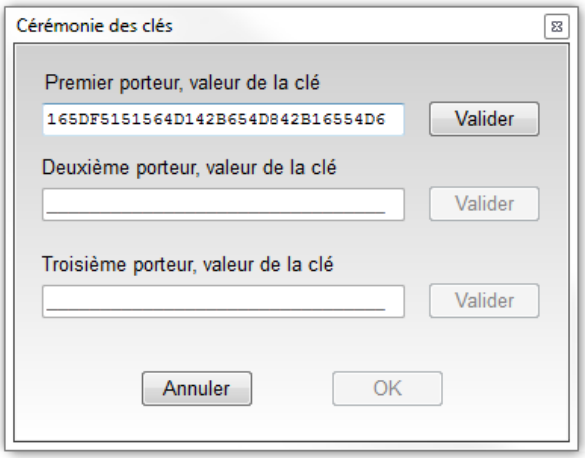
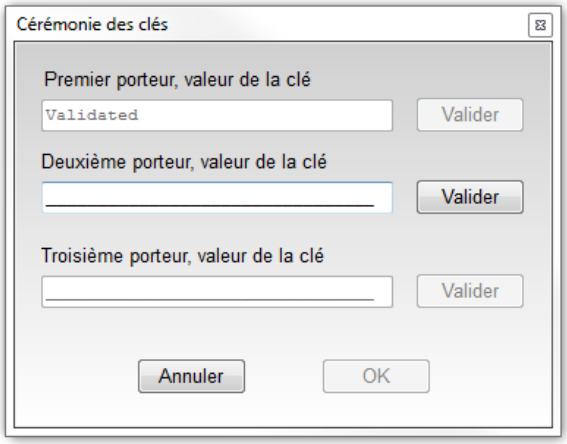
1- Sélectionner le type de Hash désiré



2- Double cliquer dans le champ « Clé actuelle » pour ouvrir la fenêtre de cérémonie des clés.

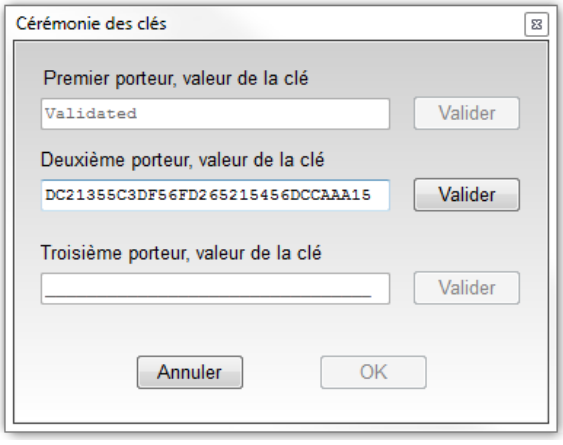
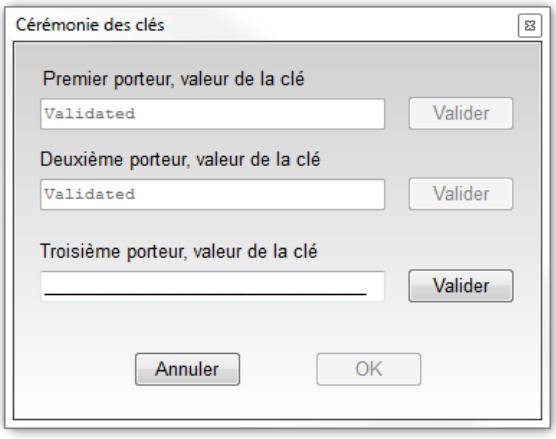


3- Premier porteur

Entrer la valeur de la premiere clé	Cliquer sur Valider
	

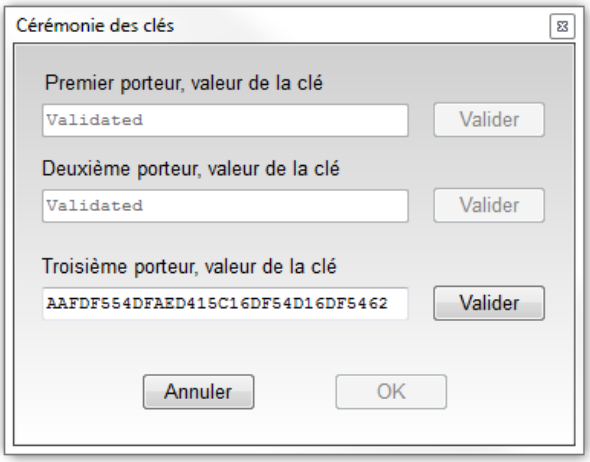
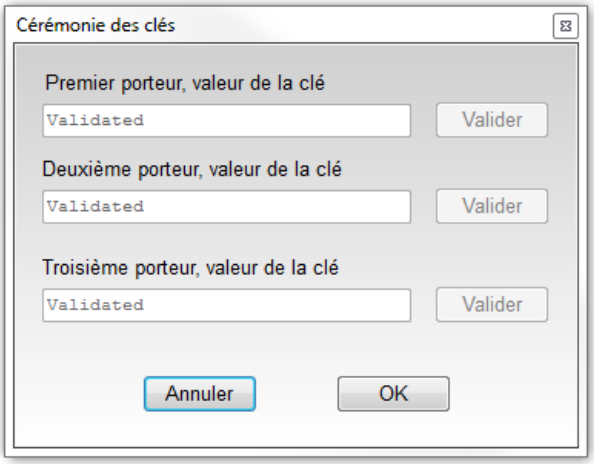
La valeur de la première clé est maintenant masquée.

4- Deuxième porteur

Entrer la valeur de la seconde clé	Cliquer sur Valider
	

Les valeurs de la première clé et de la seconde sont maintenant masquées.

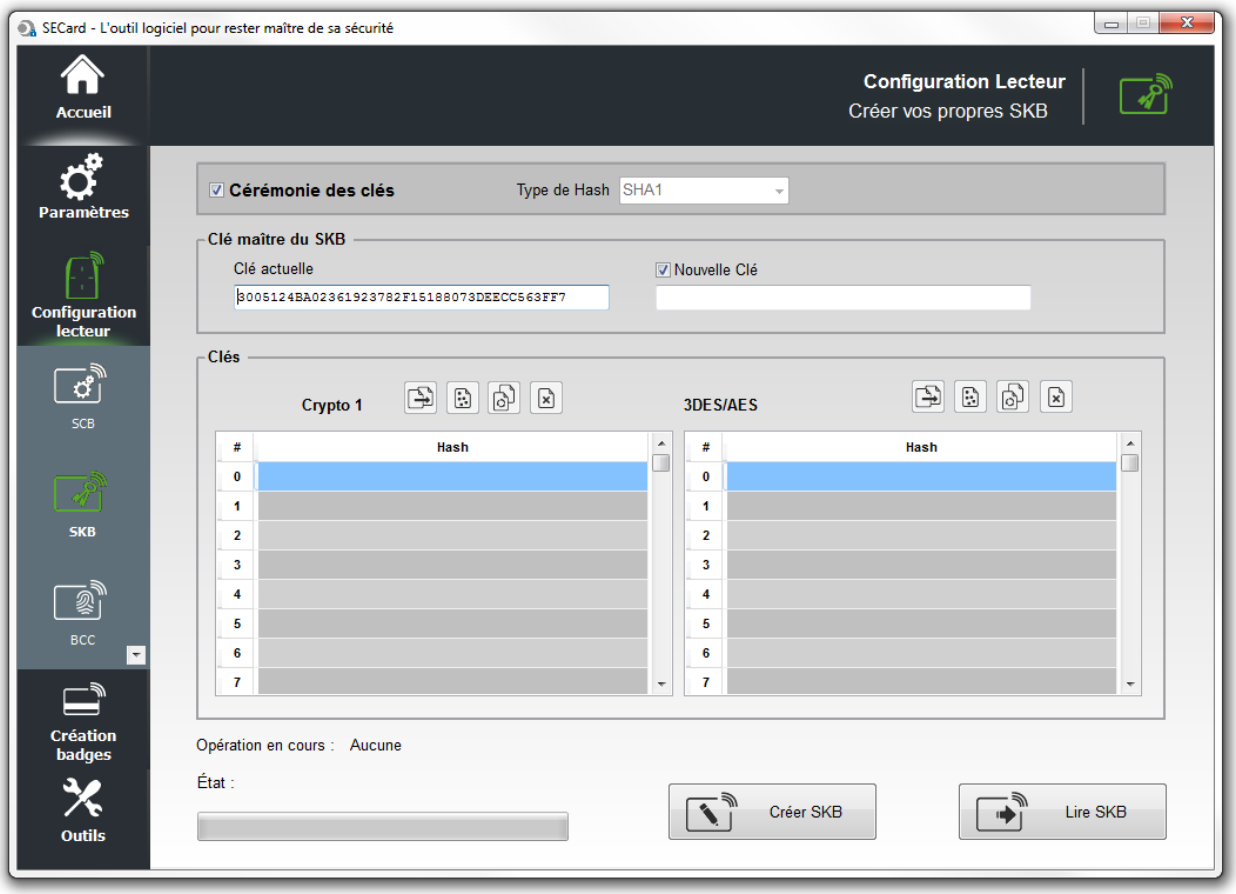
5- Troisième porteur

Entrer la valeur de la troisième clé	Cliquer sur Valider
	

Les valeurs de la première clé et de la seconde sont maintenant masquées.

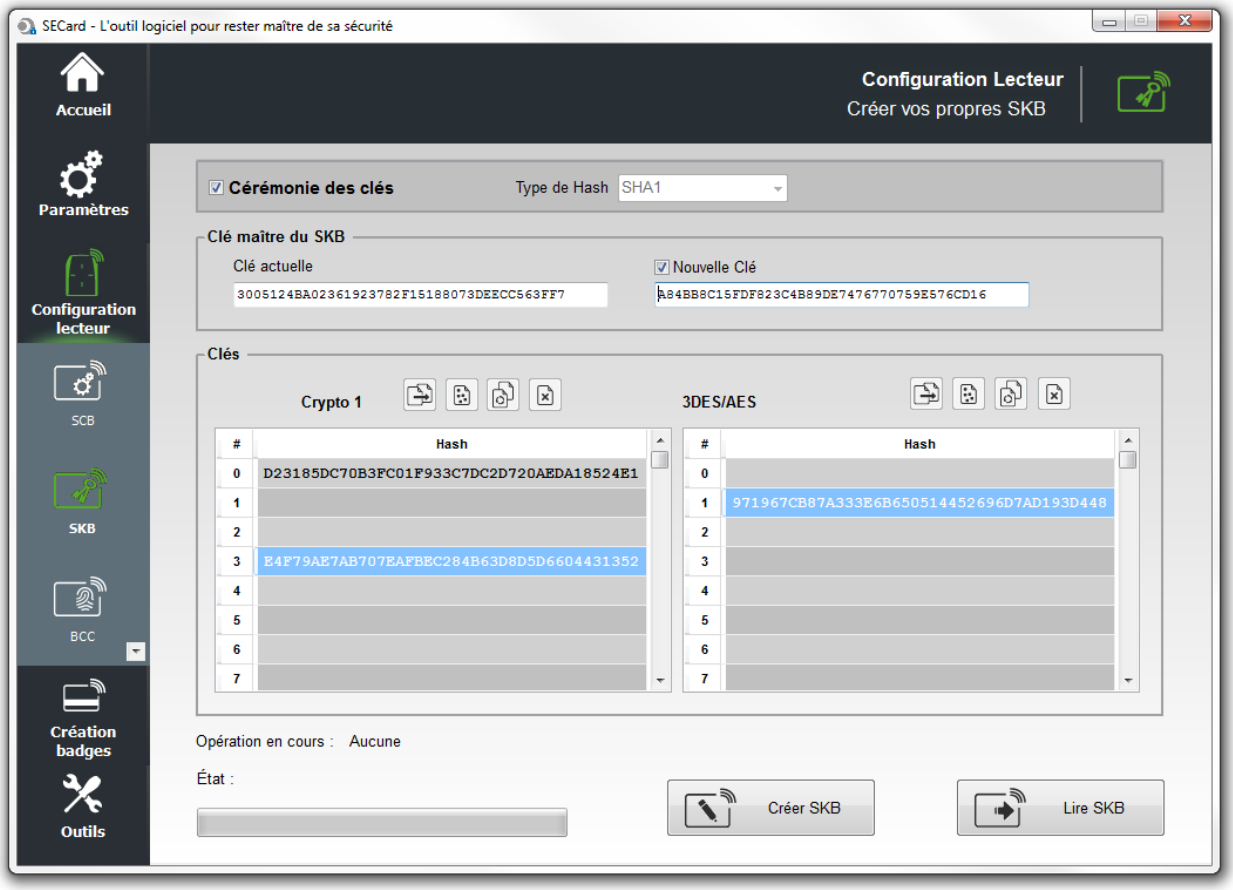
6- Cliquer sur « OK » pour terminer la cérémonie de clés pour la clé maître du badge SKB.

7- Dans la fenêtre on voit le Hash de la clé maître actuelle du SKB.



Répéter ce mode opératoire pour chaque clé utilisée.

Par exemple :



8- Créer SKB

Une fois les valeurs de clés créées, cliquer sur ce bouton pour écrire les clés dans le badge.

Lire SKB

Permet de relire un badge SKB, pour cela il faut renseigner la clé maître du badge à lire.

Pour changer la clé maître du badge SKB

Cocher Nouvelle clé, double cliquer dans le champ et répéter les étapes à partir 2 à 8.

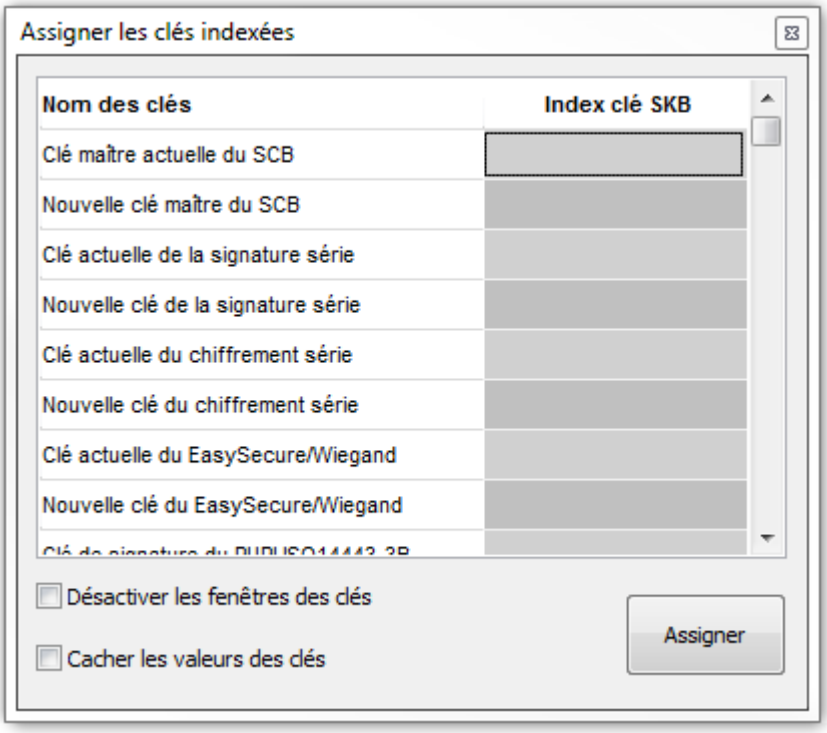
IV.3 - Utilisation de clés indexées dans la configuration SECard

A partir de la version 3.1.0, SECard permet de renseigner les champs clés de l'assistant de configuration à partir d'un badge SKB.

Les clés pouvant être ainsi assignées sont :

- Les clés Lecteur
- Les clés DESFire
- Les clés Mifare Plus Level 3
- Les clés UltraLight
- Les clés Mobile ID

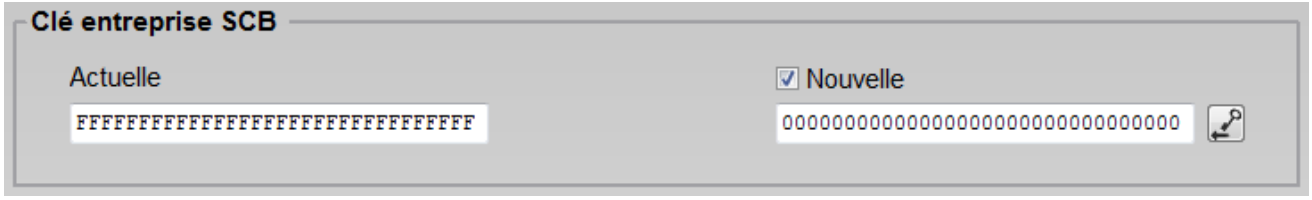
Pour ce faire, cliquer sur le bouton  , une fenêtre contenant un tableau apparait afin d'assigner des index aux différentes clés désirées.



Tous les champs ne sont pas à renseigner, uniquement ceux utiles à la configuration courante.

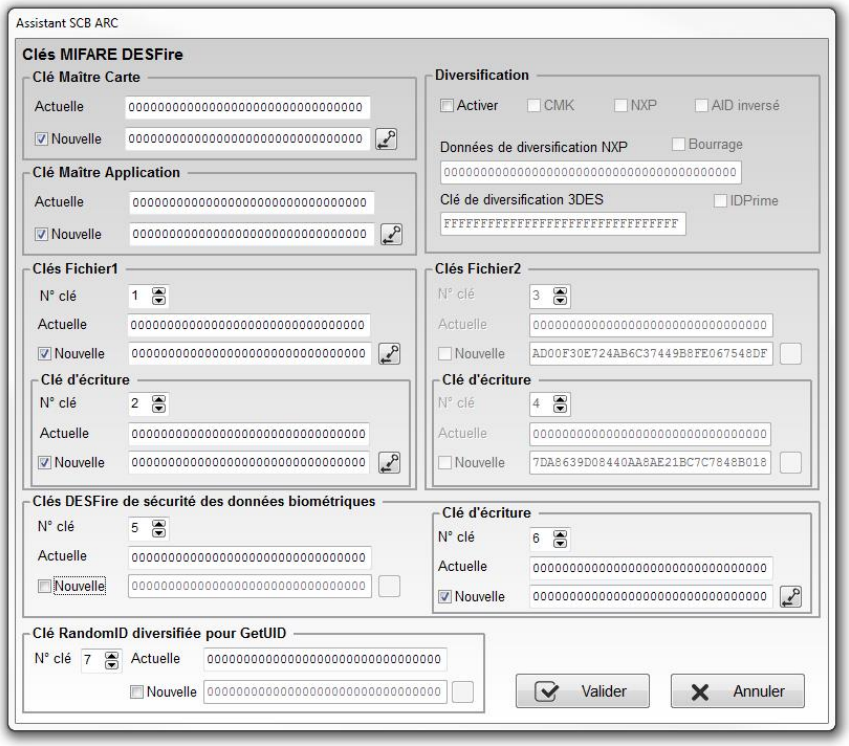
Attention : Pour faire un changement de clé, il faut impérativement dans l'assistant de configuration SCB, cocher la case Nouvelle en face du champ.

Par exemple la clé SCB actuelle est la valeur par défaut et doit passer à la valeur de la clé à l'index 2, il faut cocher la case Nouvelle pour que le changement soit effectif :



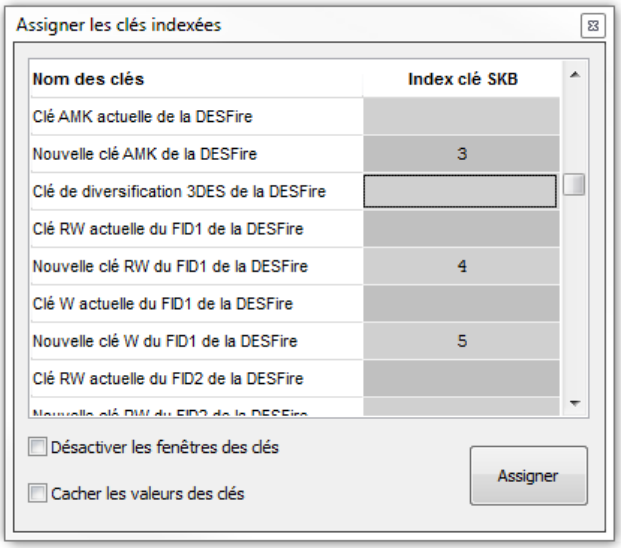
Exemple : Clés à modifier : Clé Maître Carte, Clé Maitre Application, Clé de lecture et clé d'écriture du fichier 1 d'une puce DESFire vierge.

1- Dans l'assistant SCB, après avoir renseigner les paramètres DESFire, ouvrir la fenêtre de Clés de la DESFire et cocher la case « Nouvelle » de tous les champs concernés :

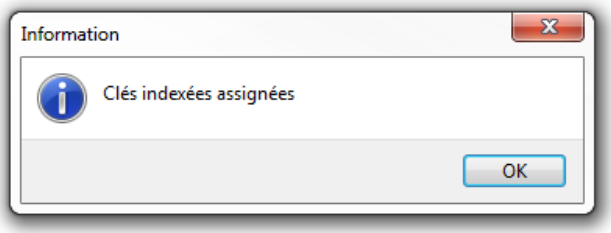


Valider

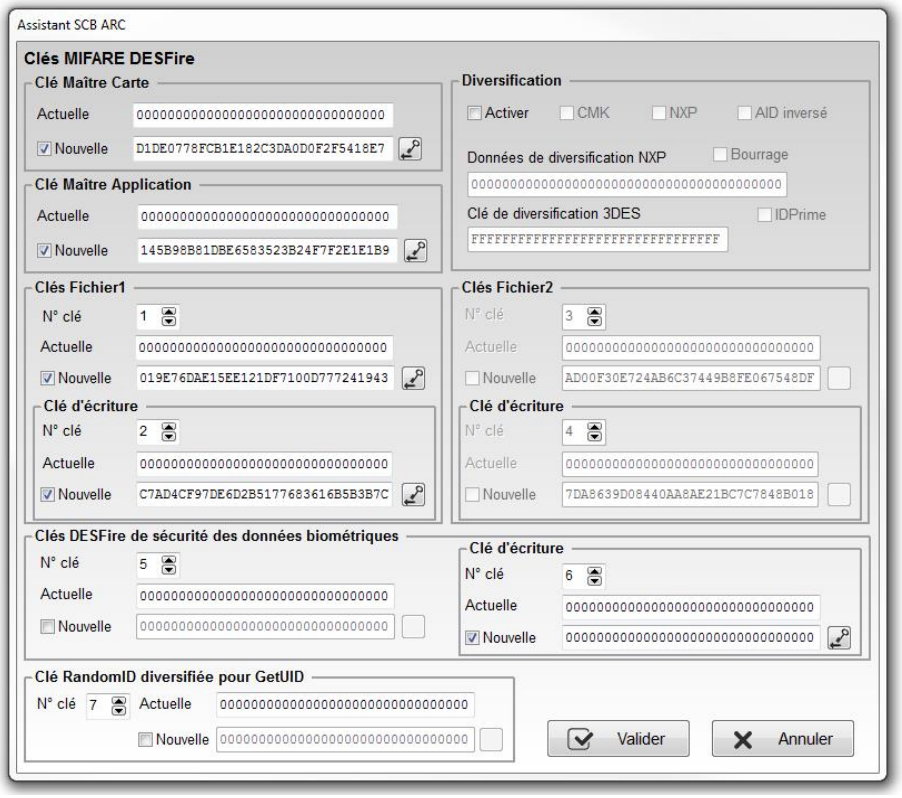
2- Dans la fenêtre SKB, charger le SKB puis ouvrir le tableau d'assignation et attribuer les numéros d'index des clés :



3- Cliquer sur le bouton Assigner



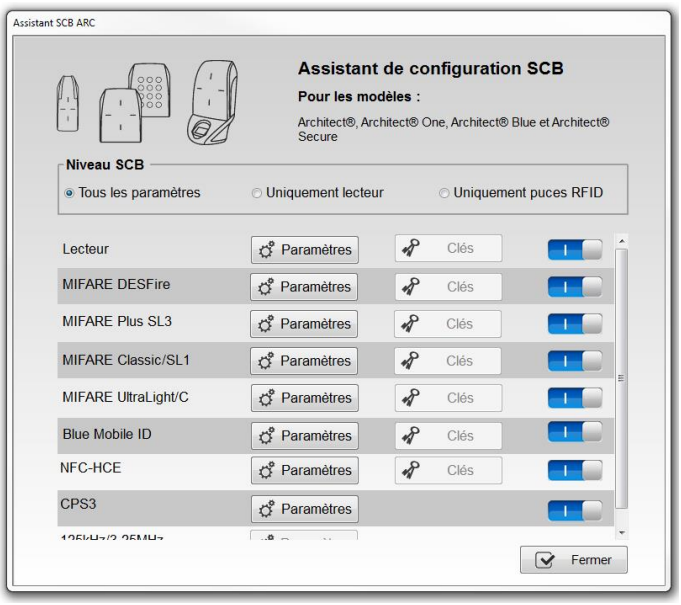
4- Si les cases « Désactiver les fenêtres des clés » et « Cacher les valeurs des clés » n'étaient pas cochées lors de l'assignation, la fenêtre de clés DESFire sera :



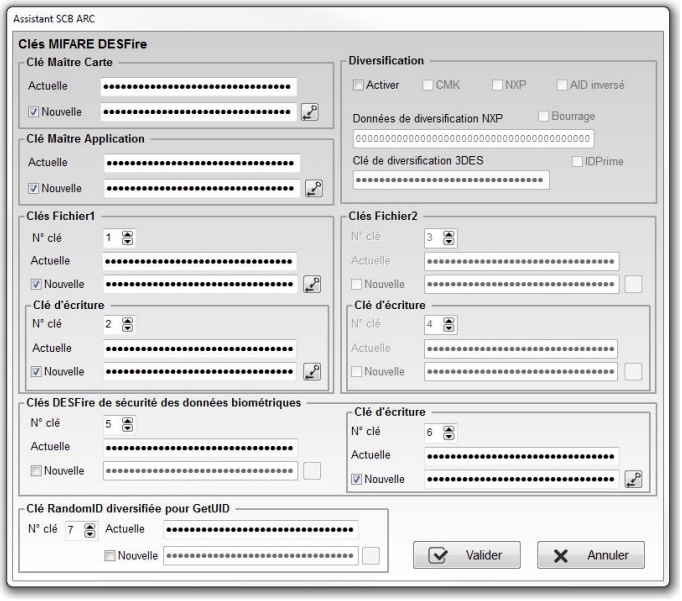
La valeur des clés apparait dans les champs conformément aux valeurs des clés indexées.

0	00000000000000000000000000000000
1	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
2	D1DE0778FCB1E182C3DA0D0F2F5418E7
3	145B98B81DBE6583523B24F7F2E1E1B9
4	019E76DAE15EE121DF7100D777241943
5	C7AD4CF97DE6D2B5177683616B5B3B7C
6	AD00F30E724AB6C37449B8FE067548DF
7	7DA8639D08440AA8AE21BC7C7848B018

5- Si la case « Désactiver les fenêtres des clés » était cochée lors de l'assignation, les boutons donnant accès aux clés seront grisés :



6- Si la case « Cacher les valeurs de clés » était cochée lors de l'assignation, la fenêtre de clés DESFire sera :

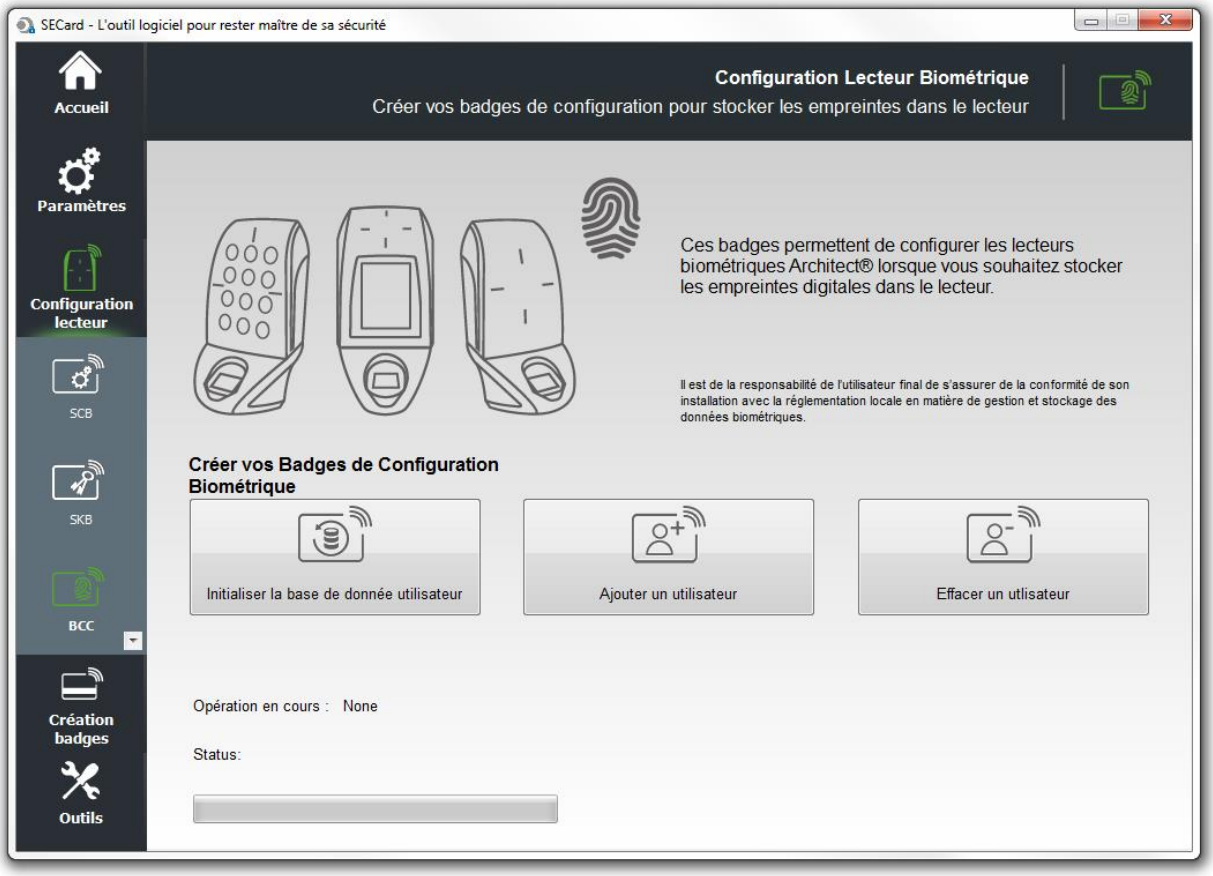


Remarque : Il est possible de modifier un index, ou les options « Désactiver les fenêtres des clés », « Cacher les valeurs des clés » en effectuant la modification et en cliquant à nouveau sur Assigner.

Attention

Toutes les valeurs de clé renseignées par cette méthode dans l'assistant de configuration ne seront pas sauvegardées dans le fichier PSE

V. Configuration Lecteur - BCC



Si dans l'assistant de configuration de l'ARC le mode choisi est ☑ Données bio dans le lecteur , la création des badges de configuration biométrique est accessible.

Trois badges de configuration sont nécessaires pour paramétrer et utiliser le lecteur dans ce mode. Les badges de configuration biométrique sont à créér avec des MIFARE®DESFire®EV1 (2ko, 4ko ou 8 ko) ou EV2.

La clé maître des badges de configurations biométrique est la valeur de la clé SCB diversifiée.

Initialiser la base de donnée utilisateur

Ce badge est utilisé pour initialiser la base de donnée dans le module.

Ajouter un utilisateur

Ce badge est utilisé pour ajouter un utilisateur dans la base de donnée.

Effacer un utilisateur

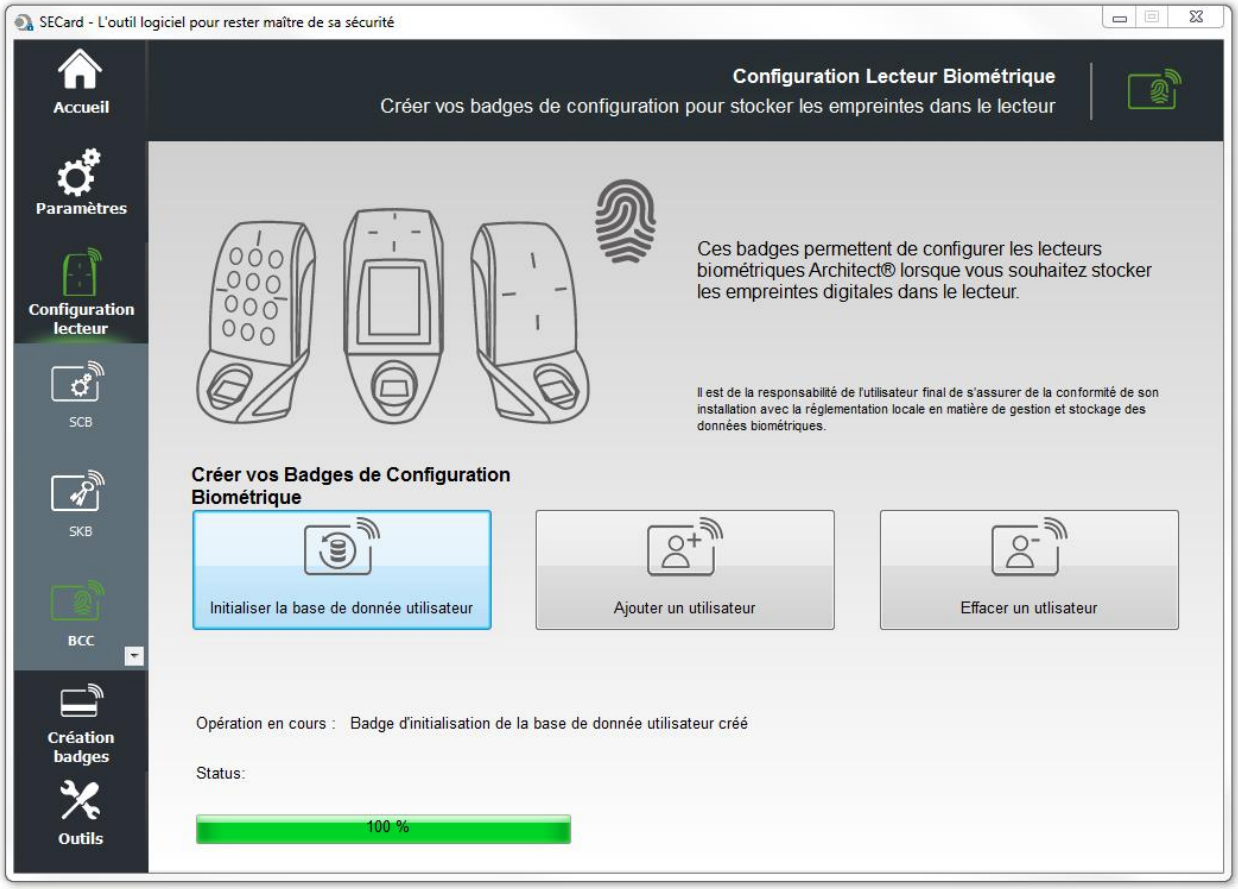
Ce badge est utiliser pour effacer un utilisateur de la base de donnée.

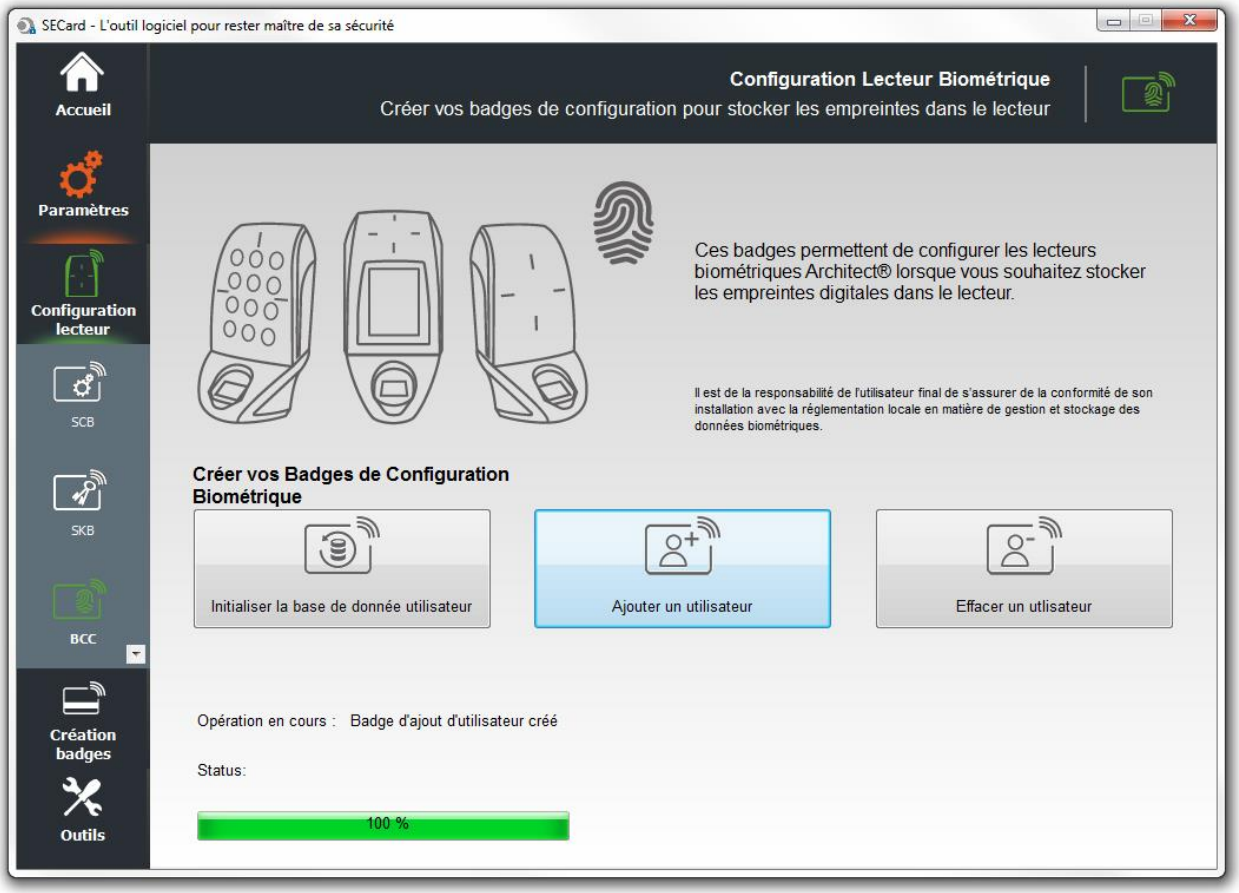
Pour plus d'information sur la procédure de configuration, d'ajout et d'effacement se référer à *T9 - Biométrie dans le lecteur*

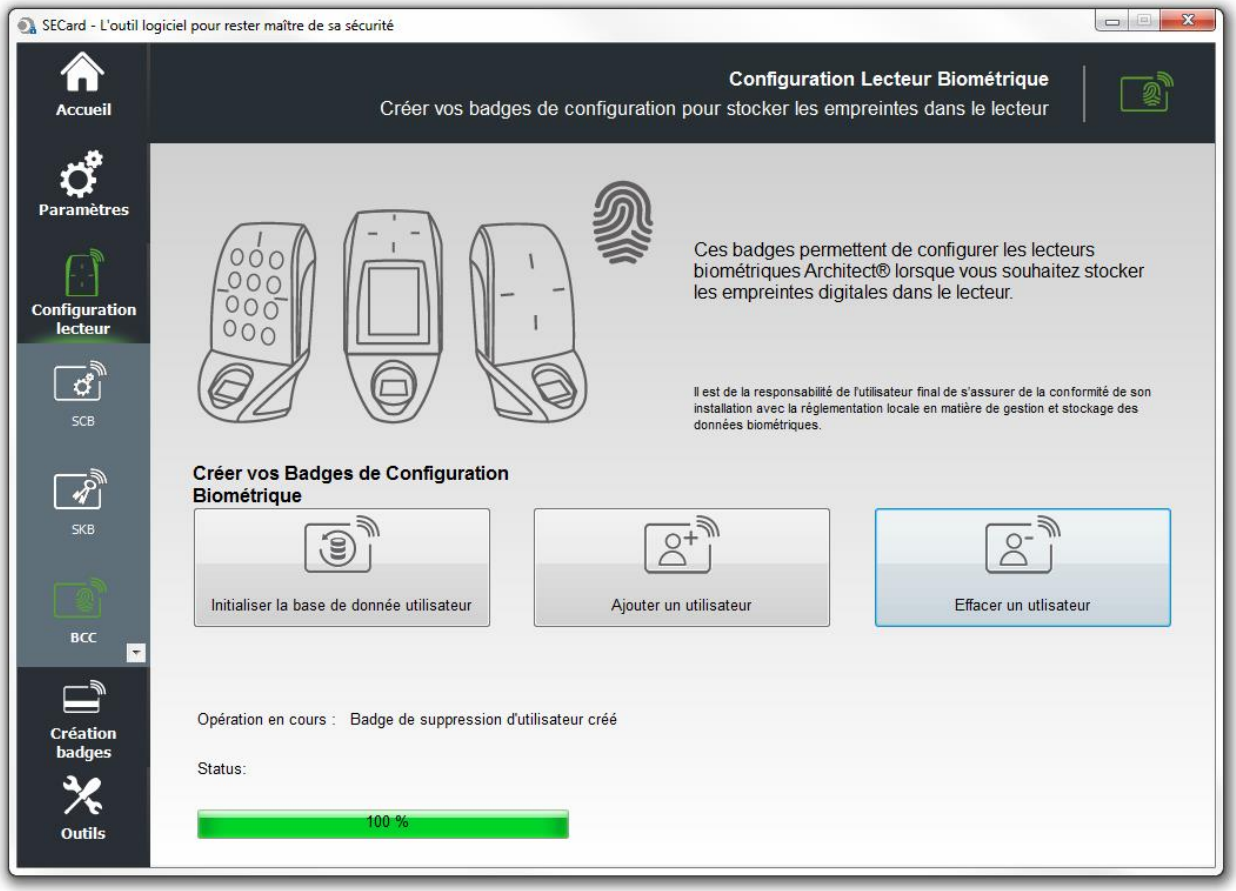
Attention

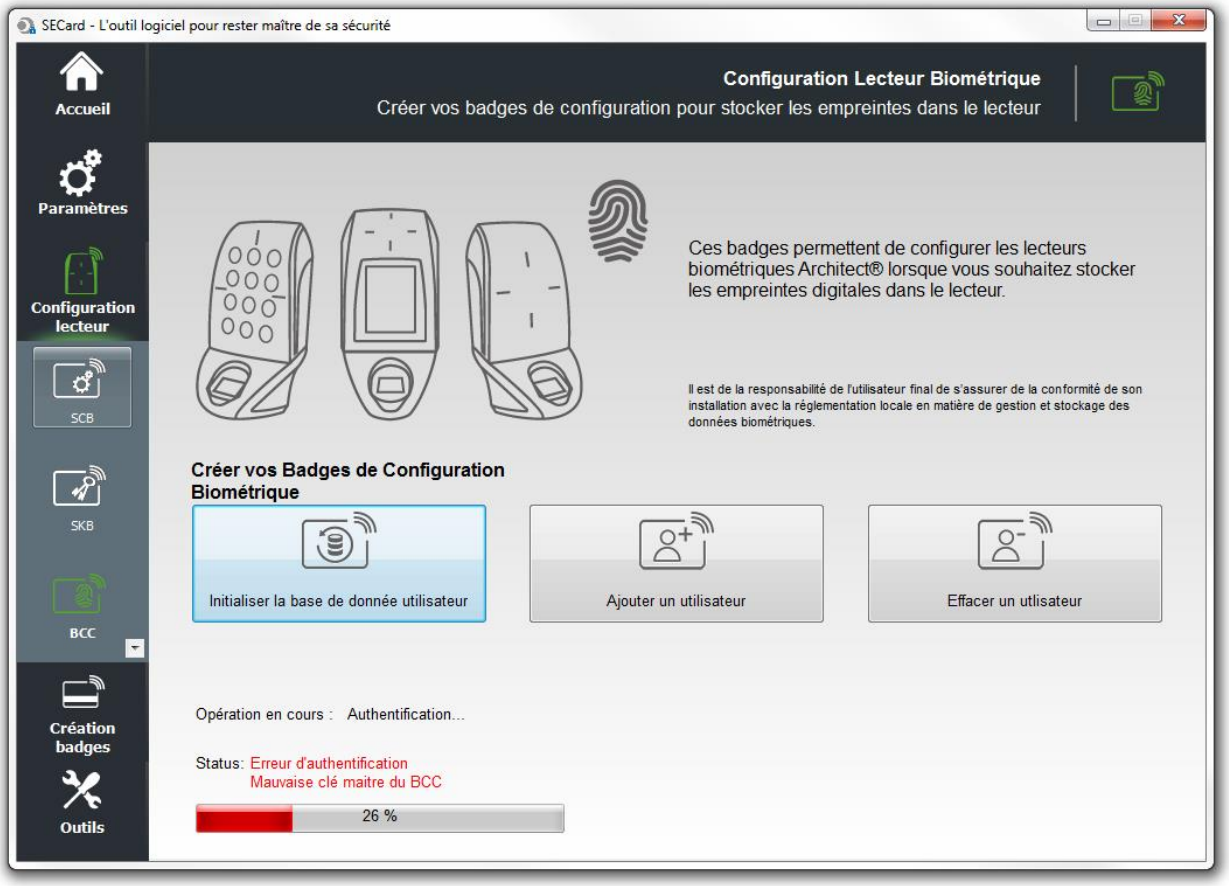
Initialiser la base de données, efface la base de données actuellement contenue dans le module.

Status


SECard - L'outil logiciel pour rester maître de sa sécurité
Accueil
Paramètres
Configuration lecteur
SCB
SKB
BCC
Création badges
Outils
Configuration Lecteur Biométrique
Créer vos badges de configuration pour stocker les empreintes dans le lecteur
Ces badges permettent de configurer les lecteurs biométriques Architect® lorsque vous souhaitez stocker les empreintes digitales dans le lecteur.
Il est de la responsabilité de l'utilisateur final de s'assurer de la conformité de son installation avec la réglementation locale en matière de gestion et stockage des données biométriques.
Créer vos Badges de Configuration Biométrique
Initialiser la base de donnée utilisateur
Ajouter un utilisateur
Effacer un utlisateur
Opération en cours : Badge d'initialisation de la base de donnée utilisateur créé
Status:
100 %

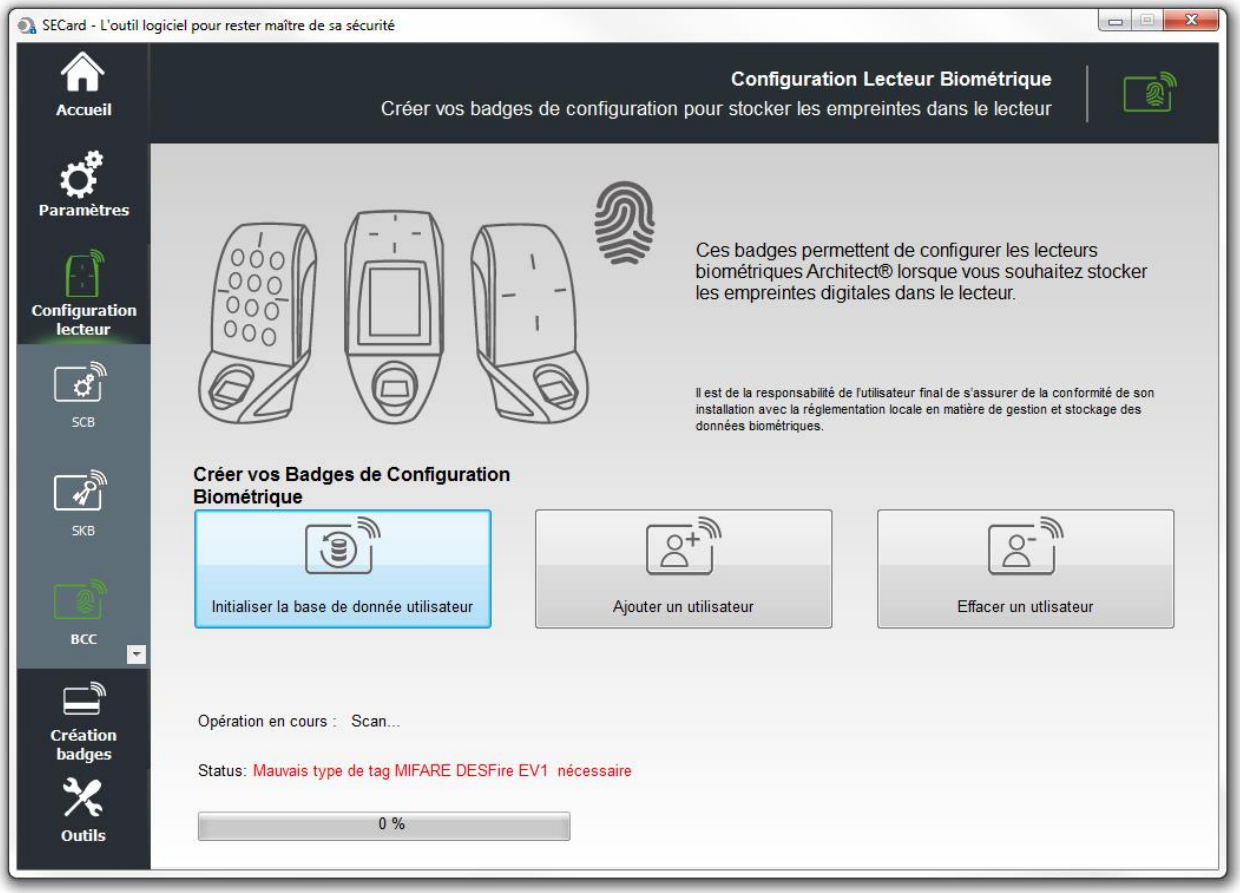

SECard - L'outil logiciel pour rester maître de sa sécurité
Accueil
Paramètres
Configuration lecteur
SCB
SKB
BCC
Création badges
Outils
Configuration Lecteur Biométrique
Créer vos badges de configuration pour stocker les empreintes dans le lecteur
Ces badges permettent de configurer les lecteurs biométriques Architect® lorsque vous souhaitez stocker les empreintes digitales dans le lecteur.
Il est de la responsabilité de l'utilisateur final de s'assurer de la conformité de son installation avec la réglementation locale en matière de gestion et stockage des données biométriques.
Créer vos Badges de Configuration Biométrique
Initialiser la base de donnée utilisateur
Ajouter un utilisateur
Effacer un utlisateur
Opération en cours : Badge d'ajout d'utilisateur créé
Status:
100 %





La clé maître des badges de configuration biométrique est la même que celle du champ SCB.

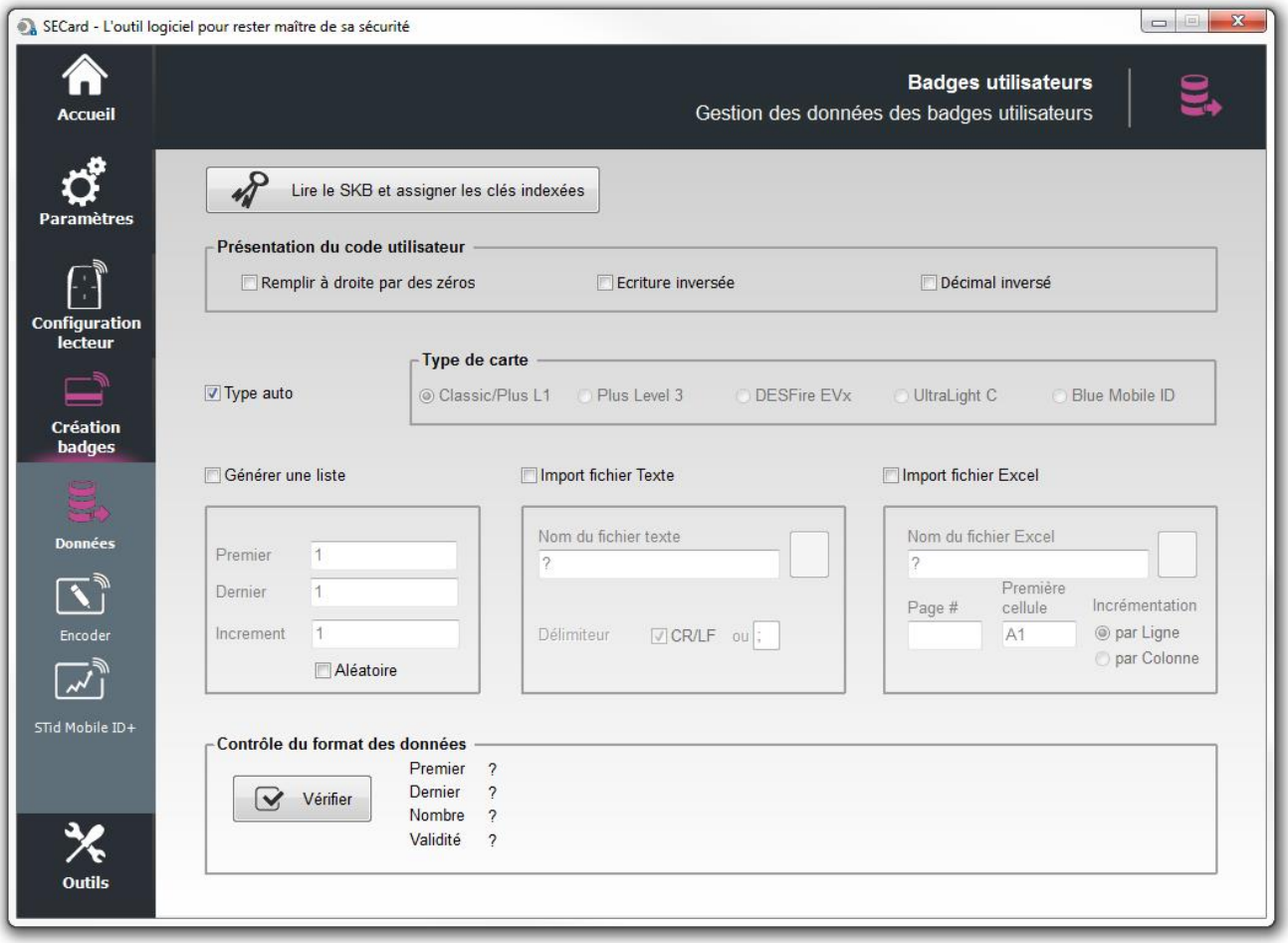
Vérifier la valeur de la clé Maître SCB ou utiliser un badge vierge.



Les badges de configuration biométrique sont à créer avec des MIFARE®DESFire®EV1 (2ko, 4ko ou 8 ko).

VI. Création badges

VI. 1 - Données



L'encodage se fait selon les paramètres définies dans la configuration. Les clés peuvent être celles définies dans la configuration ou lues dans un badge SKB.

Présentation du code utilisateur

- Remplir à droite par des zéros :
  Si la taille du numéro à encoder est inférieure à la taille définie dans la configuration, le logiciel complètera le numéro à encoder avec des zéros en poids fort par défaut.
  Si la case « Remplir à droite par des zéros » est cochée, le numéro à encoder sera complété par des zéros en poids faible.

- Ecriture inversée :
  Permet d'inverser l'écriture en hexadécimal.
  Exemple : numéro à encoder ABCDEF10, avec écriture inversée le numéro encodé est : 10EFCDAB

- Décimal inversé (ne fonctionne pas seul, option à coupler avec « Ecriture inversée » :
  Permet d'inverser l'écriture en décimal. Le numéro décimal à encoder est alors converti en hexadécimal puis inversé, sinon c'est la valeur en décimal qui est inversée puis convertie en hexadécimal.

Type de carte

Si la case « Type carte auto » est cochée, le lecteur détecte automatiquement le type de puce et l'encode selon les paramètres de la configuration en cours.

Attention

Si les puces présentées à l'encodeur sont des MIFARE Plus® Level 0 **ET** MIFARE Plus® Level 1 devant être programmées en MIFARE Plus® Level 1 **ET** en MIFARE Plus® Level 3, alors il sera nécessaire de décocher la case « *Type carte Auto* » et de choisir le type de puce à encoder.
Il est nécessaire de décocher la case « *Type carte auto* » et de cocher le mode « *Classic/Plus L1* » pour un encodage d'une puce MIFARE® Classic possédant un numéro de série sur 7 octets.

Pour Encoder la partie DESFire d'un badge IDPrime forcer le type à DESFire.

Générer une liste

Ce mode n'est disponible que pour les formats standards et les formats personnalisés de codes privés d'une longueur inférieure ou égale à 10 octets en décimal et 48 en hexadécimal.

Inscrire dans chacun des champs correspondants, le début, la fin et l'incrémentation de la liste des numéros à encoder.

Aléatoire

L'option ne peut être activée / désactivée que par l'Administrateur. Le champ incrément devient le nombre d'éléments de la liste de valeurs aléatoires.
Génère une liste de n valeurs aléatoires entre la valeur Premier et dernier.

Note :

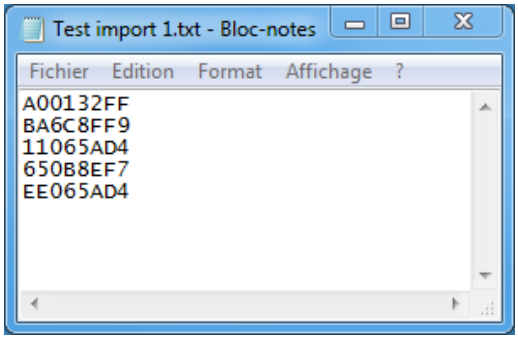
- ✓ La liste aléatoire n'est pas compatible avec le format du Wiegand 26 bits (code site + code carte).
- ✓ Le nombre maximum de valeur aléatoire est 0x7F FF FF FF (soit 2147483647 valeurs).

Avec cette option la valeur encodée n'apparaitra pas dans la fenêtre de « log de session de programmation » et il ne sera pas possible en mode Utilisateur de relire la donnée privée encodée avec la fonction « Lire Id Privé » de SECard. Seul l'administrateur pourra relire la valeur en décochant l'option.

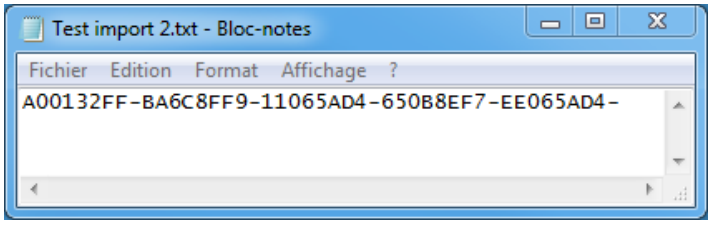
Import fichier Texte

Permet d'importer des listes sous format texte, qui seront utilisées pour la programmation des badges utilisateurs.

Délimiteur « CR/LF »



Délimiteur « - »



Attention

Le dernier numéro à encoder doit être suivi du délimiteur.

SECard complètera par des « 0 » en poids forts les numéros dont la taille est inférieure à celle définie dans le protocole.

Attention

L'import fichier Texte risque de ne pas reconnaître les valeurs dans un fichier si :

- Cas du délimiteur CR/LF : il y a des lignes vierges au milieu ou en fin de fichier.
- Cas d'un autre séparateur (Exemple « **;** ») : il y a plusieurs séparateurs accolés (ex. 12313;12385485;;;5646;;12;041)

Import fichier Excel

Permet d'importer des listes sous format Excel, qui seront utilisées pour la programmation des badges utilisateurs.

Renseigner la page (feuille) dans laquelle se trouvent les numéros à encoder, ainsi que la première cellule.

Incrémentation par ligne : à utiliser lorsque les numéros sont écrits dans une colonne.
Incrémentation par colonne : à utiliser lorsque les numéros sont écrits sur une ligne.

SECard complètera par des « 0 » en poids forts les numéros dont la taille est inférieure à celle définie dans le protocole.

Attention

L'importation Excel ne gère pas des zones discontinues. Si l'utilisateur insère des cases vides avant la dernière case, celles-ci seront considérées par SECard comme invalides et la programmation s'arrêtera.

Il est nécessaire que le logiciel Excel® soit installé.

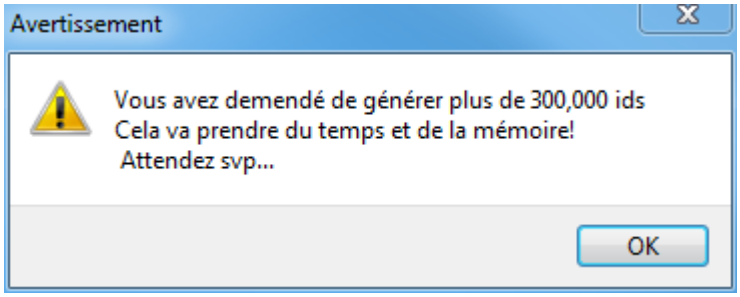
Contrôle du format des données

Permet de vérifier la validité des numéros à encoder. Celle-ci se base uniquement sur les premières et dernières valeurs à programmer.

Note :

* Le logiciel ne vérifiera que les premières et dernières valeurs des fichiers Texte et Excel. En aucun cas, cette fonction ne vérifiera les maximums et/ou les minimums.

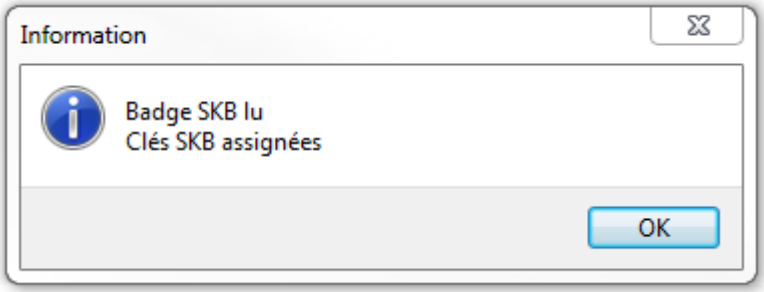
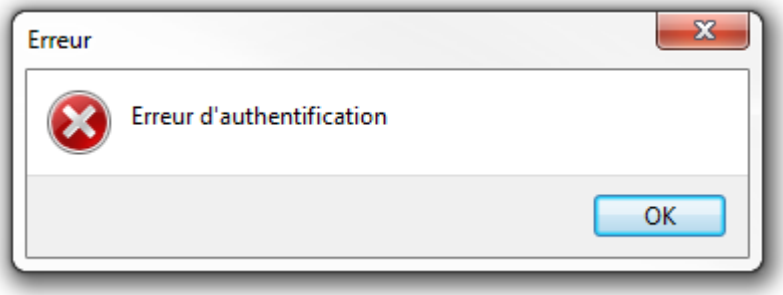
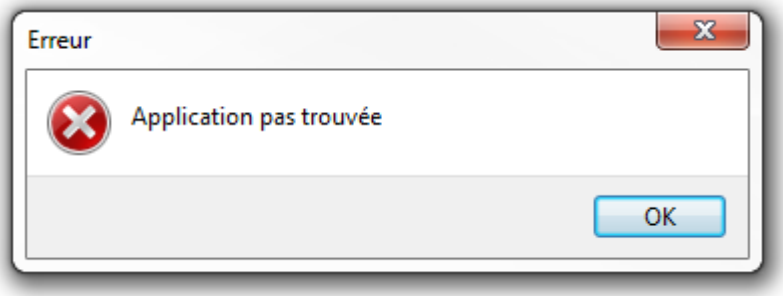
* Si le nombre d'identifiants est supérieur à 300 000, un message apparaîtra pour vous demander de patienter un peu lors de la vérification et que celle-ci nécessitera les ressources de la mémoire vive de votre ordinateur.



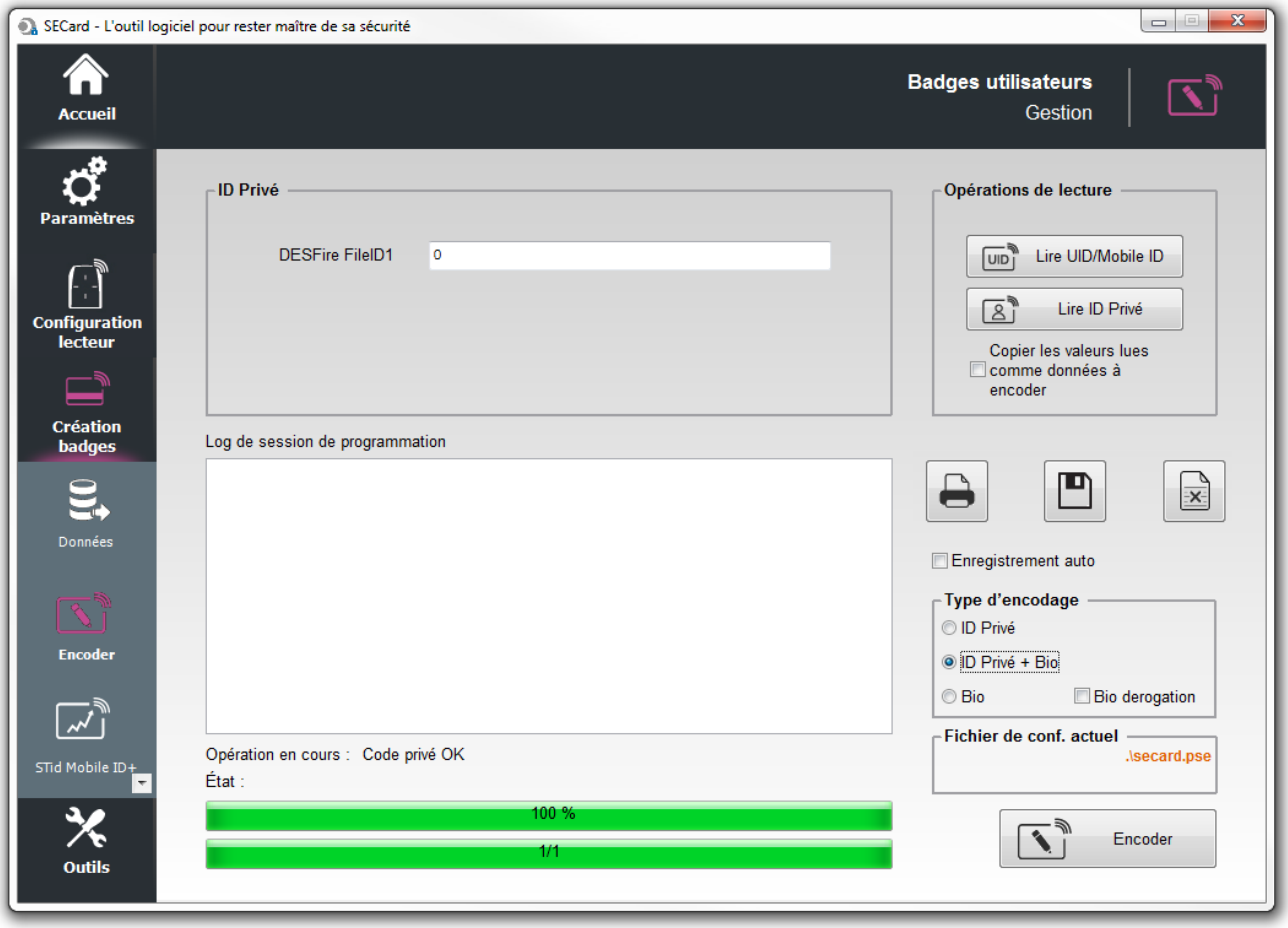
Lire le SKB et assigner les clés indexées

Dans le cas où les clés nécessaires à l'encodage sont contenues dans un badge SKB, il faut lire le badge SKB pour charger temporairement les clés dans SECard, la clé Maître du SKB doit être est contenu dans le fichier de configuration .pse.

Statut

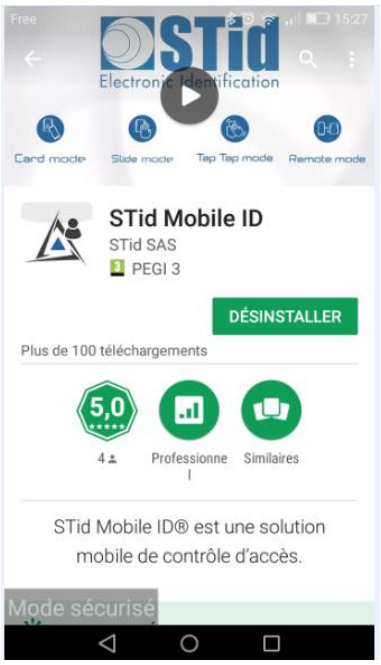
	Badge SKB lu
	La clé Maître du SKB renseignée par l'administrateur dans la partie SKB de SECard n'est pas la même que la clé du badge présenté.
	Le badge présenté n'est pas un badge SKB

VI. 2 - Encoder

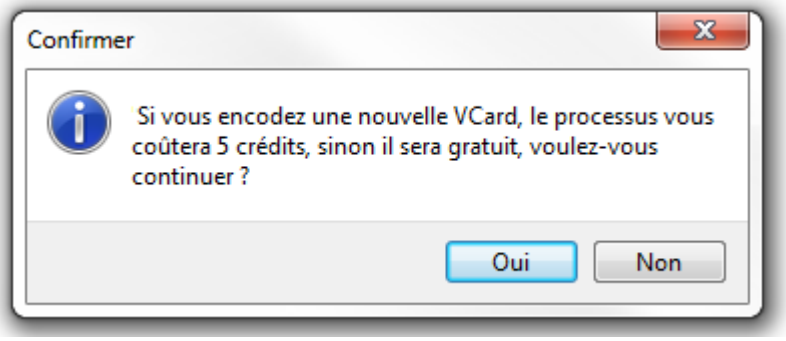


Une fois le paramétrage de l'application terminé ainsi que les numéros devant être encodés déterminés, les identifiants peuvent être programmés.

Pour encoder un identifiant dans un smartphone il est nécessaire d'installer l'application STidMobile ID depuis l'AppStore ou le PlayStore.



Encodage VCard



- Si c'est une nouvelle VCard le process d'encodage coûtera 5 crédits.
- Si la VCard est déjà encodée dans le téléphone et que l'encodage ne modifie que la valeur de l'identifiant privé le process d'encodage sera gratuit.

ID Privé

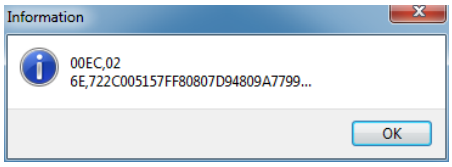
Permet de saisir manuellement la (les) valeur(s) de(s) l'id Privé(s) à encoder.

Note : si « Générer une liste » ou « Import fichier Texte ou Excel » a été sélectionné, le champ n'est pas accessible.

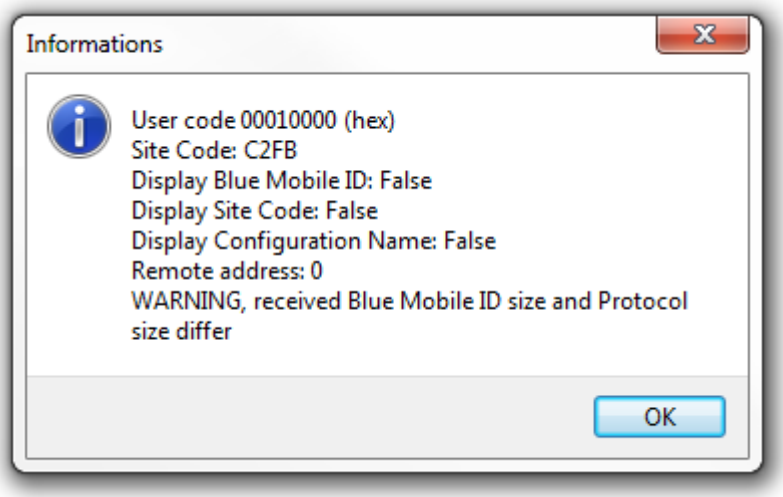
Opérations de lecture

- Lire UID/ Mobile ID : permet de lire l'UID ainsi que le type de puce de l'identifiant présenté au lecteur.
- Lire ID Privé : permet de lire le code privé ou les templates de l'identifiant présenté au lecteur selon la configuration en cours et si la case « Copier les valeurs lues comme données à encoder » est cochée, la valeur lue est copiée dans le champ à encoder.

Exemple de relecture template :



Exemple de relecture ID privé Mobile ID :



	Permet d'imprimer les opérations réalisées.
	Permet de sauvegarder les opérations réalisées.
	Permet d'effacer la liste des opérations réalisées.

Enregistrement auto

Permet d'enregistrer les opérations dans un fichier RTF dans le même dossier que le fichier de settings .pse en cours.

Type d'encodage

- ID Privé : Permet d'encoder uniquement l'identifiant privé.
- ID Privé + Bio : Permet d'encoder l'identifiant privé **et** l'empreinte biométrique.
- Bio : Permet d'encoder uniquement l'empreinte biométrique.

Bio dérogation : Disponible uniquement si la dérogation bio a été autorisé dans les options biométrique de la puce. Dans ce cas une dérogation sera encodée dans le badge et le process d'encodage ne demandera pas la présentation du doigt de l'utilisateur.

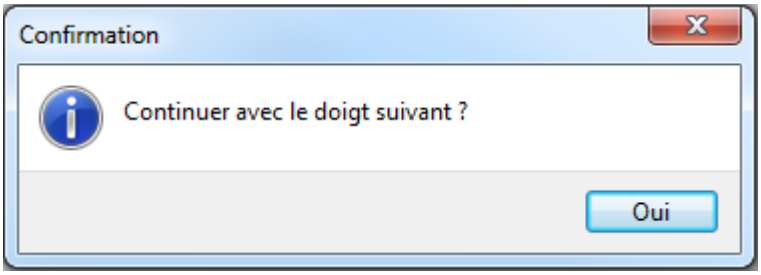
Fichier de conf. actuel

Indique le fichier de configuration actuellement chargé dans SECard et suivant lequel les identifiants vont être encodés.

Encodage des empreintes biométriques

Lorsqu'une configuration biométrique est validée et que le type d'encodage choisi est «*Bio*» ou « *ID Privé + Bio* », le logiciel SECard affiche une fenêtre de capture des empreintes digitales.	Placer alors le doigt à encoder sur le capteur biométrique. Celui-ci doit être allumé en rouge afin d'indiquer qu'il est prêt à lire l'empreinte.	Lorsque l'empreinte est lue, celle-ci s'affiche sur la fenêtre de lecture et la barre située à droite affiche la progression de l'analyse.
		

Dès que l'empreinte est lue, le logiciel vous demandera de positionner un autre doigt si la configuration le demande.



Si l'empreinte est mal positionnée, le logiciel vous informera du problème en indiquant de positionner le doigt dans la bonne position

Attention

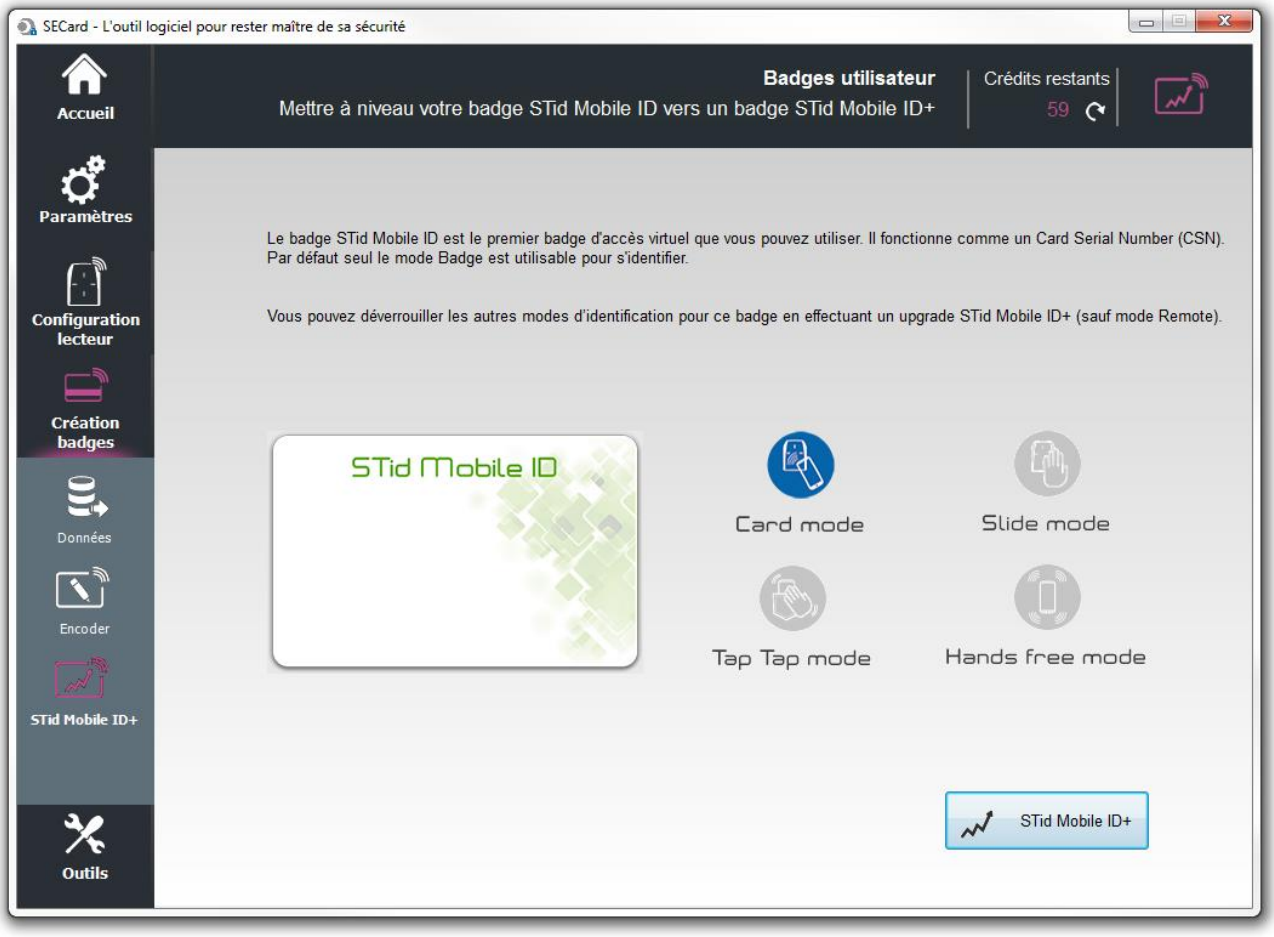
Il est nécessaire que le capteur biométrique soit connecté sur un port USB.
Le doigt présenté au capteur doit être propre et exempt de tâches, gras, etc…
La surface du capteur biométrique doit être propre et exempt de tâches, gras, etc…

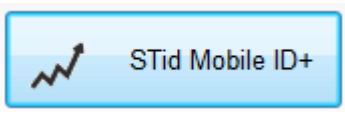
VI. 3 – STid Mobile ID+

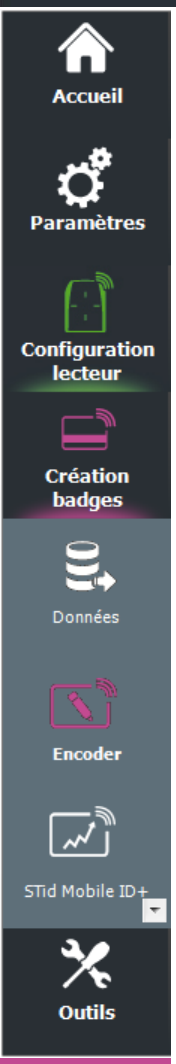
Lors de l'installation de l'application STid Mobile ID sur un smartphone, un badge d'accès « STid Mobile ID » est installé.

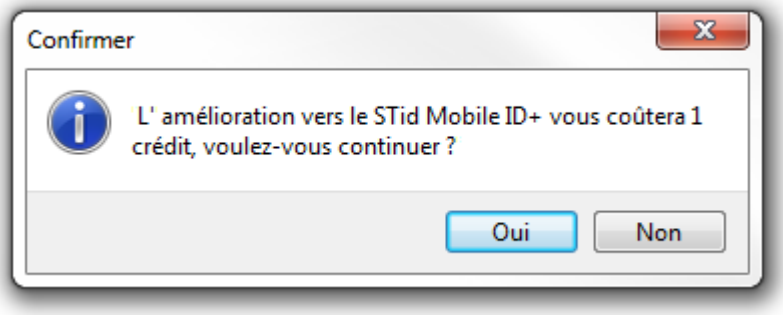
Ce badge fonctionne comme un Card Serial Number (CSN). Il fonctionne uniquement en mode de détection badge.

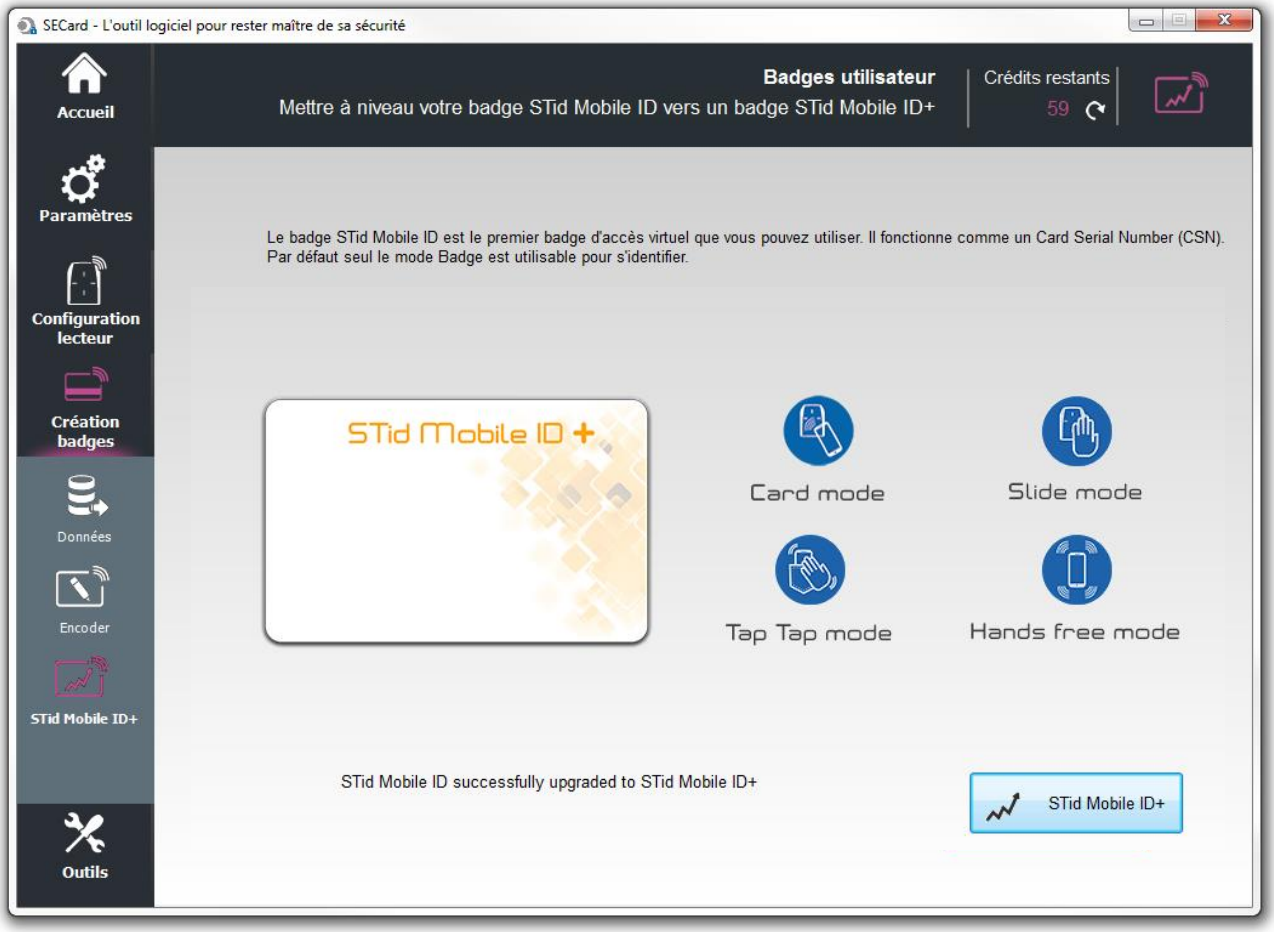
Pour bénéficier des avantages du mode Slide, Tap Tap et Mains-Libres vous pouvez passer sur le STid Mobile ID+. Cette action coûtera 1 crédit.



Cliquer sur le bouton 

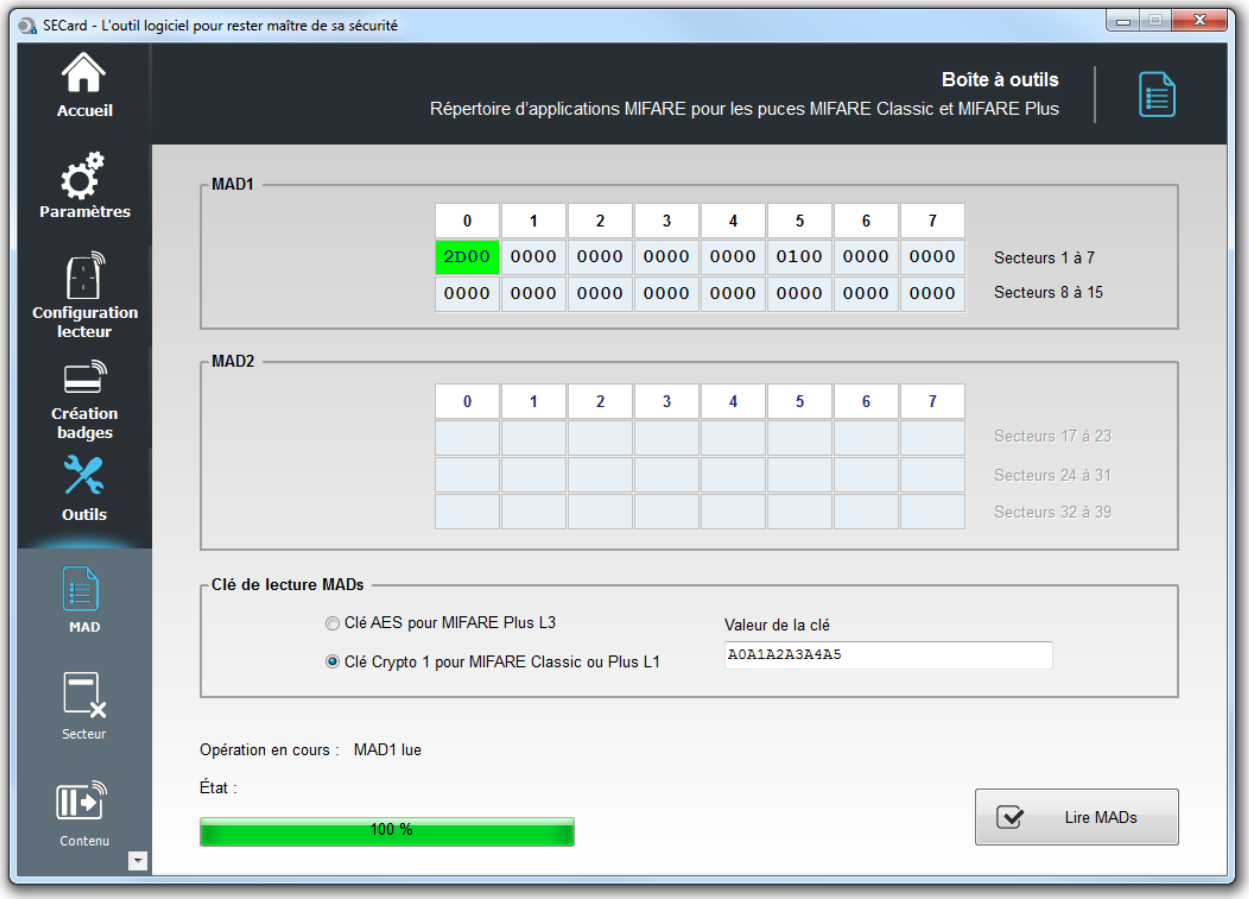

Accueil
Paramètres
Configuration lecteur
Création badges
Données
Encoder
STid Mobile ID+
Outils


Confirmer
L' amélioration vers le STid Mobile ID+ vous coûtera 1 crédit, voulez-vous continuer ?
Oui
Non


SECard - L'outil logiciel pour rester maître de sa sécurité
Accueil
Paramètres
Configuration lecteur
Création badges
Données
Encoder
STid Mobile ID+
Outils
Badges utilisateur
Mettre à niveau votre badge STid Mobile ID vers un badge STid Mobile ID+
Crédits restants
59
Le badge STid Mobile ID est le premier badge d'accès virtuel que vous pouvez utiliser. Il fonctionne comme un Card Serial Number (CSN).
Par défaut seul le mode Badge est utilisable pour s'identifier.
STid Mobile ID +
Card mode
Slide mode
Tap Tap mode
Hands free mode
STid Mobile ID successfully upgraded to STid Mobile ID+
STid Mobile ID+

VII. Outils

VII. 1 - MAD

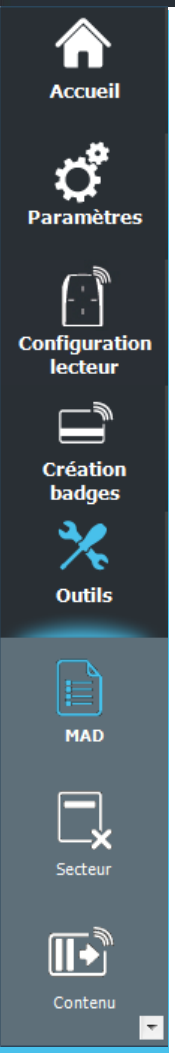


Permet de scanner une puce MIFARE® Classic ou MIFARE Plus® afin de lire le contenu de la MAD et d'afficher les codes *AID* présents.
Un emplacement de la MAD contenant un code *AID* désigne un secteur comme occupé par une application. Les secteurs 0 et 16 ne sont pas utilisables car ils contiennent la MAD1 et la MAD2.

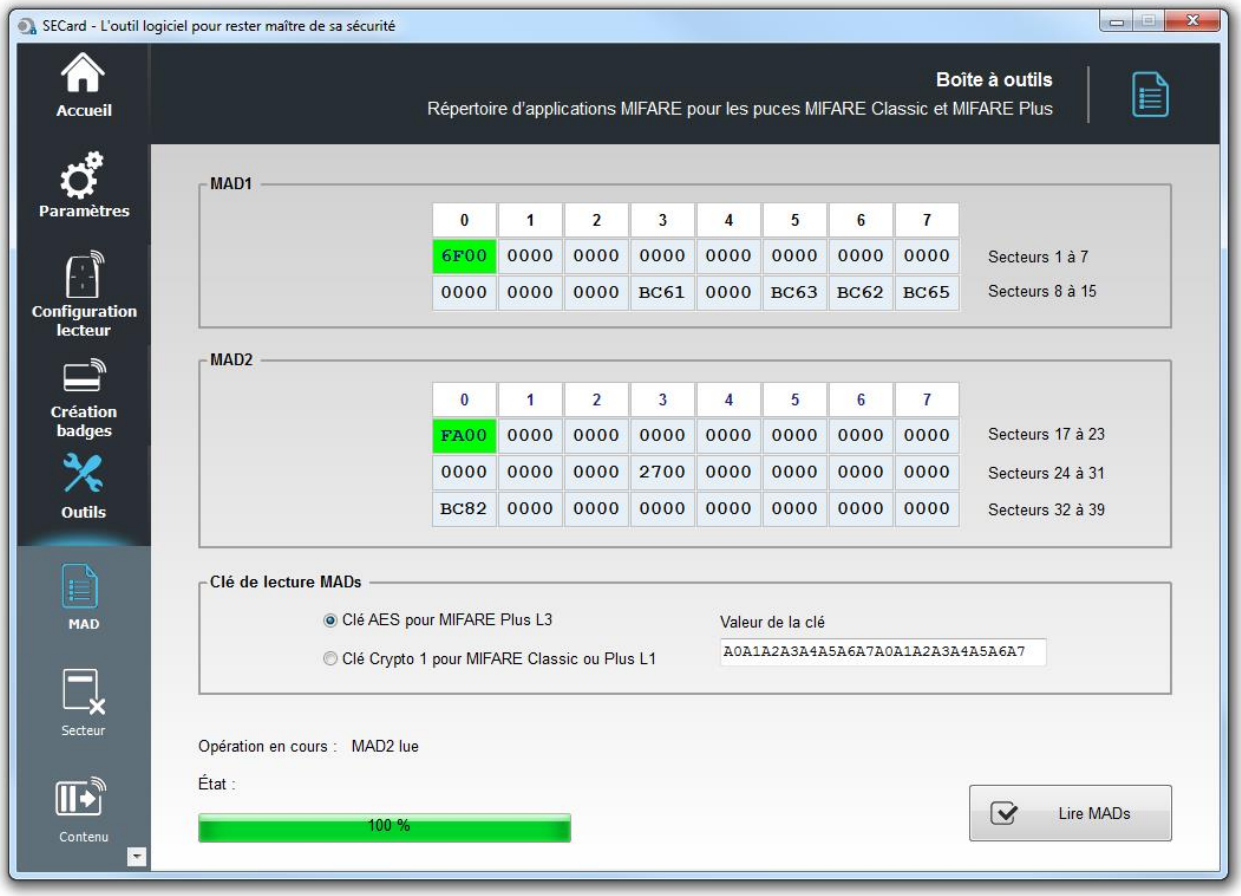
Il est nécessaire de renseigner les clés de lecture des MAD :

Pour une MIFARE® Classic ou une MIFARE Plus® Level1, la clé Crypto 1 par défaut est A0A1A2A3A4A5.

Pour une MIFARE Plus® Level 3, la clé AES par défaut est A0A1A2A3A4A5A6A7A0A1A2A3A4A5A6A7.



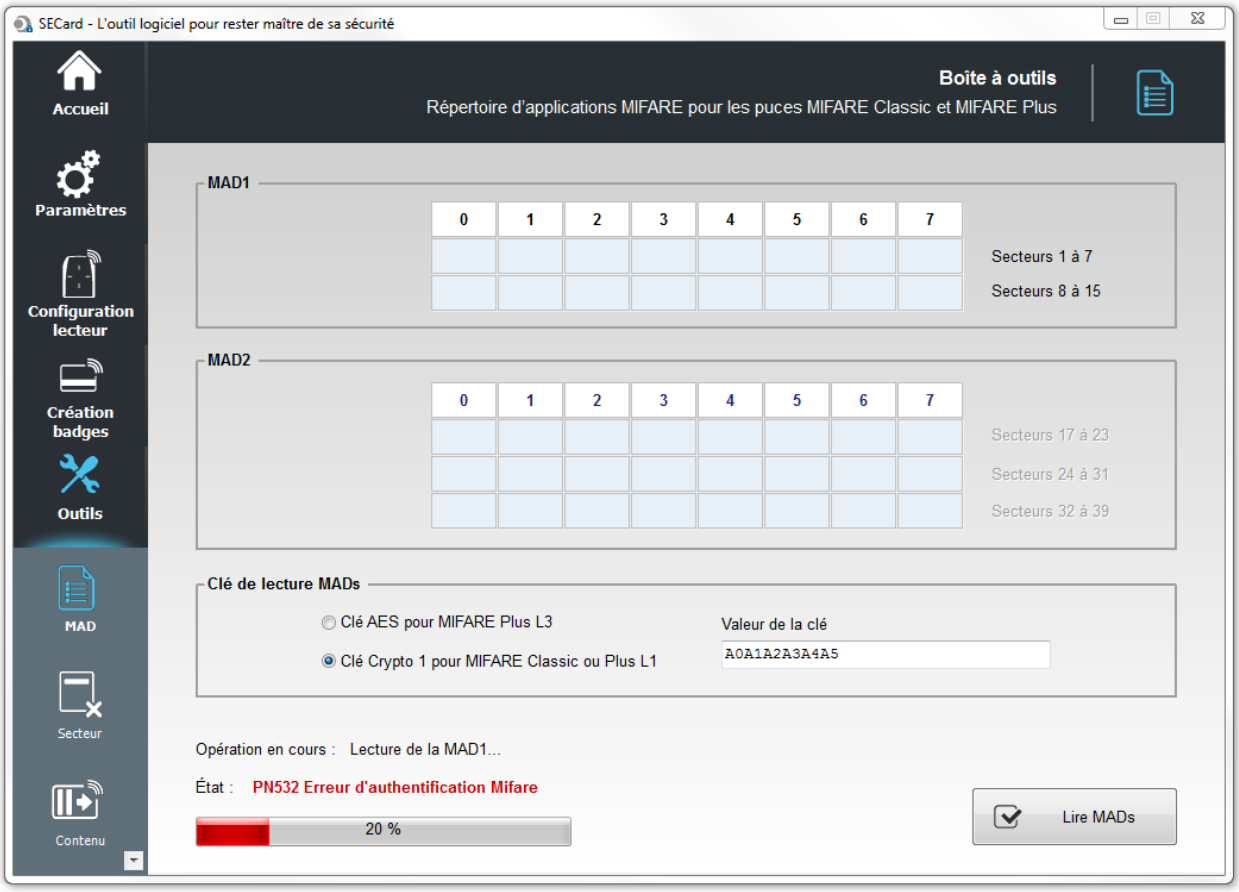
Scan de MAD réussi



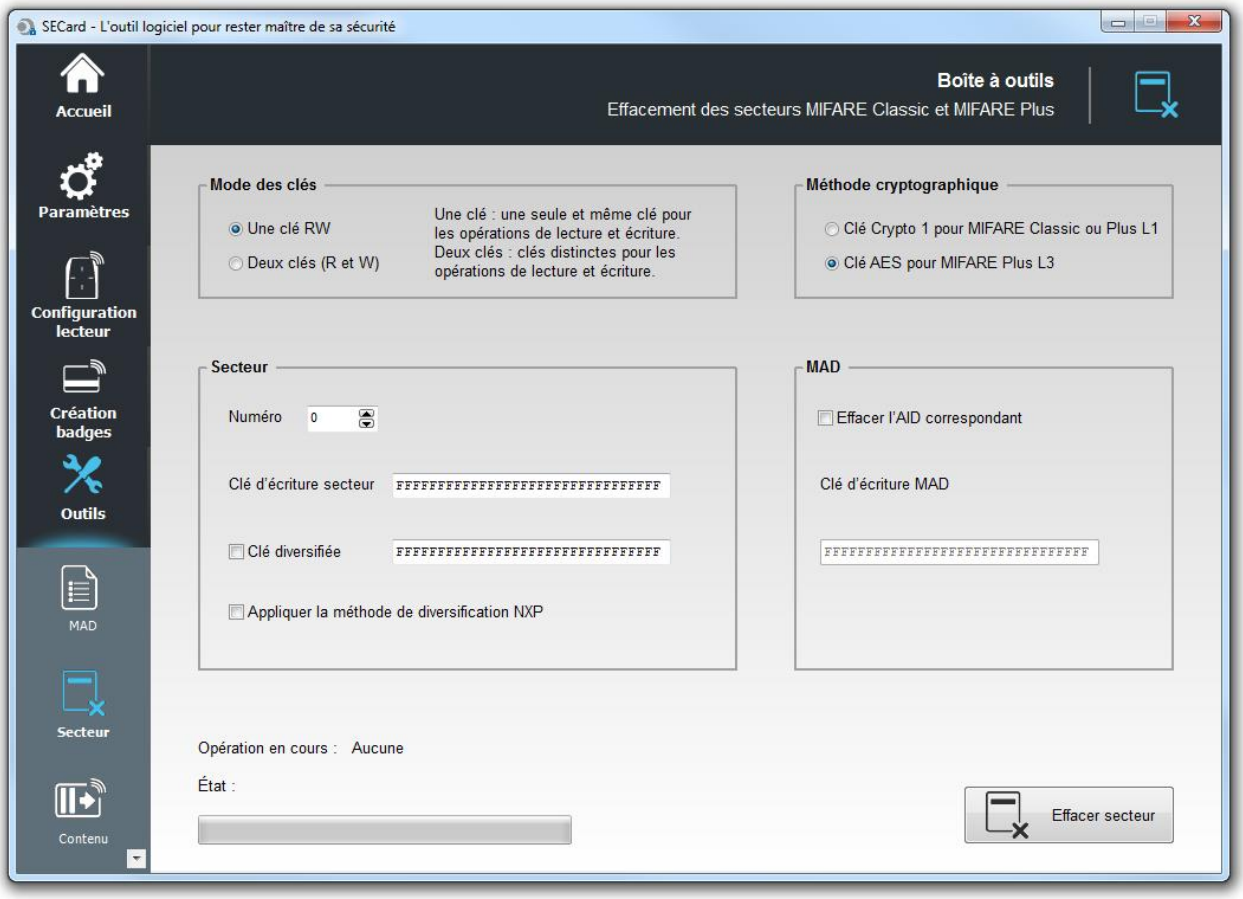
Scan de MAD réussi mais paramètres incorrects

Le CRC+Info encodé n'est pas à la bonne valeur. Effectuer l'encodage avec SECard afin de corriger le problème.

Echec du Scan de MAD : MAD non utilisée ou bien, erreur de clé



VII. 2 - Secteur



Permet d'effacer un secteur d'une MIFARE® Classic ou MIFARE Plus®.

Mode des clés

Permet de choisir le mode dans lequel le secteur à effacer a été encodé : une clé ou deux clés.

Méthode de cryptographie

Permet de choisir la méthode de crypto correspondant au type de puce utilisé.

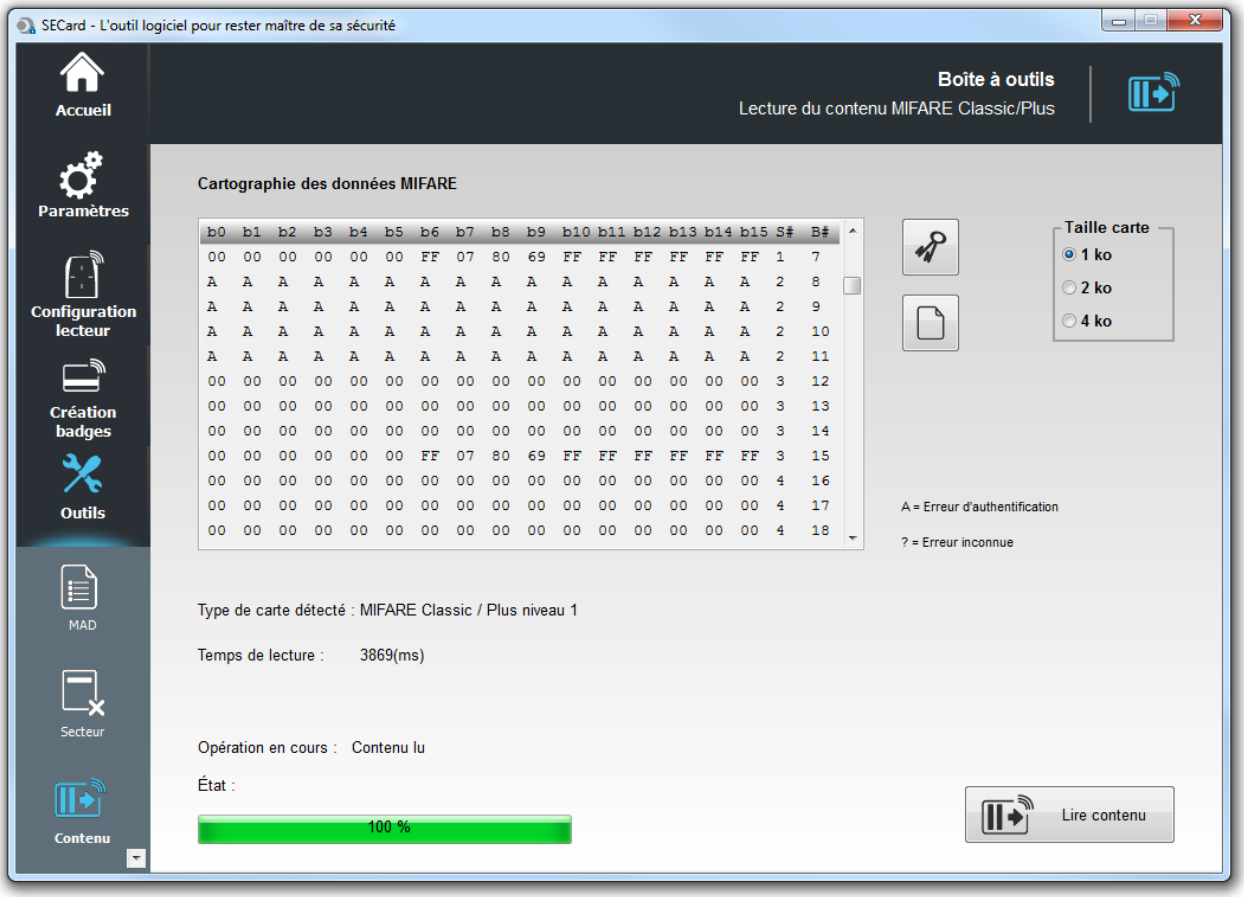
Secteur

Permet de renseigner le numéro du secteur à effacer et sa clé d'écriture.
Il est également nécessaire de cocher la case « *Clé diversifiée* » et de remplir le champ correspondant si l'encodage a été effectué avec une valeur de clé diversifiée (cocher « Appliquer la méthode de diversification NXP» si la diversification a été faite selon cette méthode).

MAD

Il est possible d'effacer l'AID correspondant au secteur dans la MAD. Pour cela, il est nécessaire de cocher la case « *Effacer l'AID correspondant* » et de renseigner la clé d'écriture utilisée pour la MAD.

VII. 3 - Contenu



Permet de lire le contenu d'une MIFARE® Classic ou MIFARE Plus®.

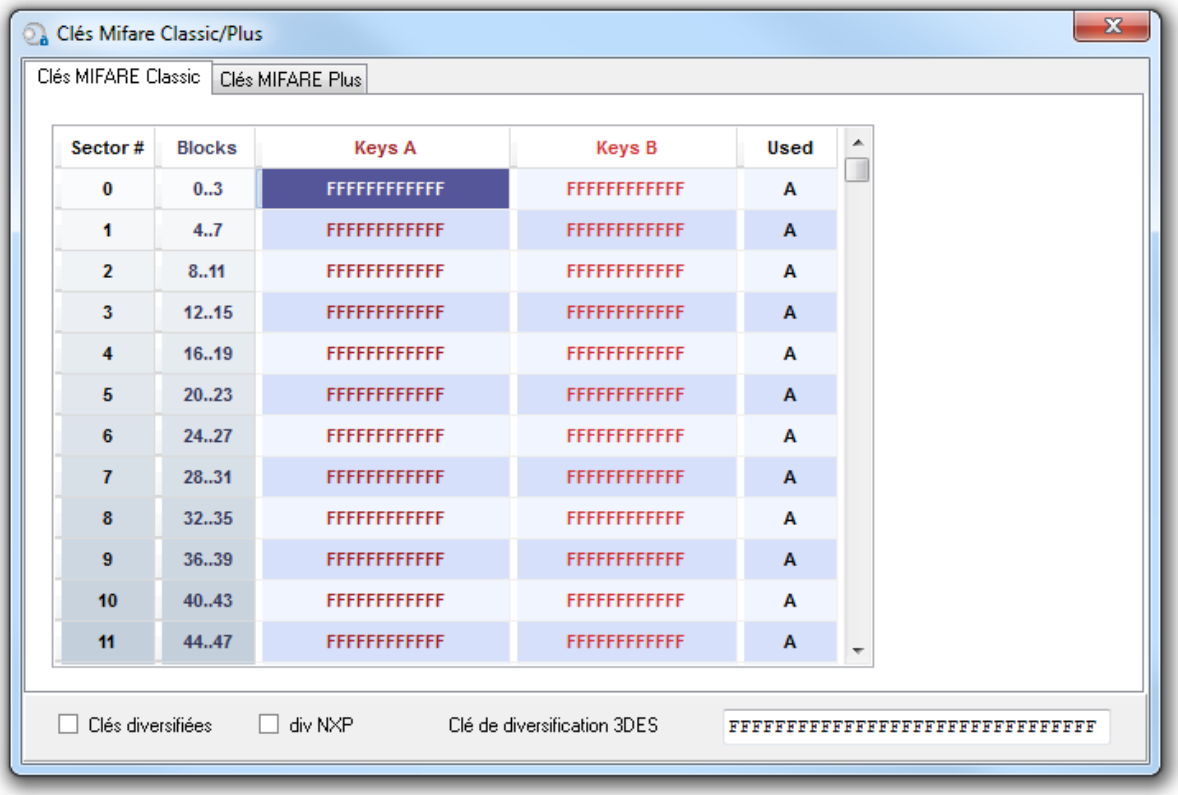
Permet d'effacer le contenu de la fenêtre.

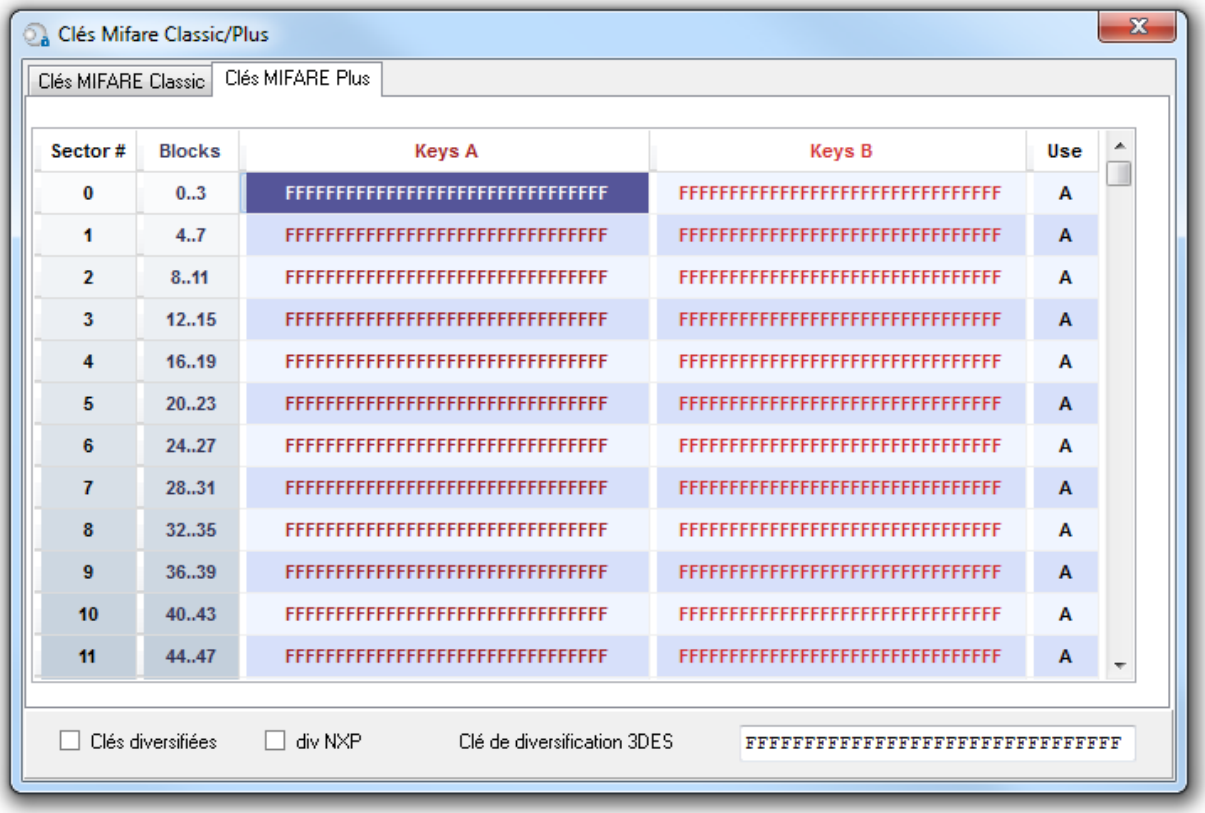
Taille carte

Permet de choisir la taille mémoire de la puce à lire.

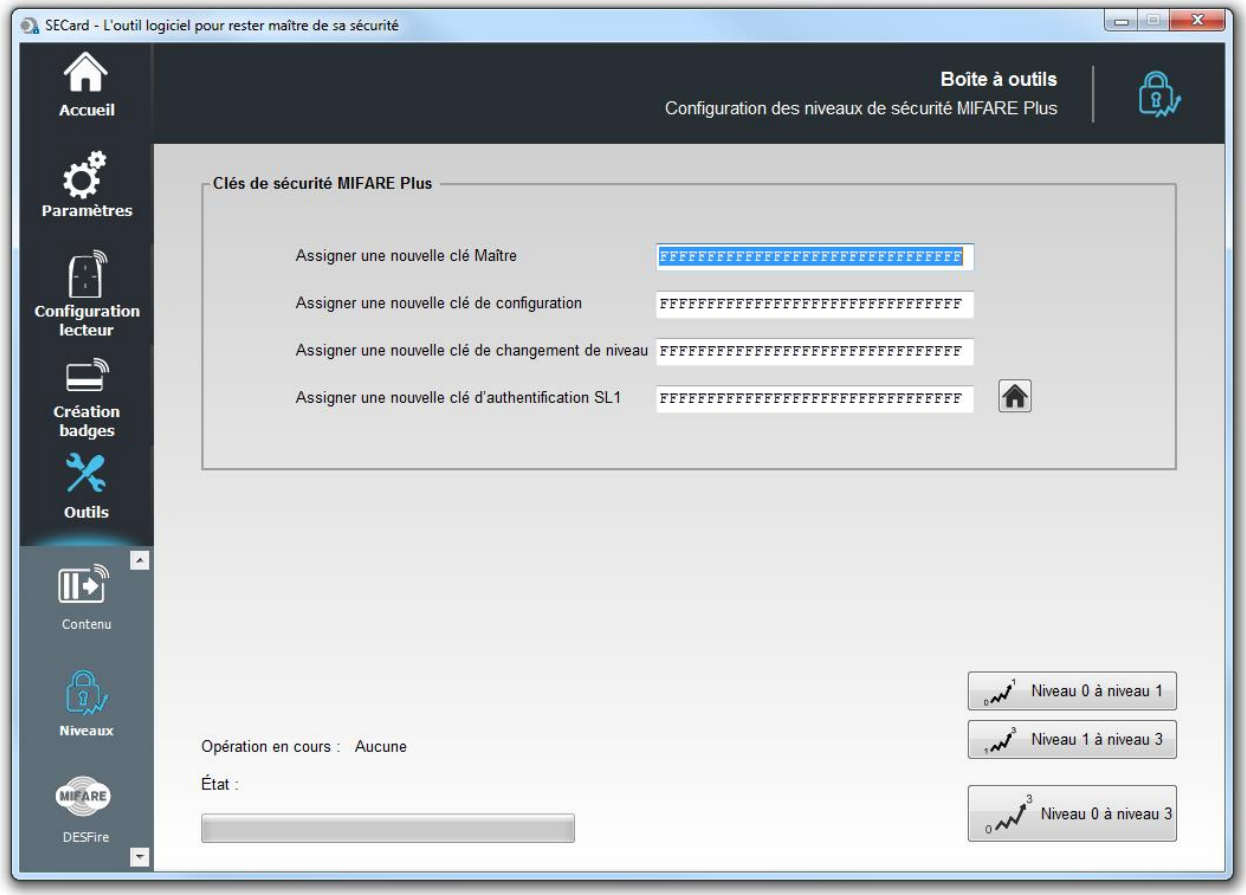
Note : il est possible d'arrêter la lecture en cours en utilisant le bouton « Echap » du clavier.

Permet de renseigner les clés à utiliser pour la lecture du ou des secteurs ainsi que le type de clé (A : clé de lecture/écriture en mode une clé ou B : clé de lecture/écriture en mode deux clés), les options de diversification sont également disponibles :





VII. 4 - Niveaux



Permet de changer manuellement les niveaux de sécurité des puces MIFARE Plus® :

- Niveau 0 (Level 0) vers le niveau 1 (Level 1)
- Niveau 1 (Level 1) vers le niveau 3 (Level 3)
- Niveau 0 (Level 0) vers le niveau 3 (Level 3)

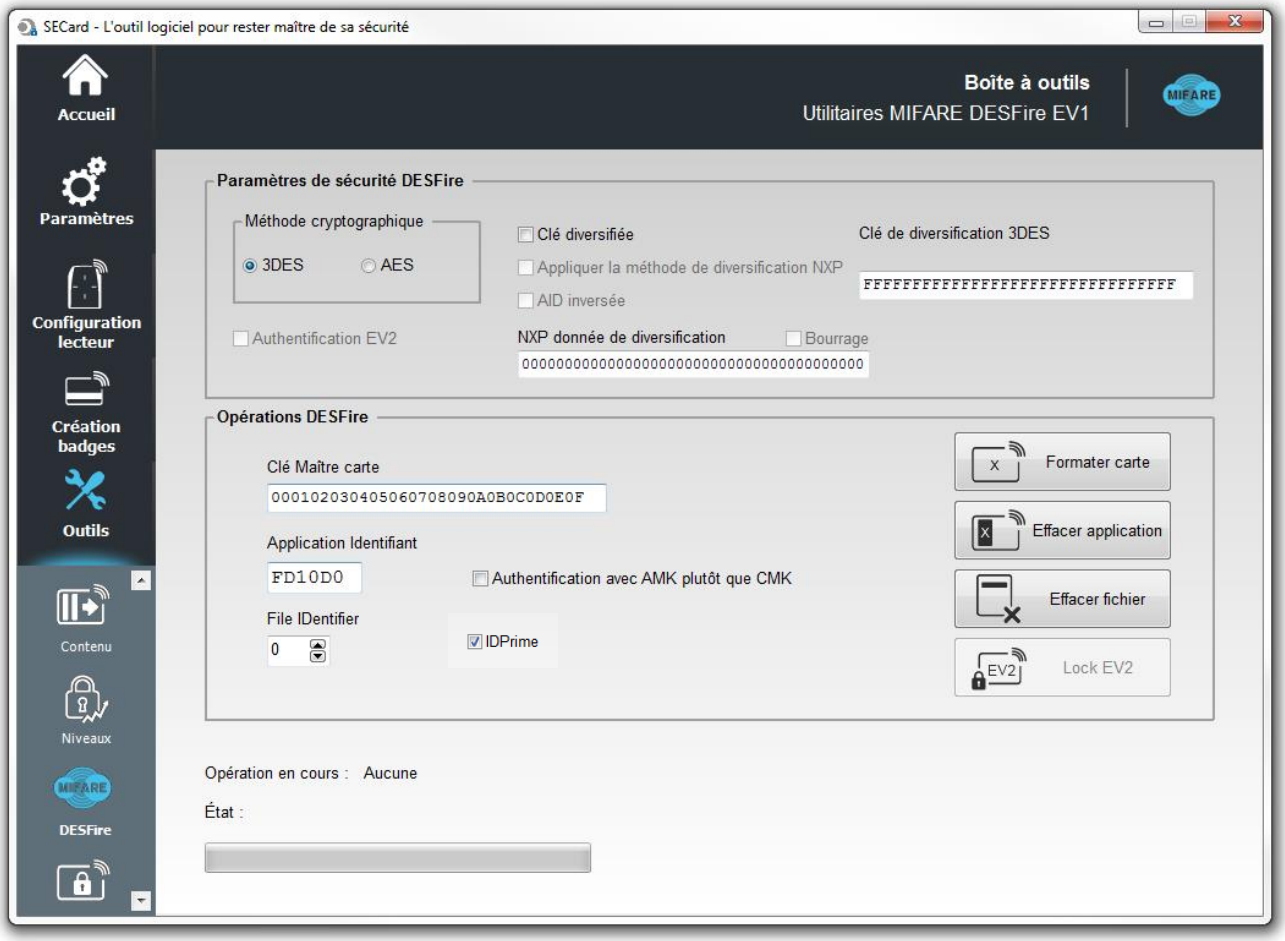
Pour effectuer un changement de niveau, il est nécessaire de renseigner les quatres champs de clés.

Par défaut, les clés d'une puce MIFARE Plus® sont : « FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF », il est recommandé de les modifier afin d'optimiser la sécurité.

Attention

Aucun retour en arrière ne sera possible lors d'un changement de niveau.

VII. 5 - DESFire

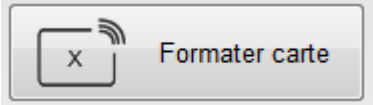
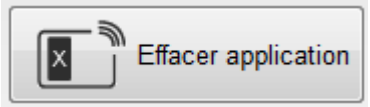


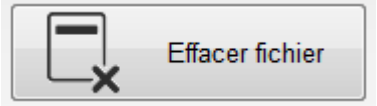
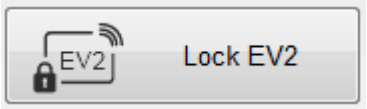
Permet de formater la puce,d'effacer une application créée sur la puce MIFARE® DESFire® EV1/2 ou de supprimer un fichier contenu dans une application.

Paramètres de sécurité DESFire

Permet de choisir la méthode de cryptographie utilisée pour la Clé Maître et de sélectionner les options de diversification éventuelles.

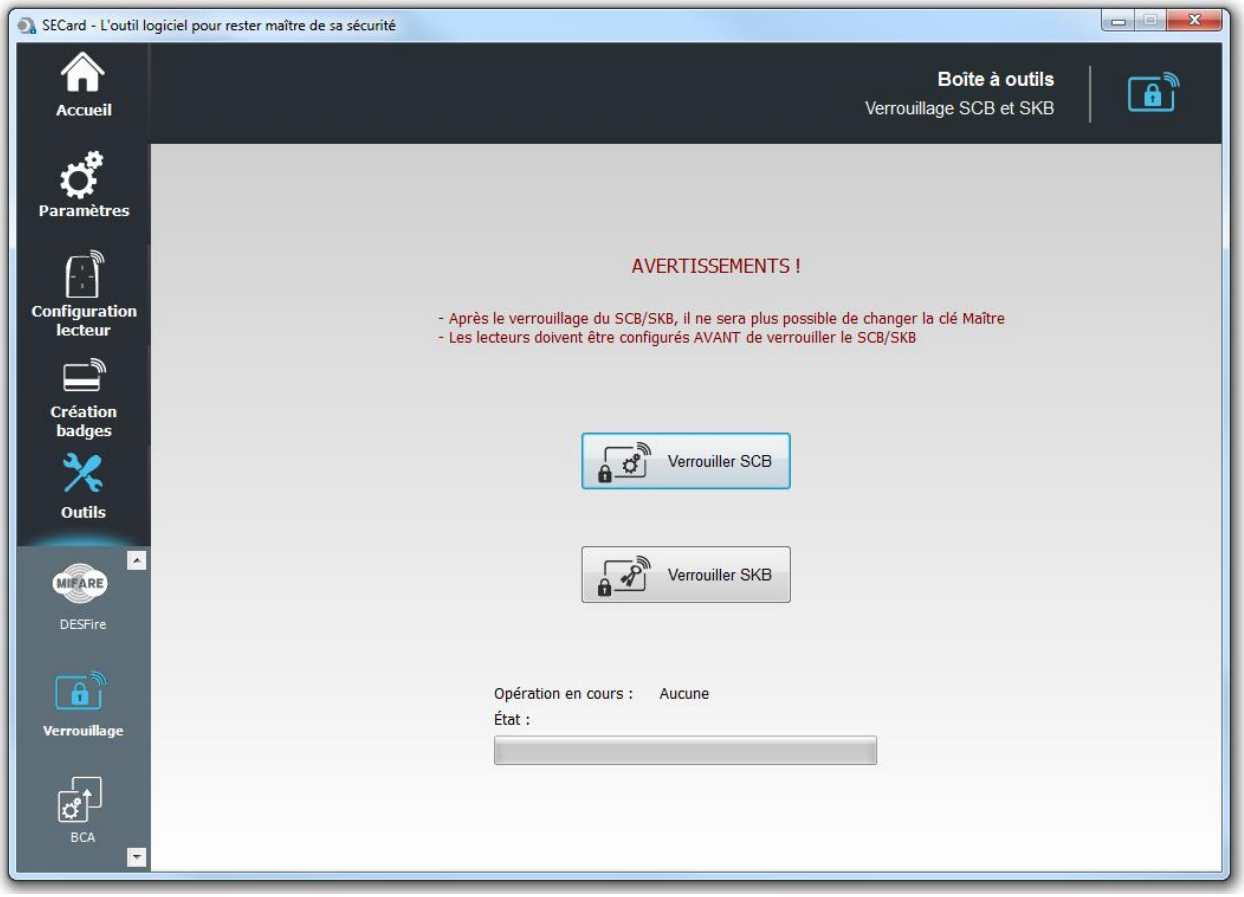
Opérations DESFire

	- Renseigner les paramètres de sécurité de la DESFire (méthode cryptographique, clé diversifiée si Ev2 en Lock Ev2 Authentifdication). - Renseigner la valeur de la Clé Maître carte. **Attention** Lors du formatage toutes les données seront perdues. Le formatage ne modifie pas la clé maître de la puce.
	- Renseigner les paramètres de sécurité de l'application (méthode cryptographique, clé diversifiée si Ev2 en Lock Ev2 Authentifdication). - Renseigner la valeur de la Clé Maître carte ou Clé Maître Application en fonction des settings de votre puce. - Renseigner l'identifiant de l'application AID **Attention** Lors de l'effacement d'une application tous les fichiers inclus seront effacés.

	- Renseigner les paramètres de sécurité de l'application contenant le fichier (méthode cryptographique et si la clé est diversifiée). - Renseigner la valeur de la Clé Maître Application - Renseigner l'identifiant de l'application AID - Renseigner le numéro de fichier à supprimer
	Permet de verrouiller une DESFire EV2 en mode Secure messaging Ev2. La communication avec la puce ne pourra plus alors se faire qu'en Ev2. - Renseigner la valeur de la Clé Maître carte. - Sélectionner la Crypto de la Clé Maître carte. **Attention** Cette action est définitive, aucun retour possible.

Pour un Effacer une aplication ou un fichier sur un badge IDPrime, cocher la case pour forcer la prise en compte de l'émulation DESFire.

VII. 6 - Verrouillage



Permet de verrouiller les badges SCB et SKB, cette action bloque définitivement le changement de la Clé Maître des badges.

Une fois le badge SCB verrouillé, il ne sera possible que de configurer des lecteurs qui ont déjà été configurés avec ce badge de configuration, il ne sera plus possible de configurer des lecteurs en clés usine ou ayant une autre clé.

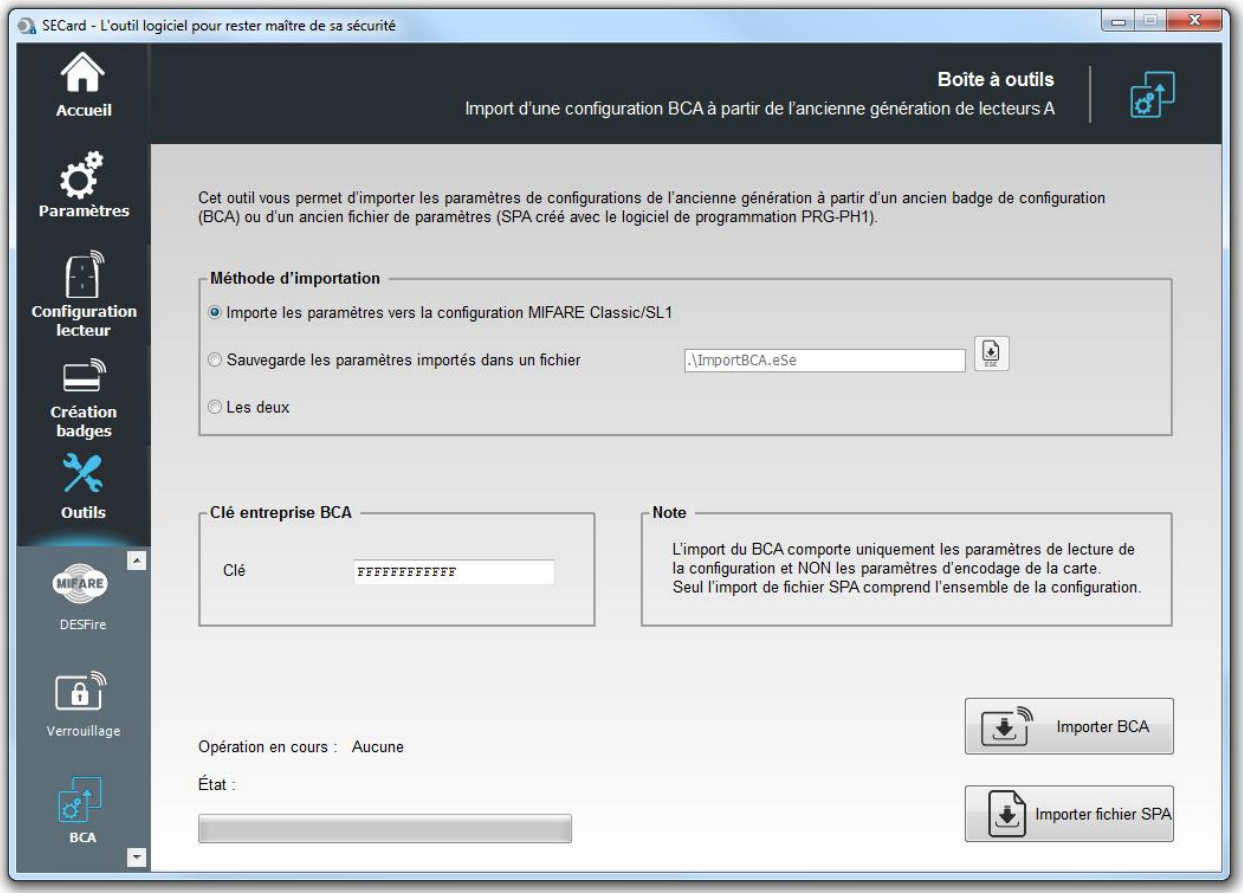
Attention

Avant d'effectuer le verrouillage, il est nécessaire que les lecteurs soient configurés par ces badges. Si cela n'est pas le cas, ces badges seront inutilisables.

Attention

Cette action est définitive, aucun retour possible.

VII. 7 - BCA



Les lecteurs standards nouvelle génération (E) doivent être configurés pour lire un ID privé dans la puce MIFARE® Classic comme sur l'ancienne génération (A).

Deux outils d'import sont proposés selon que l'on possède le badge de configuration BCA ou le fichier de configuration .spa créé dans le logiciel PRG-PH1.
Dans les deux cas, il s'agit uniquement de la configuration MIFARE® Classic.

Méthode d'importation

- Importe les paramètres vers la configuration MIFARE® Classic/SL1 :
  Les paramètres seront renseignés dans l'utilitaire de configuration de badge « Wizard SCB »

- Sauvegarde les paramètres importés dans un fichier de configuration :
  Les paramètres seront sauvegardés dans un fichier .eSe (ImportBCA.eSe par défaut) différent de celui utilisé pour la configuration générale.

- Les deux :
  Les paramètres MIFARE® Classic seront renseignés dans l'utilitaire de configuration de badge « Wizard SCB » et sauvegardés dans un fichier .eSe (ImportBCA.eSe par défaut) différent de celui utilisé pour la configuration générale.

Clé entreprise BCA

Il est obligatoirement nécessaire de connaître la clé entreprise du badge BCA et de la renseigner dans ce champ.
La clé entreprise BCA sur 6 octets sera importée dans le champ Clé entreprise SCB avec un bourrage à zéro à gauche pour atteindre les 16 octets.

Dans le cas d'un badge BCE, les valeurs des clés du badge BCE seront copiées dans le tableau des valeurs lues « Crypto 1 » du badge SKB.

Importer BCA

Permet d'importer **uniquement** les paramètres nécessaires au lecteur pour **lire** les badges utilisateurs.

Attention

Certains paramètres ne sont pas pris en compte (ceux-ci n'étant pas référencés dans le BCA) tels que les changements de clés et les paramètres MAD

Cet import ne permet pas de créer de nouveaux badges utilisateurs.

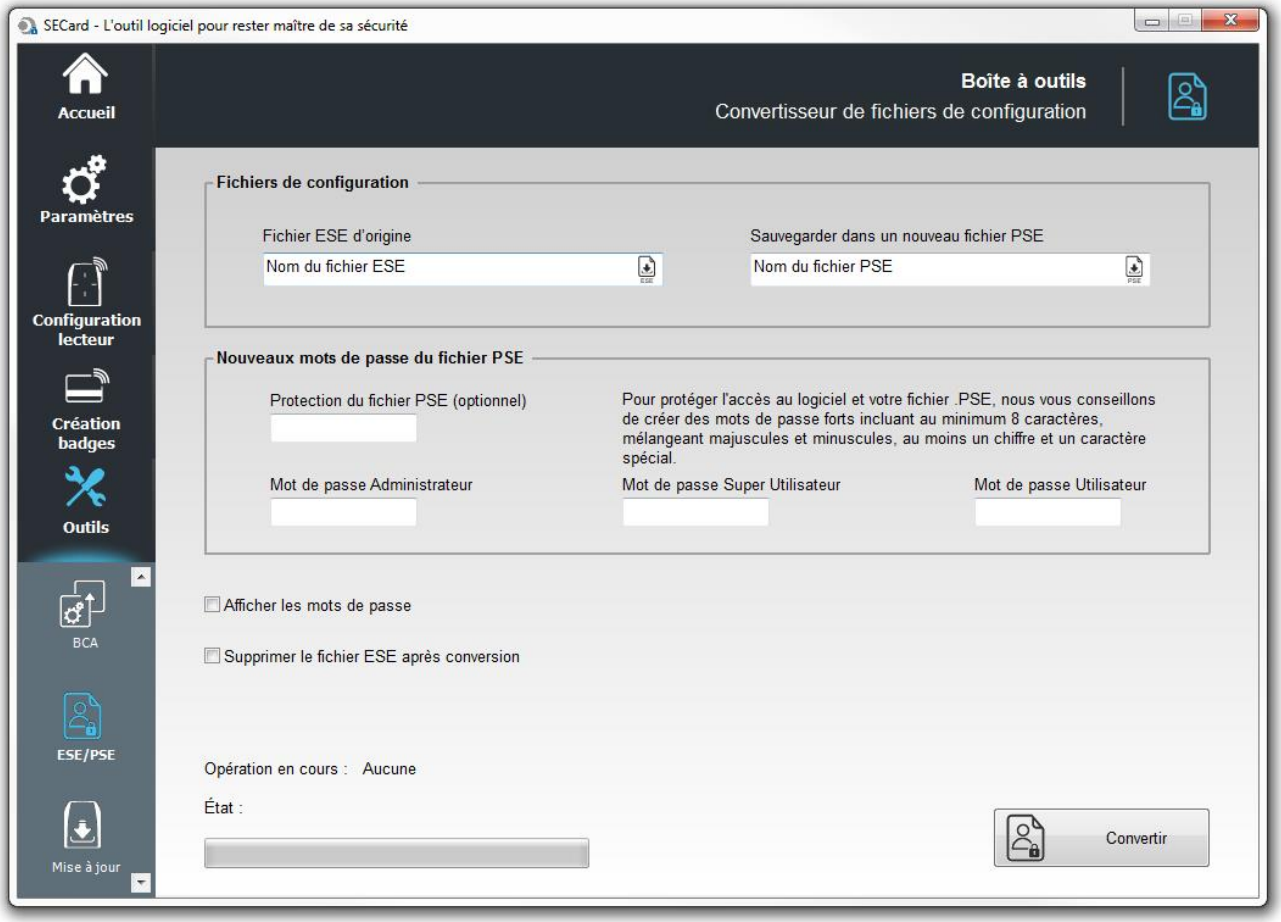
Import SPA

Permet d'importer **tous** les paramètres nécessaires au lecteur pour lire les badges utilisateurs ainsi que tous les paramètres d'écriture nécessaires à la création de nouveaux badges utilisateurs.

Note :

* Les paramètres Secure Plus ne seront pas importés car la fonctionnalité n'existe pas sous cette forme dans SECard.
* Si le fichier .spa est protégé par mot de passe, il sera nécessaire de le renseigner.

VII. 8 - Fichiers ESE/PSE



Les fichiers de configuration créés avec les versions précédentes de SECard étaient des fichiers en « .ese ». A partir de la version V2.0.x le format des fichiers de configuration est « .PSE » Protected SEttings.
Les mots de passe de connexion ainsi que le mot de passe de lecture sont contenus dans ce fichier.

Cet outil permet d'importer les fichiers de configurations « .ese » et de les convertir en « .pse » en y rajoutant les mots de passe de connexion et de lecture.

Fichiers de configuration

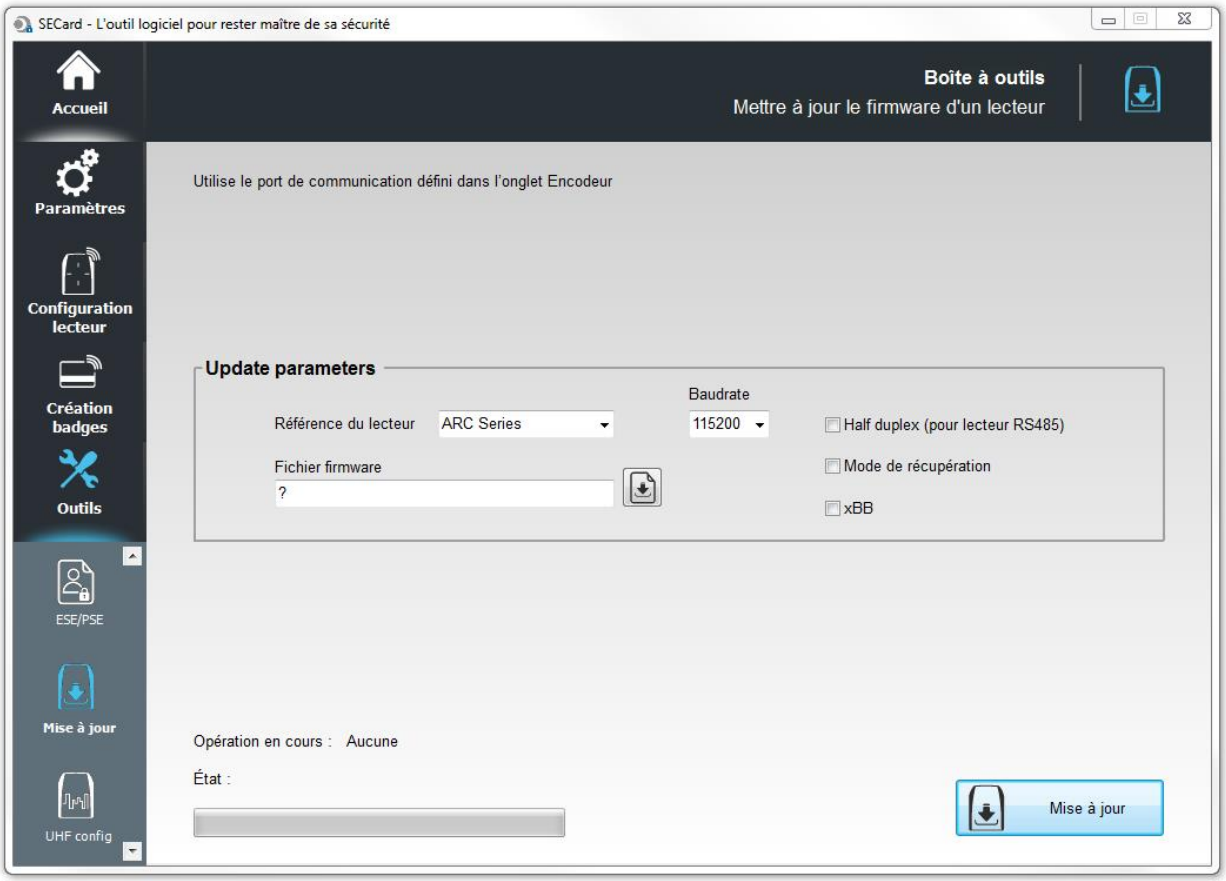
Permet de sélectionner le fichier de configuration .ese à importer et de lui attribuer un nouveau nom en pse.

Nouveaux mots de passe du fichier PSE

Il est obligatoire de renseigner les mots de passe Administrateur, Super Utilisateur et Utilisateur.

Note : cocher « Afficher les mots de passe » avant de cliquer dans un des champs « Mot de Passe ».

VII. 9 - Mise à jour



Permet de mettre à jour le firmware des lecteurs ayant une connectique série.

Attention : nécessite les DLL FlashMagicARM, FlashMagicARMCortex et nrfutil.exe (présentent dans le dossier racine SECard).

Le port de communication utilisé est à renseigner dans l'onglet Paramètres **II.** 1 - Encodeur

Paramètres de mise à jour

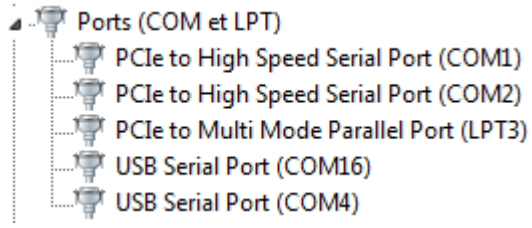
- Référence du lecteur : permet de choisir la référence du lecteur à mettre à jour.
- Baudrate : permet de choisir la vitesse de reprogrammation.
- Fichier firmware : permet de télécharger le fichier du firmware.
- Half Duplex (pour lecteur RS485).
- Mode de récupération : pour les lecteurs R/S 31, si la mise jour a échoué, recommencer l'opération en cochant le mode de récupération.
- xBB : permet la reprogrammation des lecteurs transparents (5BB ou 7BB avec firmware min Z05) .

Quand tous les paramètres ont été renseignés, mettre le lecteur sous tension et cliquer sur le bouton « Mise à jour » :

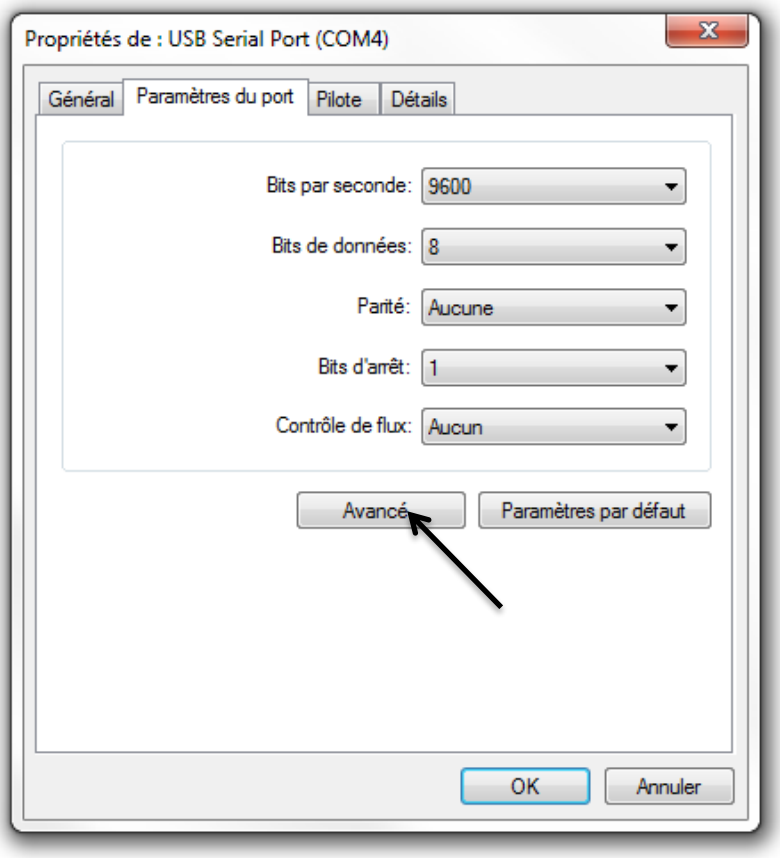
- pendant que la LED clignote en orange pour les lecteurs séries.
- à n'importe quel moment pour les lecteurs TTL.

Note : pour les lecteurs en RS485, utiliser une interface rapide (vitesse par défaut 38400).

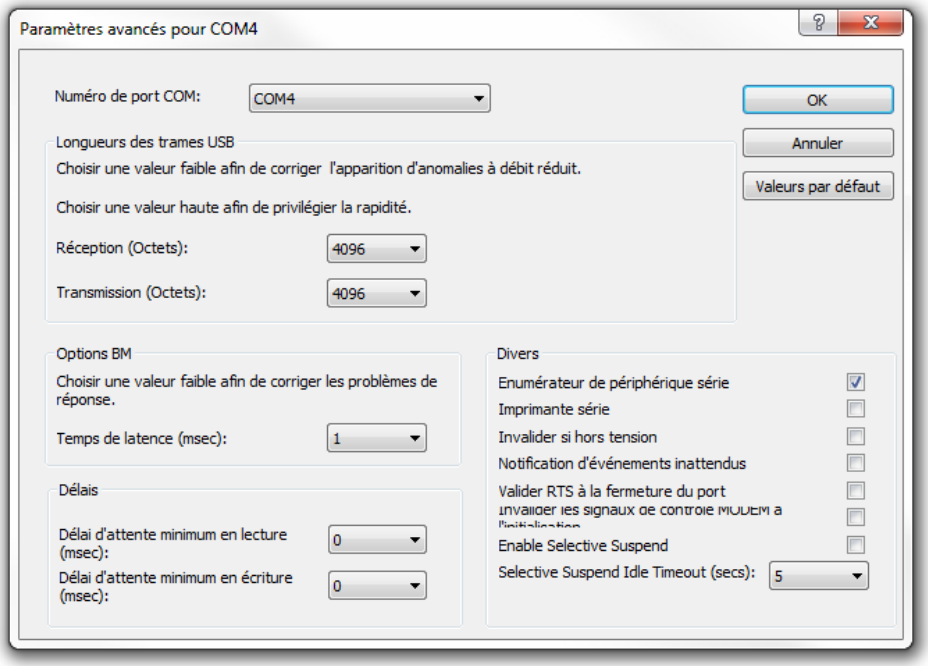
Configuration du port de communication lors de l'utilisions d'un câble convertisseur RS485 / USB :



* Double cliquer sur le port COM correspondant au lecteur.



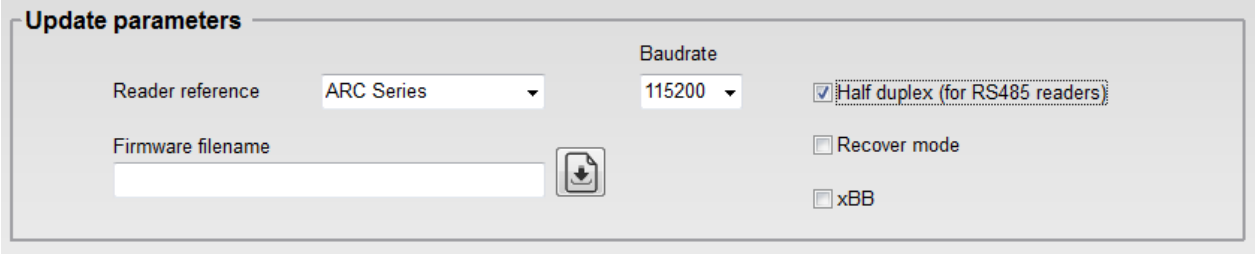
Ouvrir les paramètres Avancé…



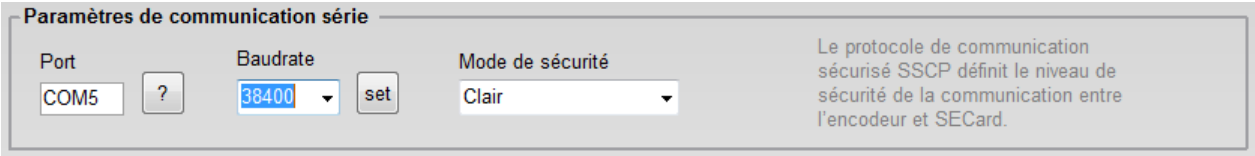
Mettre le temps de latence sur 1

Mise à jour d'un lecteur en lecture/écriture : exemple ARC-W33-A-PH5/7AA

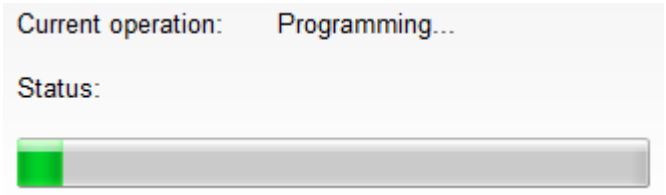
1- Sélectionner ARC series + Half Duplex + charger le bon fichier firmware

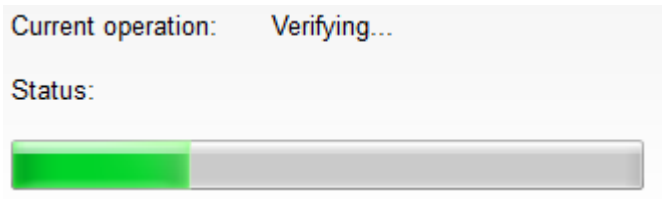


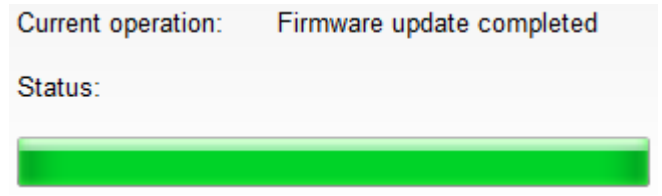
2- Configurer le port COM
Note: pour un lecteur W vous pouvez utiliser CTRL + ?



3- Cliquer sur Mise à jour, la LED devient blanche (sauf pour ARC1/ARC1S la couleur n'est pas définie)

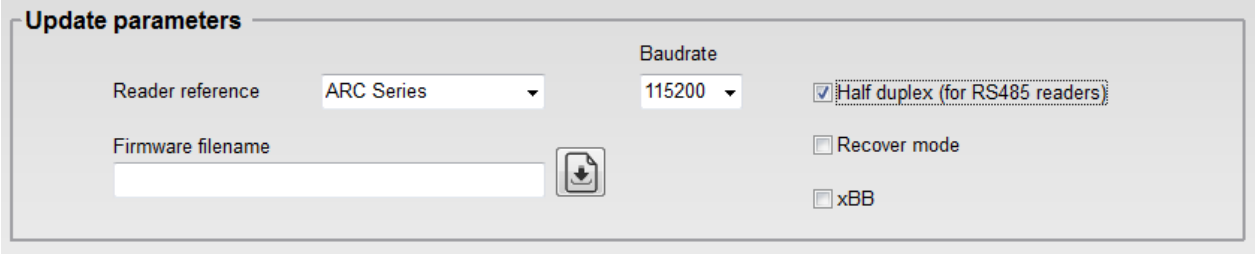




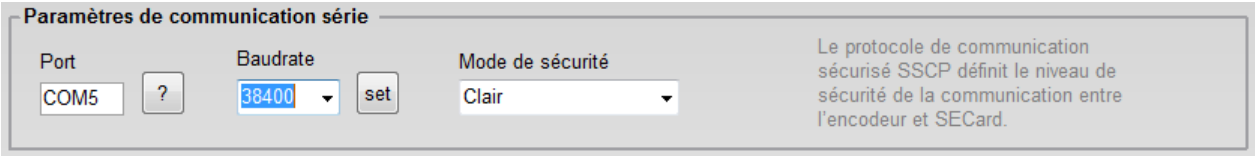


Mise à jour d'un lecteur série : exemple ARC-R33-A-PH5/7AB

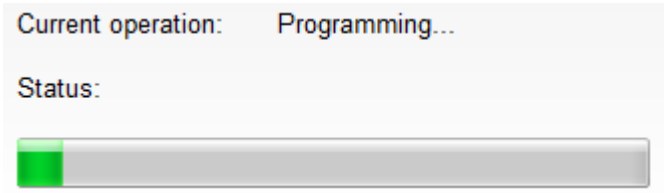
1- Sélectionner ARC series + Half Duplex + charger le bon fichier firmware

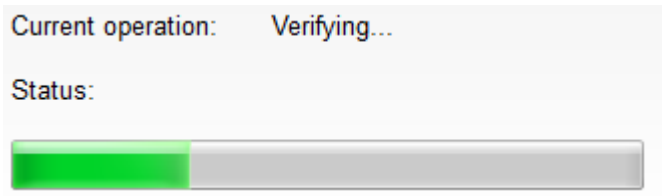


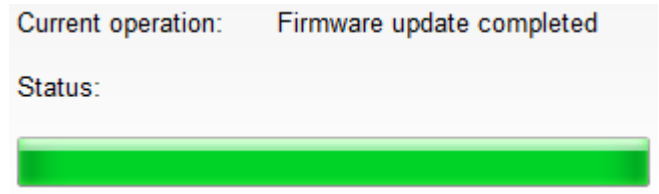
2- Configurer le port COM à 38400



3- Mettre sous tension le lecteur et cliquer sur Mise à jour pendant le clignotement de la LED en orange.

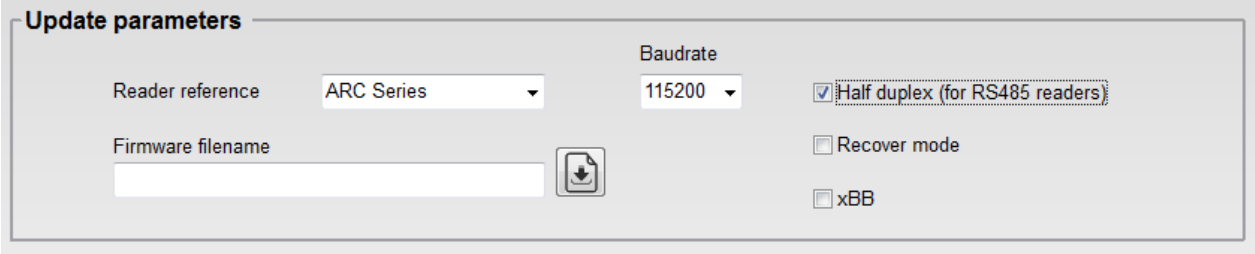




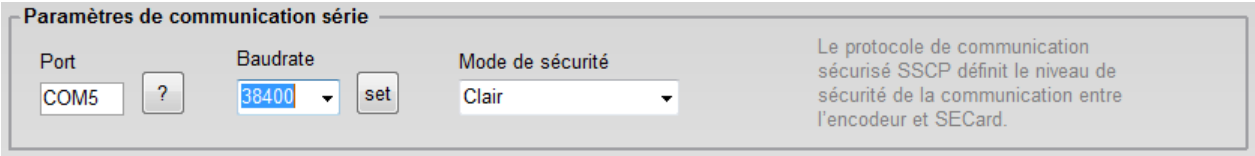


Mise à jour d'un lecteur TTL : exemple ARC-R31-A-PH5/2b

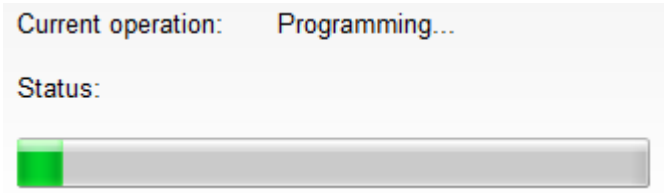
1- Sélectionner ARC series + Half Duplex + charger le bon fichier firmware

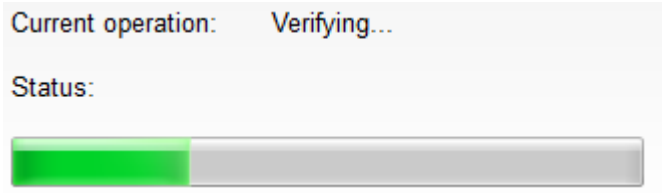


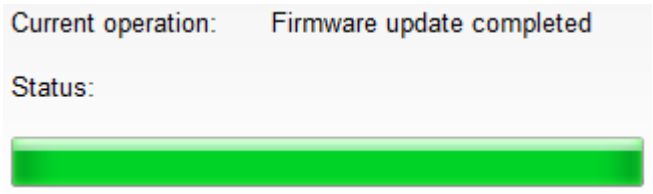
2- Configurer le port COM



3- Cliquer sur Mise à jour

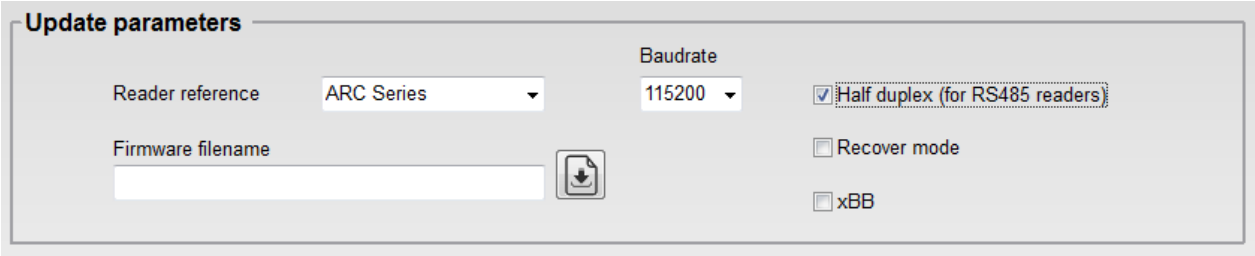




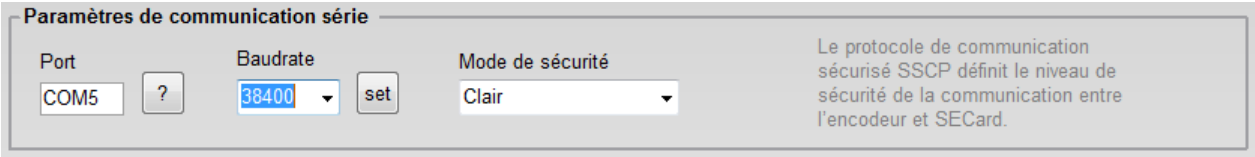


Mise à jour du chip BTSmart : exemple avec ARCS-R31-A-BT1/xx

1- Sélectionner ARCS-nRF51 + Half Duplex + charger le bon fichier

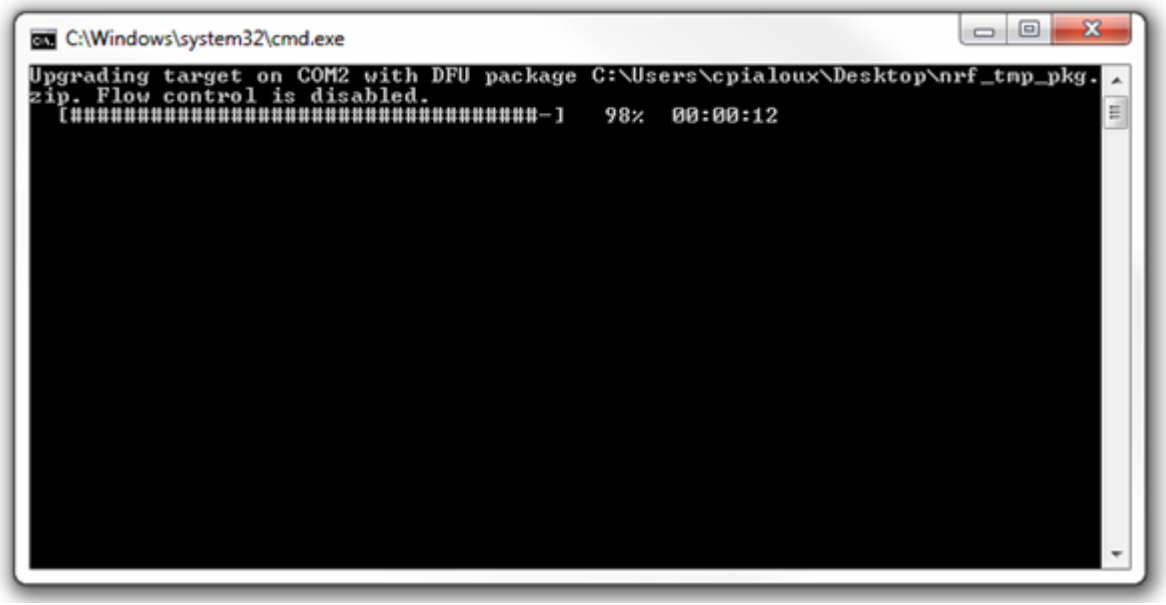


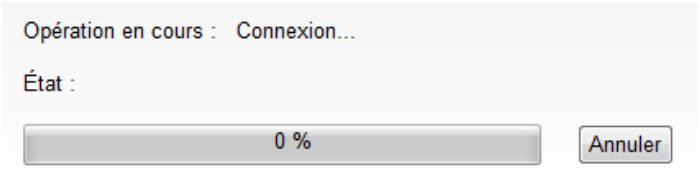
2- Configurer le port COM

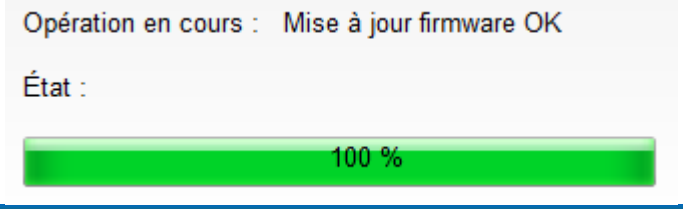


3- Cliquer sur Mise à jour

Une fenêtre DOS s'ouvre :

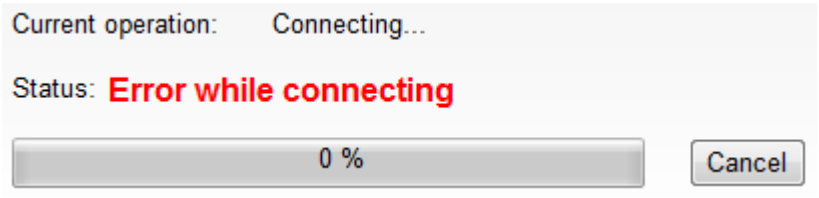






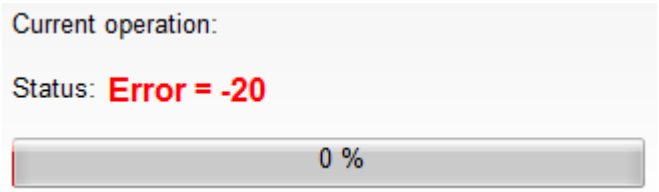
Message d'erreur

❖



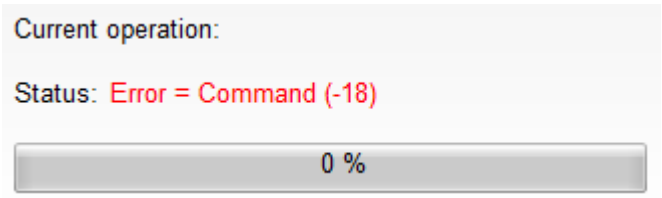
- Vérifier le numéro de port COM
- Vérifier le Baudrate
- Cliquer sur Mise à jour pendant que la LED orange clignote pour un lecteur série.

❖ Durant la mise à jour si la communication venait à être interrompue ou si l'alimentation éteinte le message ci-dessous apparait :



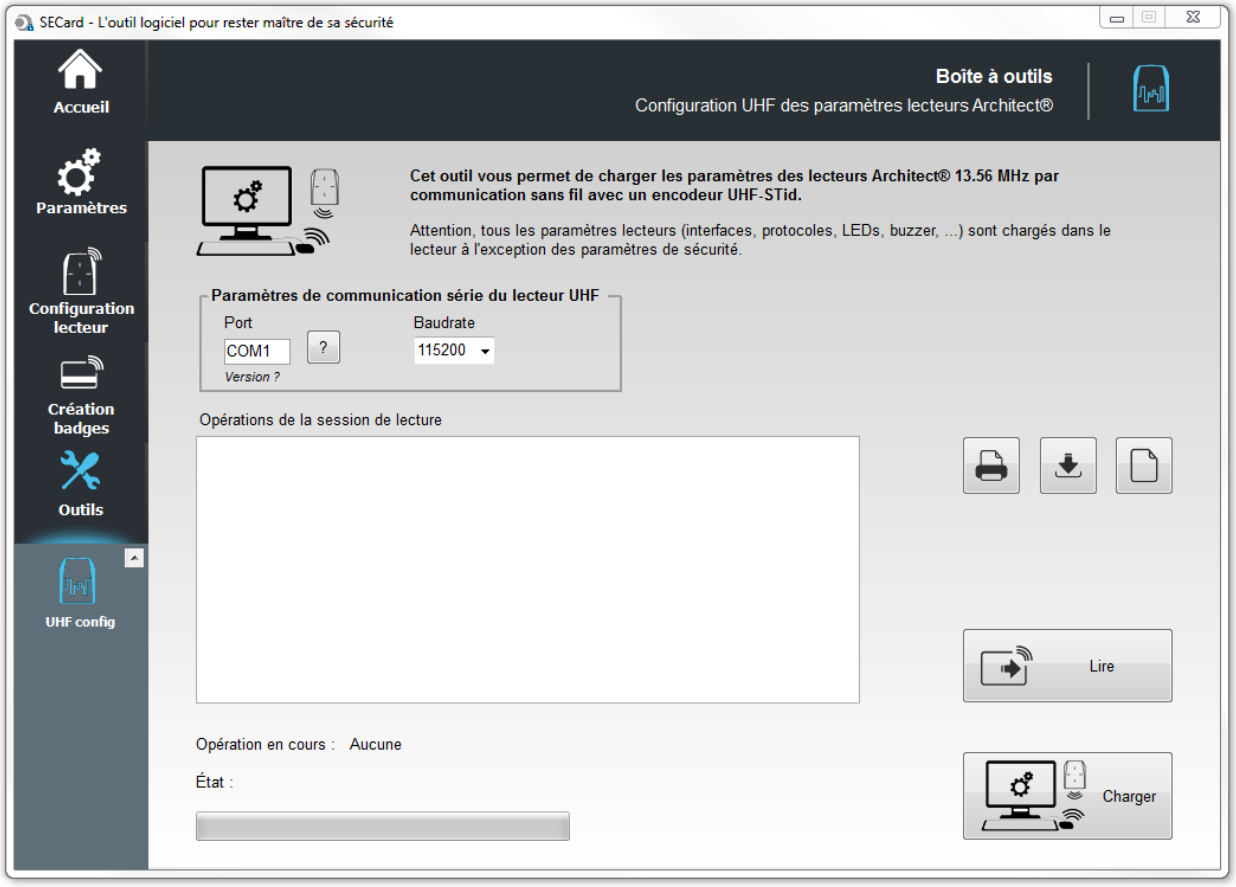
Dans ce cas il est nécessaire d'éteindre le lecteur, de sélectionner "Mode de récupération", de remettre le lecteur sous tension et de cliquer à nouveau sur Mise à jour.

❖



- Vérifier que la DLL FlashMagicARM et/ou FlashMagicARMCortex sont présentes dans le dossier d'installation de SECard.

VII. 10 - UHF config



Permet d'écrire / lire les paramètres lecteurs de la configuration courante de SECard dans la puce UHF d'un lecteur ARC.

Aucune clé ni aucun élément de sécurité n'est géré par cette fonctionnalité.

L'utilitaire utilise la clé UHF renseignée dans les paramètres lecteurs) pour écrire de manière sécurisée dans la mémoire de la puce.

	Permet d'imprimer les opérations réalisées.
	Permet de sauvegarder les opérations réalisées.
	Permet d'effacer la liste des opérations réalisées.

Renseigner le port et la vitesse de communication du lecteur UHF.

Attention

La lecture / écriture de la puce UHF ne peut se faire que si le lecteur ARC est hors tension. Cette opération est réalisée par le biais d'un lecteur UHF STid.

Lorsque le lecteur est sous tension la puce UHF est automatiquement désactivée.

SECARD

MANUEL UTILISATEUR

Partie 2 : Technique

www.stid.com

T1- Lecteurs configurables par SECard

Le logiciel SECard dispose de modules de création de badges de configuration (SCB) permettant de configurer en fonction des paramètres de sécurité tous les lecteurs de la gamme Architect® et WAL.

Pour les autres lecteurs de la gamme STid 13.56 MHz se reporter aux tableaux suivants :

GAMME LXS, LXE, LX1, LDS, STR, WAL, MS, MXS, ATX		
Références des produits	**Désignation**	**Interface**
LXS / LXE / /WAL / MXS / ATX - R31-E/103-xx	Lecture de numéro de série	Liaison Wiegand ou Clock&Data
LXS / LXE / /WAL / MXS / ATX - R31-E/PH5-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand ou Clock&Data
LXS / LXE / /WAL / MXS / ATX - S31-E/PH5-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand chiffrée par un AES 128 bits
LXS / LXE / /WAL / MXS / ATX - R32-E/PH5-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS232
LXS / LXE / /WAL / MXS / ATX - S32-E/PH5-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS232 chiffrée par un AES 128 bits et signée
LXS / LXE / /WAL / MXS / ATX - R33-E/PH5-7AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS485
LXS / LXE / /WAL / MXS / ATX - S33-E/PH5-7AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS485 chiffrée par un AES 128 bits et signée
MS-R31-E/103-xx	Lecture de numéro de série	Liaison Wiegand ou Clock&Data
MS-R31-E/PH5-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand ou Clock&Data
MS-R32-E/PH5-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS232-TTL
MS-S31-E/PH5-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand chiffrée par un AES 128 bits
MS-S31-E/PH5-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS232 chiffrée par un AES 128 bits et signée
LXC / CLA-R31-E/G/103-xx	Lecture de numéro de série	Liaison Wiegand ou Clock&Data
LXC / CLA-R31-E/G/PH5-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand ou Clock&Data
LXC / CLA-S31-E/G/PH5-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand chiffrée par un AES 128 bits
LXC / CLA-R32-E/G/PH5-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS232
LXC / CLA-S32-E/G/PH5-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS232 chiffrée par un AES 128 bits et signée
LXC / CLA-R33-E/G/PH5-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS485
LXC / CLA-S33-E/G/PH5-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS485 chiffrée par un AES 128 bits et signée

Références des produits	Désignation	Interface
INT-E-7AA/7AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS485 chiffrée par un AES 128 bits (nécessite un lecteur LXS / LXE / LXC-S33-E-PH5-7AA)
INT-R33-E/PH5-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand chiffrée par un AES 128 bits (nécessite un lecteur
LX1-R31-E/103-xx	Lecture de numéro de série	Liaison Wiegand ou Clock&Data
LX1-R31-G/103-xx	Lecture de numéro de série	Liaison Wiegand ou Clock&Data
*LX1-R31-E/PH1-xx	Lecture de numéro de série et/ou d'un numéro privé MIFARE®Classic	Liaison Wiegand ou Clock&Data
*LX1-R31-G/PH1-xx	Lecture de numéro de série et/ou d'un numéro privé MIFARE®Classic	Liaison Wiegand ou Clock&Data
LX1-R31-G/PH5-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand ou Clock&Data
LX1-S31-G/PH5-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand chiffrée par un AES 128 bits
LDS-R31-E/PH5-xx	Lecture de numéro de série et/ou de numéro privé ET d'empreintes digitales	Liaison Wiegand ou Clock&Data
LDS-S31-E/PH5-xx	Lecture de numéro de série et/ou de numéro privé ET d'empreintes digitales	Liaison Wiegand ou Clock&Data
STR-R3x/PH5-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS232 (R32) ou USB (R35)
STR-S3x/PH5-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS232 (S32) ou USB (S35) chiffrée par un AES 128 bits et signée
LXS-R31-E/BF5/BF6-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand ou Clock&Data
LXS -R32-E/BF5/BF6-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS232
LXS -R33-E/BF5/BF6-7AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS485
LXS -S31-E/BF5/BF6-xx	Lecture de numéro de série et/ou de numéro privé	Liaison Wiegand chiffrée par un AES 128 bits
LXS -S32-E/BF5/BF6-5AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS232 chiffrée par un AES 128 bits et signée
LXS -S33-E/BF5/BF6-7AB	Lecture de numéro de série et/ou de numéro privé	Liaison série RS485 chiffrée par un AES 128 bits et signée
WP3/4-R3X-A/PH5	Lecture de numéro de série et/ou de numéro privé	Version Socle
WP3/4-R3X-B/PH5	Lecture de numéro de série et/ou de numéro privé	Liaison WIFI

***** *Se référer à T2.3 - Lecteur LX1 pour plus d'informations sur les possibilités du lecteur LX1/PH1.*

T2 - Au sujet des lecteurs

T2.1 - Mise sous tension

A la mise sous tension, le lecteur est en phase d'initialisation :

1) Activation de la LED orange pour les lecteurs standards ou de la LED blanche pour les lecteurs Architect® et WAL et du buzzer pendant 100 ms.

2) Activation de la LED et du buzzer pour indication de la version firmware et du type de lecteur selon le code ci-dessous.

3) Clignotement de la LED orange 20 fois (attente de mise à jour). **Disponible uniquement sur les lecteurs RS232, RS485 et USB**.

4) Pour les ARCS Blue uniquement : Activation de la LED blanche fixe durant l'initialisation du Bluetooth.

Après la phase d'initialisation la version du firmware est indiquée par LED suivant le code couleur :

Rouge = +10
Orange = +5
Verte = +1
La version du firmware doit correspondre à l'indication inscrite sur l'étiquette au dos du lecteur.

Et le type de lecteur est indiqué par le buzzer suivant le code (ne pas tenir compte du premier entendu qui correspond au 100ms de la phase d'initialisation) :

Bip long = +5
Bip court = +1

En additionnant les BIP entendus (exemple 1 long + 1 court = 6) on obtient le type du lecteur selon le tableau de correspondance ci-dessous :

Somme des BIP	Type Lecteur
1	R31/103 & Lecteur+INT-R33F/103
2	R31/PH1 uniquement ARC1
3	R31/PH5 & R31/PH1 & Lecteur+INT-R33F/PH5
4	S31/PH5 & Lecteur+INT-S33F/PH5
5	Lecteur+INT-R33-E/PH5
6	R32/PH5 & R35/PH5 & R33/PH5
7	S32/PH5 & S35/PH5 & S33/PH5
8	Lecteur+INT-E-7AA/7AB
9	R33/PH1 uniquement ARC1

T2.2 - Configuration des lecteurs

Les lecteurs R31 en 103 ne prennent le SCB qu'au démarrage après la phase d'initialisation. Il faut donc mettre le lecteur hors tension, présenter le SCB et remettre sous tension.
Les autres lecteurs prennent le SCB sans redémarrage.

Pour indiquer que la configuration a été chargée le lecteur émet 5 bips rapidement et la LED verte clignote rapidement.

A partir de la version firmware U16 pour les lecteurs séries standards et pour tous les lecteurs Architect® séries, lors de la configuration le lecteur donne des indications sur la prise en compte ou non du SCB :

- Si la version du SCB est supérieure à la version de SCB définie dans le firmware :
  ➔ La LED rouge est activée et le buzzer est activé 1 seconde.

- Si la version du SCB est compatible à la version de SCB définie dans le firmware :
  ➔ La LED verte est activée et le buzzer émet cinq BIP rapidement.

T2.3 - Lecteur LX1

❖ Les références spécifiques LX1-R31-E/PH1-xx et LX1-R31-G/PH1-xx peuvent lire :

- MIFARE® Classic - Lecture d'un numéro de série UID et d'un ID privé
- MIFARE Plus® - Lecture d'un numéro de série UID seulement
- MIFARE® DESFire® EV1 - Lecture d'un numéro de série UID seulement
- MIFARE Ultralight® C - Lecture d'un numéro de série UID seulement
- CPS3 - Lecture d'un numéro de série UID et d'un ID contenu dans un Elementary File
- ISO14443-3B - Lecture du PUPI

Disponible : Signal de vie

Non disponible : Signal d'arrachement
Entrée Switch
MIFARE Plus® Level 1 avec authentification AES SL1
Lecture d'un ID privé sur MIFARE Plus®, MIFARE® DESFire® EV1 et MIFARE Ultralight® C

Si un badge SCB contient une configuration demandant une lecture d'un ID Privé AES/3DES (exemple : pour une puce MIFARE® DESFire® Ev1), le lecteur configuré ainsi ne lira pas la puce concernée.

❖ Les autres références LX1-R31-G/103-xx et LX1-R31-G/PH5-xx ont les mêmes fonctionnalités que les autres lecteurs.

T2.4 - Lecteur ARC1

❖ Les références spécifiques ARC1-R31-A/PH1-xx et ARC1-R31-B/PH1-xx peuvent lire :

- MIFARE® Classic - Lecture d'un numéro de série UID et d'un ID privé
- MIFARE Plus® - Lecture d'un numéro de série UID seulement
- MIFARE® DESFire® Ev1 - Lecture d'un numéro de série UID seulement
- MIFARE Ultralight® C - Lecture d'un numéro de série UID seulement
- CPS3 - Lecture d'un numéro de série UID et d'un ID contenu dans un Elementary File
- ISO14443-3B - Lecture du PUPI

❖ Les autres références de l'ARC1 lisent les mêmes puces que les autres lecteurs.

A noter :

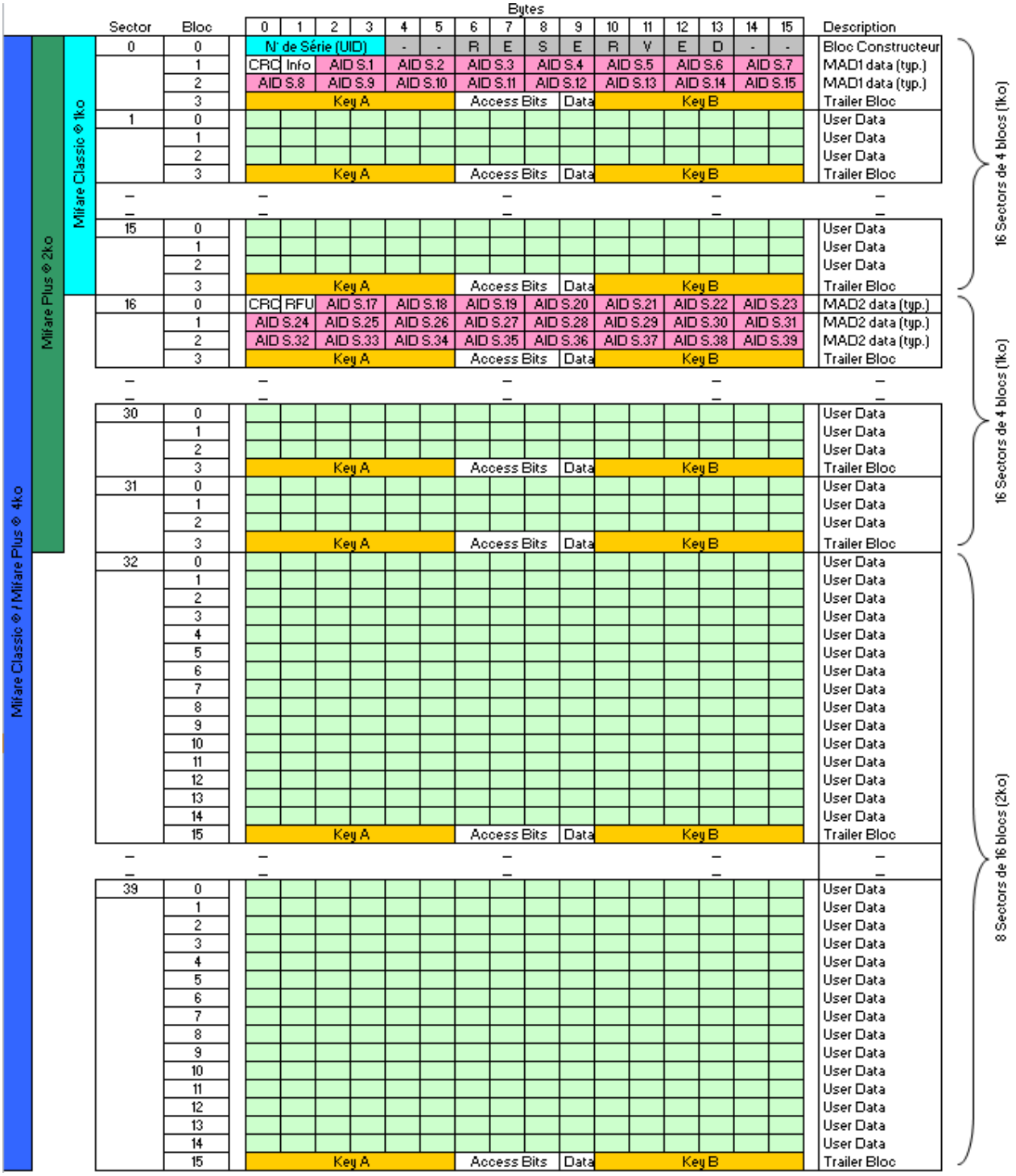
Le lecteur ARC One se configure comme un lecteur ARC hormis dans ces trois cas :

- si le mode Pulse est sélectionné, la LED de l'ARC1 sera fixe sur la couleur sélectionnée.
- si le mode ECO est sélectionné, seul le temps de Scan sera impacté (pas d'impact sur la luminosité de la LED).
- si les options Biométrie, Clavier et/ou Ecran sont activées, elles ne seront pas prises en compte.

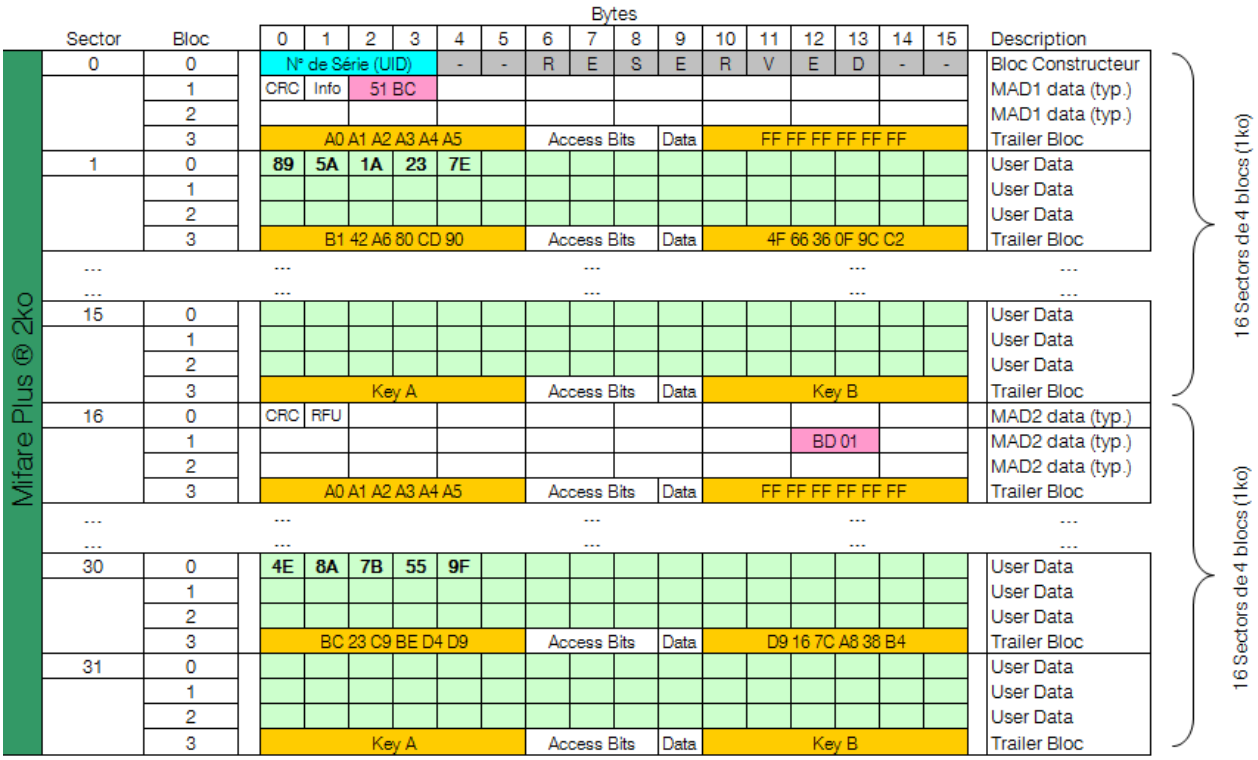
T3 - Au sujet des puces

T3.1 - Organisation de la mémoire des puces MIFARE® Classic et MIFARE Plus®

Plan mémoire global



Exemple de mémoire découpée : MIFARE Plus® Level 1



Dans le cas ci-dessus, la mémoire de la puce MIFARE Plus® Level 1 contient deux informations encodées dans le secteur 1 et 30, protégés par des clés différentes.

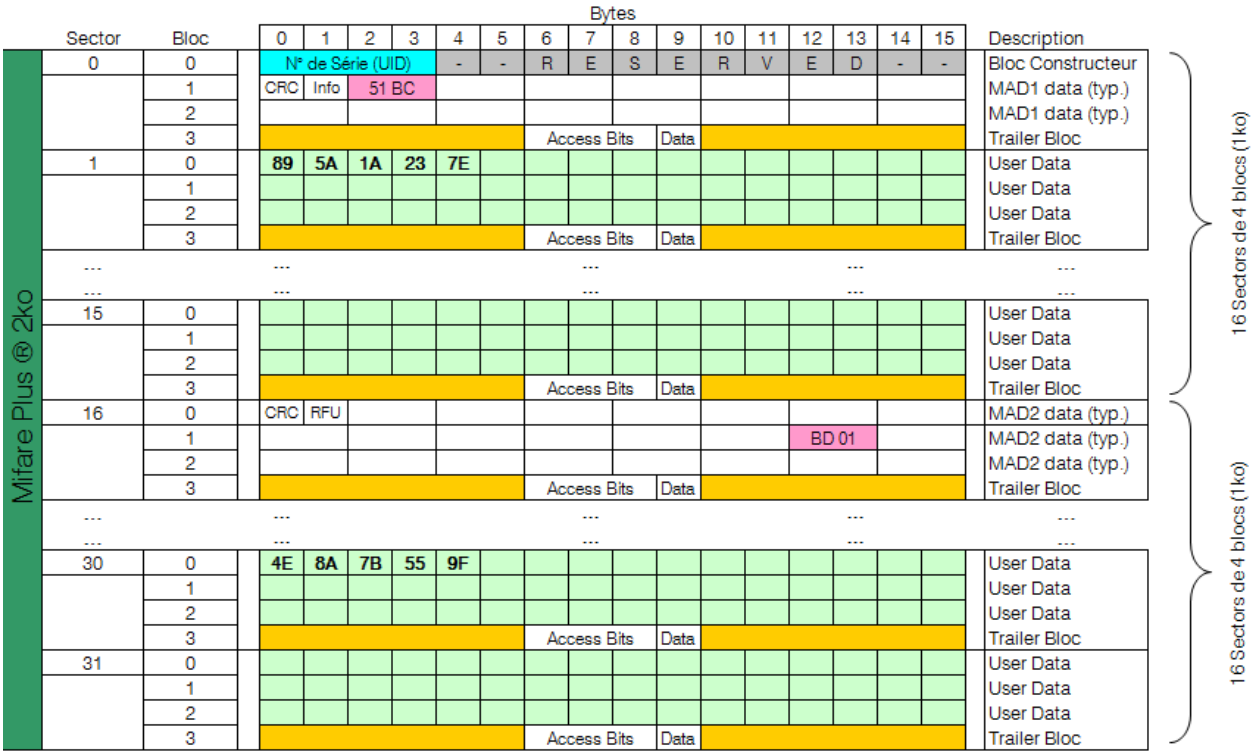
Chaque information est répertoriée dans la MAD à son emplacement de secteur respectif.

- ✓ Clé A MAD : « *A0 A1 A2 A3 A4 A5* »
- ✓ Clé B MAD : « *FF FF FF FF FF FF* »

- ✓ Clé A Secteur 1 : « B1 42 A6 80 CD 90 »
- ✓ Clé B Secteur 2 : « 4F 66 36 0F 9C C2 »

- ✓ Clé A Secteur 30 : « BC 23 C9 BE D4 D9 »
- ✓ Clé B Secteur 30 : « D9 16 7C A8 38 B4 »

Exemple de mémoire de découpée : MIFARE Plus® Level 3



Dans le cas ci-dessus, la mémoire de la puce MIFARE Plus® Level 3 contient deux informations encodées dans le secteur 1 et 30 protégés par des clés différentes. Chaque information est répertoriée dans la MAD à son emplacement de secteur respectif. En *Level* 3, les clés *AES* sont contenues dans un espace mémoire différent du quatrième bloc de chaque secteur.

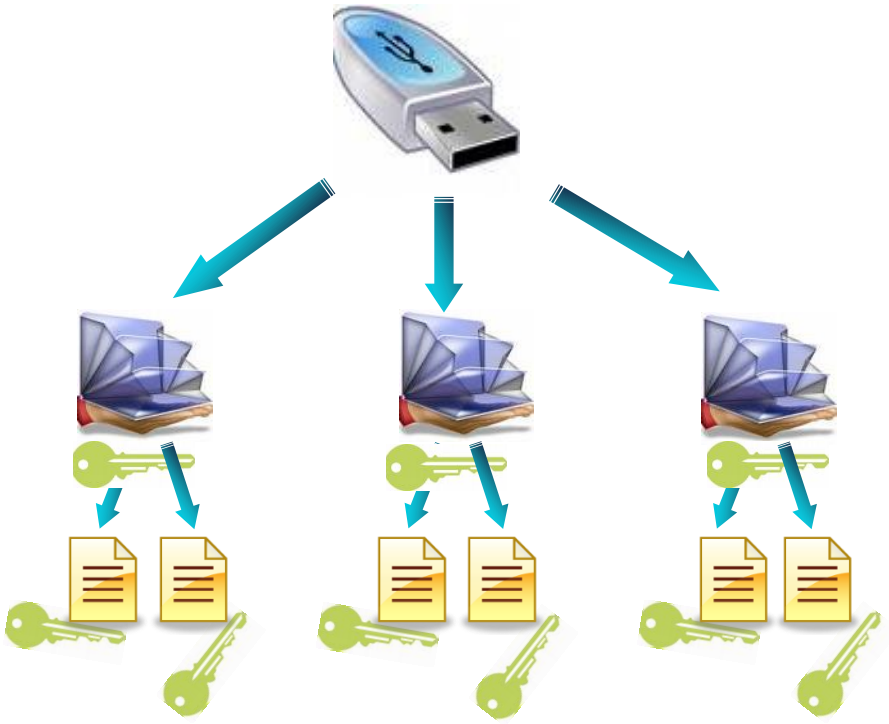
- ✓ Clé A *AES* MAD : « *A0 A1 A2 A3 A4 A5 A6 A7 A0 A1 A2 A3 A4 A5 A6 A7* »
- ✓ Clé B *AES* MAD : « *FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF* »

- ✓ Clé A *AES* Secteur 1 : « 11 10 8F 86 3E EA 98 5E CB 0C 4D 91 5E 0A 95 24 »
- ✓ Clé B *AES* Secteur 2 : « 9B E4 90 91 D7 45 B7 4A 7C 25 80 D3 52 5C 2D 6E»

- ✓ Clé A *AES* Secteur 30 : « 9A 55 AC 3F F7 AB 1C F5 BF 20 E6 73 60 29 F0 16 »
- ✓ Clé B *AES* Secteur 30 : « AA 20 40 AB FC 16 E2 49 BE FE 3F B3 42 5E 59 BE »

T3.2 - Organisation de la mémoire des puces MIFARE® DESFire® et MIFARE® DESFire® EV1/2

Plan mémoire global



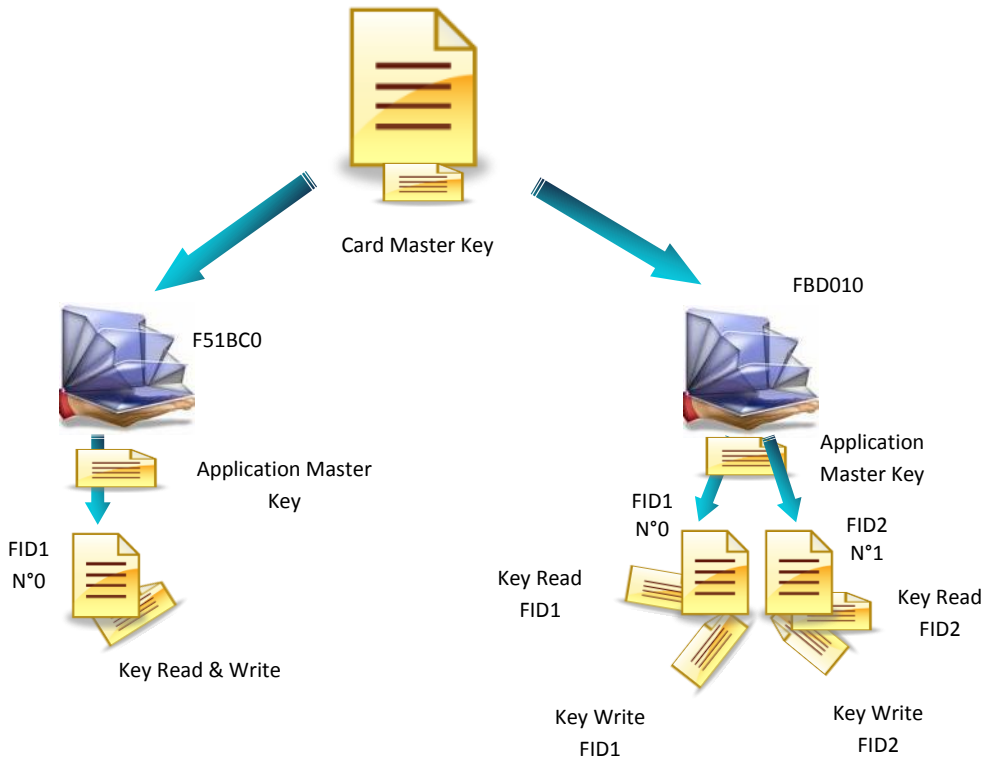
→ Une application racine.

→ Jusqu'à 28 applications.

→ Jusqu'à 32 fichiers par application.

→ Jusqu'à 14 clés par application. Utilisation indépendante pour chaque fichier. (SECard crée le maximum de clés par application soit 14).

Exemple de mémoire découpée



T3.3 - Organisation de la mémoire des puces MIFARE Ultralight® et Ultralight® C

Plan mémoire global

			Bytes				
			0	1	2	3	Pages
Mifare UltraLight C ®	Mifare UltraLight ®	Chip serial Number 7 bytes	CSN0	CSN1	CSN2	BCC0	0
			CSN3	CSN4	CSN5	CSN6	1
		Internal Lock bytes	BCC1	INTERNAL	LOCK0	LOCK1	2
		OTP	OTP0	OTP1	OTP2	OTP3	3
		Data Read / Write	Data0	Data1	Data2	Data3	4
			...	...	...	...	...
			...	...	...	Data47	15
			Data48	Data49	...	...	16
			...	...	...	...	17
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	...	...	...
			...	...	Data142	Data143	39
		Lock bytes Auth. Configuration Counter	LOCK / AUTH / COUNTER				40-43
		Security Key	3DES AUTHENTICATION KEY				44-47

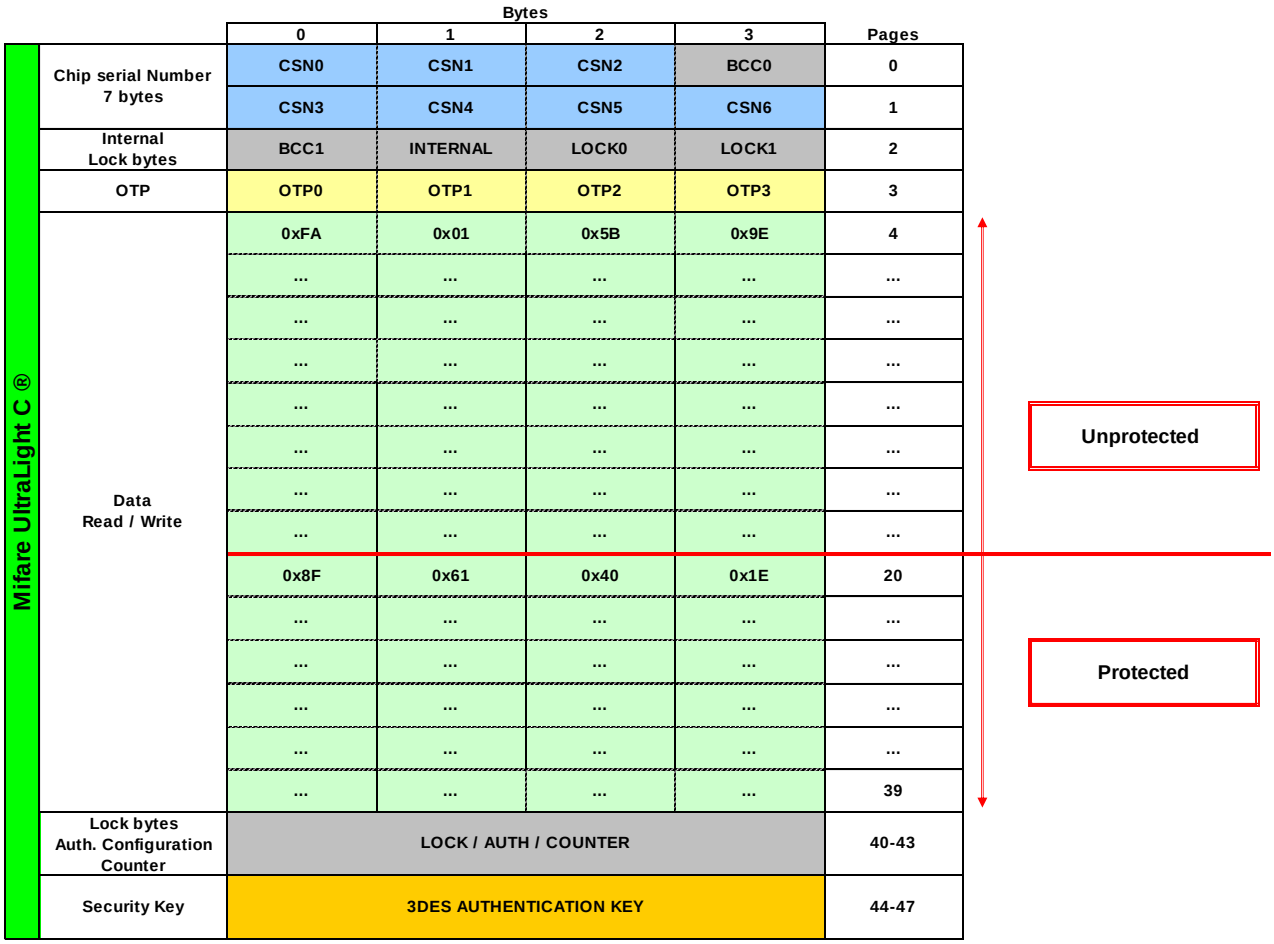
- ✓ La mémoire des puces MIFARE Ultralight® et Ultralight® C est découpé en plusieurs *Pages* de 4 octets chacune.

- ✓ La partie lecture / écriture débute à la *Page* 4. La *Page* 3 étant une zone OTP (One Time Programming), celle-ci ne peut être encodée qu'une seule fois.

- ✓ Le verrouillage des opérations d'écritures et le verrouillage des authentifications (*Lock bytes*) s'effectuent toujours à partir d'une page jusqu'à la dernière.

  Exemple : il est possible de s'authentifier uniquement de la *Page* 17 à la *Page* 39 incluse.

Exemple de mémoire découpée



Mifare UltraLight C ®		Bytes 0	1	2	3	Pages	
	Chip serial Number 7 bytes	CSN0	CSN1	CSN2	BCC0	0	
		CSN3	CSN4	CSN5	CSN6	1	
	Internal Lock bytes	BCC1	INTERNAL	LOCK0	LOCK1	2	
	OTP	OTP0	OTP1	OTP2	OTP3	3	
	Data Read / Write	0xFA	0x01	0x5B	0x9E	4	
		...	...	...	...	...	
		...	...	...	...	...	
		...	...	...	...	...	
		...	...	...	...	...	
		...	...	...	...	...	
		...	...	...	...	...	Unprotected
		...	...	...	...	...	
		...	...	...	...	...	
		0x8F	0x61	0x40	0x1E	20	
		...	...	...	...	...	
		...	...	...	...	...	Protected
		...	...	...	...	...	
		...	...	...	...	...	
		...	...	...	...	39	
	Lock bytes Auth. Configuration Counter	LOCK / AUTH / COUNTER				40-43	
	Security Key	3DES AUTHENTICATION KEY				44-47	

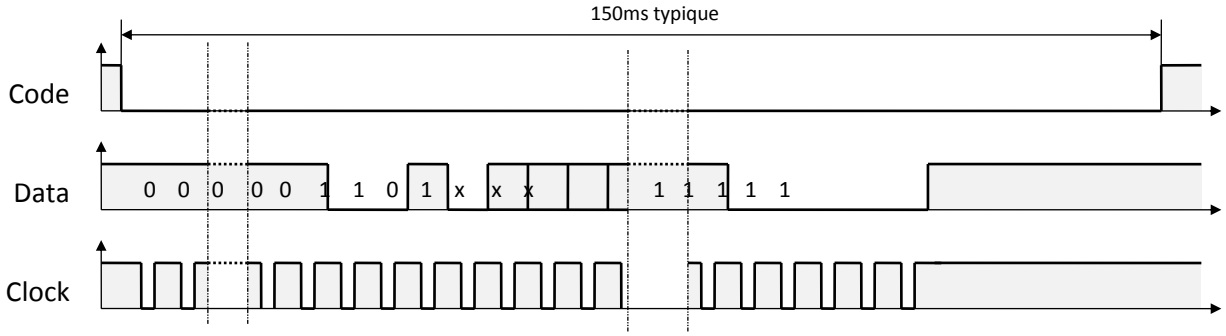
Dans le cas ci-dessus, la zone de la *Page* 4 à la *Page* 19 incluse n'est pas protégée en lecture et ne nécessitera donc pas d'authentification avec la clé *3DES*. Le code privé en *Page* 4 sera donc lisible sans aucune contrainte.

La zone de la *Page* 20 à la *Page* 39 est protégée. Le code privé situé en *Page* 20 ne pourra être lu qu'après une authentification avec la clé *3DES.*

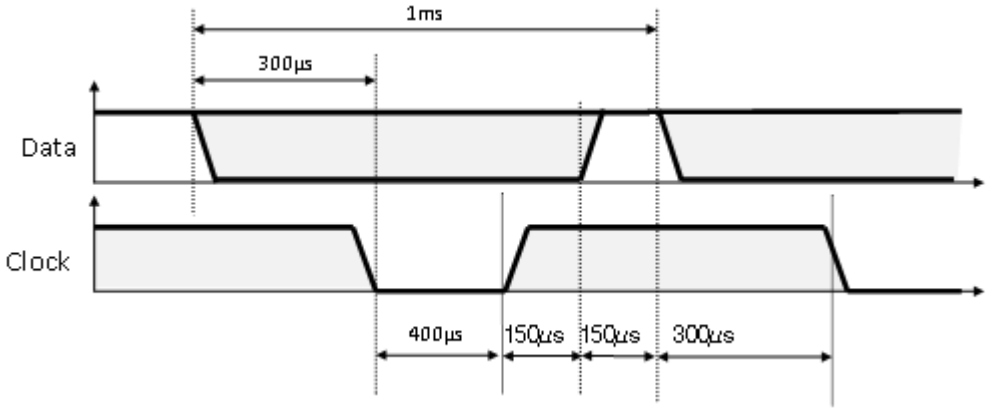
T4 - Au sujet des protocoles de communication TTL

T4.1 - Protocole ISO2 Clock&Data

Chronogrammes



Détails de l'horloge



Structure du message *2B & 2H*

Zéros de début	*Start Sentinel*	*Données*	*End Sentinel*	*LRC*	*Zéros de fin*

Description du message

La trame est constituée d'une première série de 16 zéros de synchronisation suivie par des caractères de 5 bits (4 bits, LSB en premier, plus 1 bit de parité). Elle se termine par des zéros de fin de trame sans horloge. Le message se décompose comme suit :

Start Sentinel :	1 caractère 1011b (0x0B) - bit de parité 0. Transmission 1101 0
Données :	Selon type protocole : 13 ou 10 caractères décimaux
End Sentinel :	1 caractère 1111b (0x0F) - bit de parité 1. Transmission 1111 1
LRC :	1 caractère de contrôle, qui est le XOR de tous les caractères.

Protocole 2B (13 caractères)

Lecture d'un identifiant sur 5 octets (40 bits) et conversion en décimal.

Variante	Décodage	Trame totale sur 112 bits	Valeurs
2B	*Décimal (BCD)*	*13 caractères*	*0 à 9*

Exemple

Pour un code privé en hexadécimal « 0x187E775A7F », le code sera : « *0105200966271* ».
La trame envoyée par le lecteur sera de la forme suivante :

000...	1101 0	0000 1	1000 0	0000 1	1010 1	. . . .	0110 1	0100 0	1110 0	1000 0	1111 1	1111 1	000...
	B	*0*	*1*	*0*	*5*	*2 0 09 6*	*6*	*2*	*7*	*1*	*F*	*F*	
Zéros	*S.S*	*Car.1*	*Car.2*	*Car.3*	*Car.4*	*Car….*	*Car.10*	*Car.11*	*Car.12*	*Car.13*	*E.S*	*LRC*	*Zéros*

Protocole 2H (10 caractères)

Lecture d'un identifiant sur 4 octets (32 bits) et conversion en décimal.

Variante	Décodage	Trame totale sur 112 bits	Valeurs
2H	*Décimal (BCD)*	*10 caractères*	*0 à 9*

Exemple

Pour un code privé en hexadécimal « 0x06432F1F», le code sera : « *0105066271* ».
La trame envoyée par le lecteur sera de la forme suivante :

000...	1101 0	0000 1	1000 0	0000 1	1010 1	. . . .	0110 1	0100 0	1110 0	1000 0	1111 1	0010 1	000...
	B	*0*	*1*	*0*	*5*	*0 6*	*6*	*2*	*7*	*1*	*F*	*4*	
Zéros	*S.S*	*Car.1*	*Car.2*	*Car.3*	*Car.4*	*Car….*	*Car.7*	*Car.8*	*Car.9*	*Car.10*	*E.S*	*LRC*	*Zéros*

Particularité pour la lecture d'un identifiant 125kHz

Type de détection UID : Lecture sur 5 octets puis conversion en décimal puis tronqué à 10 caractères.

Type de détection ID Privé : Lecture sur 5 octets puis tronque à 4 puis converti en décimal.

Protocole 2S Crosspoint (10 caractères)

Uniquement pour la partie 125 kHz du lecteur bifréquences (BF5)

Variante	Décodage	Trame totale sur 112 bits	Valeurs
2S	*Décimal (BCD)*	*9-10 caractères*	*0 à 9*

Les caractères BCD contenus dans la trame sont obtenus en :

- Se référant aux trois octets de poids faible.
- Convertissant la valeur hexadécimale de l'identifiant en binaire.
- Intervertissant les bits de chaque octet.

b7	b6	b5	b4	b3	b2	b1	b0		b7	b6	b5	b4	b3	b2	b1	b0		b7	b6	b5	b4	b3	b2	b1	b0
b6	b4	b7	b5	b1	b3	b0	b2		b6	b4	b7	b5	b5	b3	b0	b6		b1	b3	b1	b2	b4	b2	b0	b7
0	1	0	0	0	0	0	1		1	0	1	0	0	1	0	1		1	1	0	1	1	0	1	1
1	0	0	0	0	0	1	0		0	0	1	1	0	1	1	1		0	0	1	0	1	1	1	1
Octet [2]									Octet [1]									Octet [0]							

- Convertissant la valeur binaire en hexadécimal, puis en BCD.

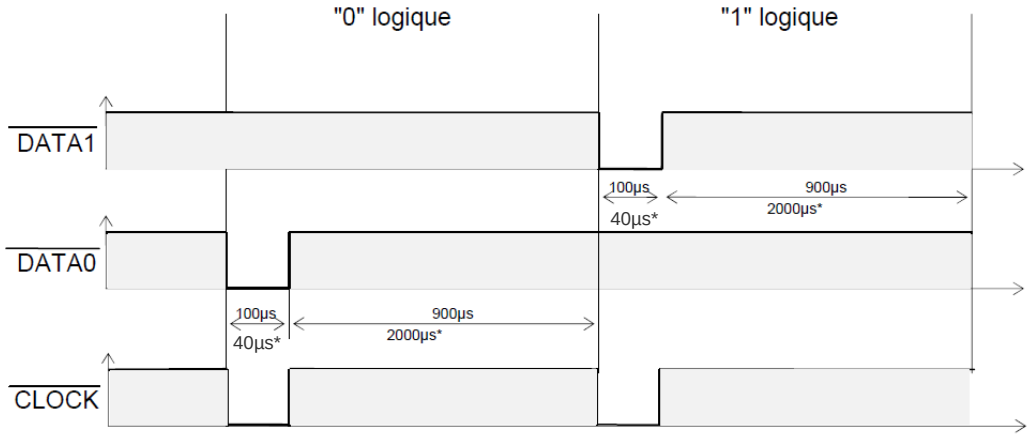
Exemple

Pour un identifiant « 0x0A0041A5DB» :

SOURCE	41	A5	DB	0100 0001	1010 0101	1101 1011
Codage	82	37	2F	1000 0010	0011 0111	0010 1111

T4.2 - Protocole Wiegand

Chronogrammes



*Temps pour la variante 3i, 3V

Protocole Wiegand 3i

Variante	Décodage	Données 24 bits	Valeurs
3i	*Hexadécimal*	*6 caractères*	*0 à F*

Structure du message

Bit 1	Bit 2 ... Bit 25	Bit 26
Parité paire sur bit 2 ... bit 13	*Données (24 bits)*	*Parité impaire sur bit 14 ... bit 25*

Description du message

La trame est constituée d'une totalité de 26 bits, et se décompose comme suit :

1ère parité : *1 bit de parité paire sur les 12 bits suivants*
Données : *6 caractères hexadécimaux « MSByte first »*
2nde parité : *1 bit de parité impaire sur les 12 bits précédents*

Exemple

Pour un code hexadécimal « *0x0FC350* », la trame envoyée sera la suivante :

0	0000	1111	1100	0011	0101	0000	1
	0	*F*	*C*	*3*	*5*	*0*	
Parité	*Car.1*	*Car.2*	*Car.3*	*Car.4*	*Car.5*	*Car.6*	*Parité*

Note

Un code site est généralement associé au troisième octet (octet [2]). Dans l'exemple ci-dessus, celui-ci vaut *0x0F* soit *15* en décimal (maximum *255* en décimal – *0xFF* en hexadécimal).

Le code carte est généralement associé au premier et second octet (octet [1] et octet [0]). Dans l'exemple ci-dessus, celui-ci vaut *0xC350* soit *50000* (maximum *65535* en décimal – *0xFFFF* en hexadécimal).

Protocole Wiegand 3CB

Bit 1 ... Bit 40	Bit 41... Bit 44
Donnée « MSB first »	*LRC*

Description du message

La trame est constituée de 44 bits et se décompose comme suit :

Données : *10 caractères hexadécimaux « MSByte first »*
LRC : *1 caractère de contrôle, XOR de tous les caractères*

Exemple
Pour un code hexadécimal « *0x01001950C3* », la trame envoyée sera la suivante :

0000	0001	0000	0000	0001	1001	0101	0000	1100	0011	0011
0	*1*	*0*	*0*	*1*	*9*	*5*	*0*	*C*	*3*	*3*
Car.1	*Car.2*	*Car.3*	*Car.4*	*Car.5*	*Car.6*	*Car.7*	*Car.8*	*Car.9*	*Car.10*	*LRC*

Protocole Wiegand 3CA

Bit 1 ... Bit 32	Bit 33... Bit 36
Donnée « MSB first »	*LRC*

Description du message

La trame est constituée de 36 bits et se décompose comme suit :

Données : *8 caractères hexadécimaux « MSByte first » (32 bits)*
LRC : *1 caractère de contrôle, XOR de tous les caractères*

Exemple
Pour un code hexadécimal « *0x001950C3* », la trame envoyée sera la suivante :

0000	0000	0001	1001	0101	0000	1100	0011	0010
0	*0*	*1*	*9*	*5*	*0*	*C*	*3*	*2*
Car.1	*Car.2*	*Car.3*	*Car.4*	*Car.5*	*Car.6*	*Car.7*	*Car.8*	*LRC*

Note
Dans le cas d'un identifiant sur 5 octets (40 bits), le lecteur tronquera l'octet (8 bits) de poids fort.

Protocole Wiegand 3LB
Wiegand 40 bits identique au Wiegand 3CB sans LRC

Protocole Wiegand 3LA
Wiegand 32 bits identique au Wiegand 3CA sans LRC

Protocole Wiegand 3T

Bit 1 ... Bit 8	Bit 9 ... Bit 64	Bit 65... Bit 68
Type de puce	*Donnée « MSB first »*	*LRC*

La trame est constituée de 68 bits et se décompose comme suit :

Type de puce : *1 octet (8 bits)*
Données : *14 caractères hexadécimaux « MSByte first » (56 bits)*
LRC : *1 caractère de contrôle, XOR de tous les caractères (4 bits)*

L'octet « *Type de puce* » indique le type de puce lue par le lecteur en mode UID :

- 0x40 ➔ MIFARE® Classic
- 0x41 ➔ MIFARE® DESFire® / DESFire® Ev1
- 0x42 ➔ 125 kHz (EM/Nedap/HID) (sur gamme standard et ARC/ARCS)
- 0x43 ➔ MIFARE Ultralight® / Ultralight® C
- 0x44 ➔ MIFARE Plus® Level 0 / Level 2 / Level 3
- 0x45 ➔ PUPI ISO 14443-3B
- 0x46 ➔ CPS3
- 0x47 ➔ Moneo
- 0x4A ➔ 3.25 MHz (uniquement sur gamme standard)
- 0x4E ➔ HCE
- 0x50 ➔ Type de tag non défini
- 0x60 ➔ BLE (Bluetooth Smart Android ≥5 & iOS ≥8)
- 0x70 ➔ Arrachement

Exemple pour une puce MIFARE® DESFire® Ev1

Pour un code hexadécimal « *0x80AF01001950C3* », la trame envoyée sera *0x41 80AF01001950C3 B.*

Exemple pour une puce MIFARE® Classic

Pour un code hexadécimal « *0xA771FE4C* », la trame envoyée sera *0x40 000000A771FE4C 6.*

Note

- ✓ Il n'est pas possible de forcer un code site en mode « *UID* ».
- ✓ Pas de type de carte ajouté en mode « *PrivateID* ». Seules les données en mémoire sur 8 octets sont transmises.

Protocole Wiegand 3Eb

Variante	Décodage	Données 32 bits	Valeurs
34 bits	*Hexadécimal*	*8 caractères*	*0 à F*

Structure du message

Bit 1	Bit 2 ... Bit 33	Bit 34
Parité paire sur bit 2 ... bit 17	*Données (32 bits)*	*Parité impaire sur bit 18 ... bit 33*

Description du message

La trame est constituée d'une totalité de 34 bits, et se décompose comme suit :

1ère parité : *1 bit de parité paire sur les 16 bits suivants*
Données : 8 *caractères hexadécimaux « MSByte first »*
2nde parité : *1 bit de parité impaire sur les 16 bits précédents*

Protocole Wiegand 3W

Variante	Décodage	Données 32 bits	Valeurs
35 bits	*Hexadécimal*	*8 caractères*	*0 à F*

Structure du message

Bit 1-2	Bit 3 ... Bit 34	Bit 35
2 Parités paire	*Données (32 bits)*	*Parité impaire*

Protocole Wiegand 3V

Variante	Décodage	Données 32 bits	Valeurs
37 bits	*Hexadécimal*	*8 caractères*	*0 à F*

Structure du message

Bit 1	Bit 2 ... Bit 36	Bit 37
Parité paire sur bit 2 ... bit 19	*Données (35 bits)*	*Parité impaire sur bit 19 ... bit 36*

Description du message

La trame est constituée d'une totalité de 37 bits, et se décompose comme suit :

1ère parité : *1 bit de parité paire sur les 18 bits suivants*
Données : 9 *caractères hexadécimaux « MSByte first »*
2nde parité : *1 bit de parité impaire sur les 18 bits précédents*

Exemple

Pour un code hexadécimal « *0x 0F3129DD3B* », la trame envoyée sera la suivante :

1	111	0011	0001	0010	1001	1101	1101	0011	1011	0
	7	*3*	*1*	*2*	*9*	*D*	*D*	*3*	*B*	
Parité	*Car.1*	*Car.2*	*Car.3*	*Car.4*	*Car.5*	*Car.6*	*Car.7*	*Car.8*	*Car.9*	*Parité*

T4.3 - Protocole Wiegand chiffré

Les lecteurs S31 restituent l'information sur une liaison Wiegand 128 bits chiffrée par algorithme public AES + 4 bits LRC (non chiffré). La clé AES est celle défini dans « Clé AES de chiffrement de la sortie », elle doit impérativement être différente de 0xFF...FF.

Chaque trame est composée d'un paquet de données sur 12 octets, d'une valeur aléatoire sur 2 octets et d'un CRC-CCITT 16 bits (polynôme 0x1021, valeur initiale 0xFFFF).

Si un identifiant est supérieur à 12 octets, plusieurs trames sont émises de la façon suivante :

Data ***12 octets***	***Valeur aléatoire*** ***2 octets***	***CRC*** ***2 octets***

Trame1 chiffrée

Data ***12 octets***	***Valeur aléatoire*** ***2 octets***	***CRC*** ***2 octets***

Trame 2 chiffrée

Data ***12 octets***	***Valeur aléatoire*** ***2 octets***	***CRC*** ***2 octets***

Trame 3 chiffrée

T5 - Au sujet des protocoles de communication Série

T5.1 - Mode de communication unidirectionnel

Dans ce mode, les données sont envoyées en clair sur la liaison série. La communication s'effectue uniquement du lecteur vers le système.

Les LED et le buzzer sont gérés par le lecteur via la configuration du badge *SCB*.

Il est possible de configurer la structure de la trame grâce à l'encadré « Paramètres de communication série» avec les paramètres suivants :

- ✓ Pas de zéros : Complète la trame avec des 0 non significatifs (en début de trame).
- ✓ STX+ETX : Ajout d'un 0x02 (STX) et 0x03 (ETX) en début et fin de trame
- ✓ CR+LF : Option Retour chariot (0x0D + 0x0A)
- ✓ LRC : Octet de contrôle inclus en fin de trame (XOR de tous les octets précédents hormis STX).
- ✓ ASCII : Si cette option est activée, les données incluses dans la trame seront au format ASCII.
- ✓ Base : Données transmises en décimal ou hexadécimal.
- ✓ Baudrate : 9600, 19200, 38400, 57600 ou 115200 bauds.

La partie « Données » correspond au code de l'identifiant lu ou aux touches du lecteur clavier en mode Badge Ou Touche

1 octet	***X octets***	***1 octet***	***1 octet***	***1 octet***	***1 octet***
STX	*Données**	*LRC*	*0x0D*	*0x0A*	*ETX*

**Concernant les lecteurs clavier, se référer à* *T6 - Au sujet des* lecteurs Clavier

- ✓ Signal d'arrachement : Si l'option du signal d'arrachement est activée, le lecteur enverra sur la liaison série l'octet 0xAA en cas de changement d'état soit de l'entrée « SW » soit de l'accéléromètre.

- ✓ Signal de vie : Si l'option « *Signal de vie* » est activée, le lecteur enverra toutes les minutes un octet indiquant sa présence :

  - Signal de vie Générique : 0x50
  - Signal de vie Spécifique LXS/MXS/ATX : 0x50

- Signal de vie Spécifique LXE : 0x54
- Signal de vie Spécifique MS : 0x52
- Signal de vie Spécifique LXC : 0x55
- Signal de vie Spécifique WAL : 0x56
- Signal de vie Spécifique ARC : 0x61

Note :

- ✓ Les lecteurs R33/PH5 et S33/PH5 ne sont pas adressables dans le mode de communication monodirectionnel.
- ✓ La taille des données est multipliée par deux si l'option *ASCII* est activée.
- ✓ Le champ « *Taille* » permet d'ajuster la taille des données transmises par le lecteur.

T5.2 - Mode de communication bidirectionnel

Dans ce mode, la communication peut s'effectuer du lecteur vers le système pour la transmission des données et du système vers le lecteur pour la gestion des LED et buzzer. Sans action du système, le lecteur les gérera suivant la configuration définie dans la partie « Action par défaut de la LED ».

Il est recommandé de n'adresser que maximum 2 lecteurs sur un même BUS, voire 4 maximum pour des accès moins utilisé.

Lors d'une lecture d'un code valide (suivant la configuration définie dans l'Assistance SCB), celui-ci est transmis au système par le lecteur. Il est alors possible à ce moment et pendant une durée de 1.5s de piloter les LED et buzzer via l'émission d'une trame du système.

Note : les modes *Signé*, *Chiffré* et *Signé et Chiffré* sont accessibles uniquement avec les lecteurs S32, S35 et S33.

La communication série entre le lecteur et le système s'effectue selon le protocole STid SSCP.
Au démarrage du lecteur et après passage d'un SCB, le lecteur initialise la communication (selon le mode choisi) avec le Host. Si une erreur survient dans le processus de communication, l'initialisation de la communication est relancée toutes les minutes.

Il est possible de transmettre l'information selon les 4 modes suivants :

- ✓ Clair
- ✓ Signé
- ✓ Chiffré
- ✓ Signé et chiffré

✓ Clair

Trame complète envoyée par le lecteur

#02	Len	CTRL	CMD	Reserved	L_{out}	$Data_{out}$	CRC
1 octet	2 octets	2 octets	4 octets	2 octets	2 octets	L_{out} octets	2 octets

Trame complète envoyée par le système

#02	Len	CTRL	ACK	L_{in}	$Data_{in}$	Status	CRC
1 octet	2 octets	2 octets	2 octets	2 octets	L_{in} octets	2 octets	2 octets

✓ Signé

Les informations sont transmises en clair et signées.
L'algorithme de signature utilisé sera la version réduite du *HMAC-SHA-1*, c'est à dire les **10 premiers octets**).

Trame complète envoyée par le lecteur

#02	Len	CTRL	CMD	Reserved	L_{out}	$Data_{out}$	$HMAC\text{-}SHA\text{-}1_k$ (Commande)	CRC
1 octet	2 octets	2 octets	4 octets	2 octets	2 octets	L_{out} octets	10 octets	2 octets

Trame complète envoyée par le système

#02	Len	CTRL	ACK	L_{in}	$Data_{in}$	Status	Signature $HMAC\text{-}SHA\text{-}1_k$ (Réponse)	CRC
1 octet	2 octets	2 octets	2 octets	2 octets	L_{in} octets	2 octets	10 octets	2 octets

✓ **Chiffré**

Les informations sont transmises chiffrées.
L'algorithme utilisé est un *AES* utilisant une clé de 128 bits

Trame complète envoyée par le lecteur

#02	Len	CTRL	C (Commande)	..	C (Commande) suite et fin	Bourrage	Vecteur d'initialisation	CRC
1 octet	2 octets	2 octets	(k-1)*16 octets	..	16-x octets	X octets	16 octets	2 octets

Trame complète envoyée par le système

#02	Len	CTRL	C (Réponse)	..	C (Réponse) suite et fin	Bourrage	Vecteur d'initialisation	CRC
1 octet	2 octets	2 octets	(k-1)*16 octets	..	16-x octets	X octets	16 octets	2 octets

✓ **Signé et chiffré**

Les informations sont transmises signées et chiffrées avec les mêmes algorithmes décrits précédemment.

Trame complète envoyée par le lecteur

#02	Len	CTRL	C (Commande)	..	C (Commande) suite et fin	Bourrage	Vecteur d'initialisation	Signature	CRC
1 octet	2 octets	2 octets	(k-1)*16 octets	..	16-x octets	X octets	16 octets	10 octets	2 octets

Trame complète envoyée par le système

#02	Len	CTRL	C (Réponse)	..	C (Réponse) suite et fin	Bourrage	Vecteur d'initialisation	Signature	CRC
1 octet	2 octets	2 octets	(k-1)*16 octets	..	16-x octets	X octets	16 octets	10 octets	2 octets

T5.2.1 Authentification mutuelle

Les modes de communication *Signé*, *Chiffré* et *Signé ET Chiffré* reposent sur deux clés de session distinctes. Ces deux clés sont générées lors d'une authentification système / lecteur à partir d'un élément aléatoire et de deux clés utilisateurs connues du lecteur et du système.
Il est donc nécessaire de définir une méthode pour créer ces clés de session ***(k_c, k_s)*** à partir des clés utilisateurs ***(K_c, K_s)*** (ces clés ne servant qu'à générer des clés de session). Ce mécanisme utilise un dialogue spécifique chiffré, qui permettra de réaliser une authentification mutuelle des deux partenaires avant de créer des clés de session ***(k_c, k_s).***

Avec :

- ✓ ***k_s*** clé de session utilisée pour l'algorithme de signature *sur 10 octets*
- ✓ ***k_c*** clé de session utilisée pour l'algorithme de chiffrement sur 16 octets
- ✓ ***K_s*** (Sign Key) clé utilisateur utilisée pour générer la clé ks de signature sur 10 octets
- ✓ ***K_c*** (Chiff Key) clé utilisateur utilisée pour générer la clé kc de cryptographie sur 16 octets

Attention

Par défaut les clés utilisateur ont pour valeur :

K_s* = *0x FFFFFFFFFFFFFFFFFFFF

K_c* = *0x FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Il est conseillé de modifier ces clés utilisateurs afin d'optimiser la sécurité.

L'initialisation de l'authentification mutuelle est effectuée par le lecteur lorsque le champ « *Mode Sécurité* » n'est pas en « *Clair* ». Cette procédure est décrite dans le document du protocole *SSCP* suivant :

- ✓ Spec_Protocole_5AA-7AA_MIFARE_GLOBAL_Vx.x_FR

Nous consulter pour l'obtention de cette documentation.

T5.2.2 Echange d'informations

Les informations transmises par le système sont formatées de la façon suivante :

#02	*Len*	*CTRL*	*CMD*	*Reserved*	*L_{out}*	*$Data_{out}$*	*CRC*
1 octet	2 octets	2 octets	4 octets	2 octets	2 octets	L_{out} octets	2 octets

# 02	Marqueur de début de trame Start Of Frame « SOF » (sur un octet 02h)		
Len	Détermine la longueur de la commande à envoyer (deux octets)		
CTRL	Mot de deux octets englobant un octet définissant le mode de communication (message en clair, chiffré, signé etc.…) et un octet définissant le type de liaison série utilisée (RS485 ou RS232)		
	CTRL @	Détermine le type de liaison série utilisée (RS232 ou RS485) (bit 0) ainsi que l'adresse du lecteur si liaison RS485 (bit 7 à bit 1)	***b7 – b1*** : ***Adresse du lecteur RS485 1111 111" à "0000 000*** ; ***b0*** : ***Liaison série utilisée "0" RS232 "1" RS485***
	CTRL Mode	Détermine le mode de communication (un octet)	○ 00h ➔ Mode non sécurisé message transmis en clair. ○ 01h ➔ Mode signé ○ 02h ➔ Mode chiffré ○ 03h ➔ Mode signé et chiffré
CMD	Mot de quatre octets englobant deux octets déterminant le type de commande (lecteur, *Mifare DESFire* & *DESFire Ev1, Mifare Classic, Mifare Ultralight C* ou *Mifare PLUS*) et deux octets définissant le code de la commande à transmettre		
	RFU	1 octet	00h
	Type	Détermine le type de commande (1 octet)	00h ➔ Commande lecteur 01h ➔ Commande *Mifare Classic* ® 02h ➔ Commande *Mifare DESFire & DESFire® Ev1* 03h ➔ Commande *Mifare Plus*® 05h ➔ Commande *Mifare Ultralight C*® 09h ➔ Commande *CPS3* 0Bh ➔ Commande biométrique
	Code	Détermine le code commande à transmettre au lecteur (deux octets)	
Reserved	AAh 55h (deux octets).		
L_{out}	Détermine la taille des données envoyées par le host (deux octets).		
$Data_{out}$	Représente les données envoyées par le host (dans le cas d'une écriture par exemple) (L_{out} octets)		
CRC	CRC-^{16}-CCITT [Len….Command] ***[Polynôme « $x^{16} + x^{12} + x^5 + 1$ »*** 0x1021]; *Valeur Initiale 0xFFFF*		

Les informations transmises par le lecteur sont formatées de la façon suivante :

#02	*Len*	*CTRL*	*ACK*	*L_{in}*	*$Data_{in}$*	*Status*	*CRC*
1 octet	2 octets	2 octets	2 octets	2 octets	L_{in} octets	2 octets	2 octets

# 02	Marqueur de début de trame Start Of Frame « SOF » (sur un octet 02h)		
Len	Détermine la longueur de la commande à envoyer (deux octets)		
CTRL	Mot de deux octets englobant un octet définissant le mode de communication (message en clair, chiffré, signé etc.…) et un octet définissant le type de liaison série utilisée (RS485 ou RS232)		
	CTRL @	Détermine le type de liaison série utilisée (RS232 ou RS485) (bit 0) ainsi que l'adresse du lecteur si liaison RS485 (bit 7 à bit 1)	***b7 – b1*** : ***Adresse du lecteur RS485 1111 111" à "0000 000*** ; ***b0*** : ***Liaison série utilisée "0" RS232 "1" RS485***
	CTRL Mode	Détermine le mode de communication (un octet)	○ 00h ➔ Mode non sécurisé message transmis en clair. ○ 01h ➔ Mode signé ○ 02h ➔ Mode chiffré ○ 03h ➔ Mode signé et chiffré
ACK	Acquittement de début de trame, égal au code commande envoyé par le host.		
L_{in}	Détermine la taille des données que le host va recevoir (deux octets).		
$Data_{in}$	Données envoyées par le lecteur en réponse à la commande du host (L_{in} octets).		
Status	Données envoyées par le lecteur en réponse à la commande du host (L_{in} octets).		
	RFU	1 octet	00h
	Type	Détermine le type de commande (un octet)	00h ➔ Commande lecteur 01h ➔ Commande *Mifare Classic* ® 02h ➔ Commande *Mifare DESFire & DESFire® Ev1* 03h ➔ Commande *Mifare Plus®* 05h ➔ Commande *Mifare Ultralight C®* 09h ➔ Commande *CPS3* 0Bh ➔ Commande biométrique
	Code	Détermine le code erreur (un octet)	
CRC	CRC-^{16}-CCITT [Len….Command] ***[Polynôme « $x^{16} + x^{12} + x^5 + 1$ »*** 0x1021]; *Valeur Initiale 0xFFFF*		

T5.2.3 Commandes disponibles en mode de sécurité « clair »

Output_Protocol

Description

Cette commande est générée par le lecteur lors de la lecture d'un identifiant et / ou code clavier valide. Le retour de cette fonction informe le lecteur sur l'état à appliquer aux LED et buzzer.

Lecteur : CTRL CMD AAh 55h L_{out} $Data_{out}$

CMD *2 octets* : 01h 00h

L_{out} *2 octets :* $Data_{Len}$ Egal au nombre d'octets de Data

$Data_{out}$ *x octets* : Valeur de l'ID lu par le lecteur en hexadécimal.

Système : CMD L_{in} LedColor LedDuration BuzzerDuration 00h 00h

CMD *2 octets* : 01h 00h

L_{in}*2 octets* : 00h 03h (LedColor + LedDuration + BuzzerDuration)

LedColor *1 octet :* Octet déterminant la couleur de la LED.
[00h … 03h]

- 00h LED éteinte
- 01h LED verte
- 02h LED rouge
- 03h LED orange

LedDuration *1 octet* : Octet déterminant la valeur de la durée du changement de couleur de la LED.
multiple de 100 ms. [00h … FFh] avec la valeur FFh figeant la LED pour une durée indéterminée (jusqu'au prochain reset du lecteur ou prochain envoi avec une valeur différente de FFh).

BuzzerDuration *1 octet* : Octet déterminant la valeur de la durée de l'activation du buzzer.
multiple de 100 ms. [00h … FFh] avec la valeur FFh activant le buzzer pour une durée indéterminée (jusqu'au prochain reset du lecteur ou prochain envoi avec une valeur différente de FFh).

Remarque

Le lecteur dispose d'un Timeout de 1.5s pour recevoir la réponse du système concernant le pilotage des LEDS et buzzer. Une fois ce délai passé, celui-ci n'acceptera plus aucune trame jusqu'à la prochaine émission de la commande ***Output_Protocol***.

Life_Signal

Description

Cette commande est générée par le lecteur toutes les minutes. Celle-ci informe le système de la présence du lecteur sur la liaison série.

Lecteur : CTRL CMD AAh 55h L_{out} $Data_{out}$

CMD *2 octets* : 01h 02h

L_{out} *2 octets :* 00h 02h Egal au nombre d'octets de Data

$Data_{out}$ *2 octets :* 00h + XXh ; Avec XXh valant :

- 01h Si signal de vie générique
- 01h Si signal de vie spécifique pour LXS/LXC/MXS/ATX
- 03h Si signal de vie spécifique pour MS
- 05h Si signal de vie spécifique pour LXE
- 06h Si signal de vie spécifique pour LXC
- 07h Si signal de vie spécifique pour ARC

Système : CMD L_{in} 00h 00h

CMD *2 octets :* 01h 02h

L_{in} *2 octets :* 00h 00h

Remarque

Il est nécessaire que cette option soit activée via « *l'Assistant SCB* » du logiciel SECard afin que le signal de vie soit transmis par le lecteur.

Wrenching_Signal

Description

Cette commande est générée par le lecteur lorsque celui-ci détecte un changement d'état sur l'entrée « SW ». Elle a pour but d'informer le système de changement (dans le cas d'un arrachement par exemple).

Lecteur : CTRL CMD AAh 55h L_{out} 00h

CMD *2 octets :* 01h 03h

L_{out} *2 octets :* 00h 01h Egal au nombre d'octets de Data

Système : CMD L_{in} 00h 00h 00h 00h

CMD *2 octets :* 01h 03h

L_{in} *2 octets :* 00h 00h

Remarque

Il est nécessaire que cette option soit activée via « *l'Assistant SCB* » du logiciel SECard afin que le signal d'arrachement soit transmi par le lecteur.

Read_input

Description

Cette commande est envoyée périodiquement par le lecteur au système. Elle permet au système de commander l'activation des LED et du buzzer.

Lecteur : CTRL CMD AAh 55h 00h

CMD *2 octets :* 01h 04h

Système : CMD L_{in} LedGreen LedRed Buzzer 00h 00h

CMD *2 octets:* 01h 04h

L_{in} *2 octets :* 00h 03h

LedGreen *1 octet* : 01h inactive
00h active

LedRed *1 octet* : 01h inactive
00h active

Buzzer *1 octet :* 01h inactif
00h actif

Remarque
Il est nécessaire que cette option soit activée avec le pooling désiré via « *l'Assistant SCB* » du logiciel SECard.

T5.2.4 Commandes disponibles en mode de sécurité « Signé », « Chiffré » ou « Signé & Chiffré »

Toutes les fonctions du mode « *Clair* » sont disponibles ainsi que les suivantes

Authenticate

Description

Cette commande permet de s'authentifier avec le lecteur et de générer les clés de session de signature et de chiffrement. Le paramètre mode permet de définir le type d'authentification requis.

ResetAuthenticate

Description

Cette commande permet de remettre à zéro toutes les clés de session et donc d'annuler l'authentification (signature et/ou le chiffrement) en cours avec le système.

ChangeReaderKeys

Description

Cette commande permet de changer les clés utilisateur d'authentification et/ou de chiffrement contenues dans le système.
Ces commandes sont décrites dans les documents du protocole *SSCP* suivants :

- ✓ Spec_Protocole_5AA-7AA_MIFARE_GLOBAL_Vx.x_FR

Nous consulter pour l'obtention de ces documentations.

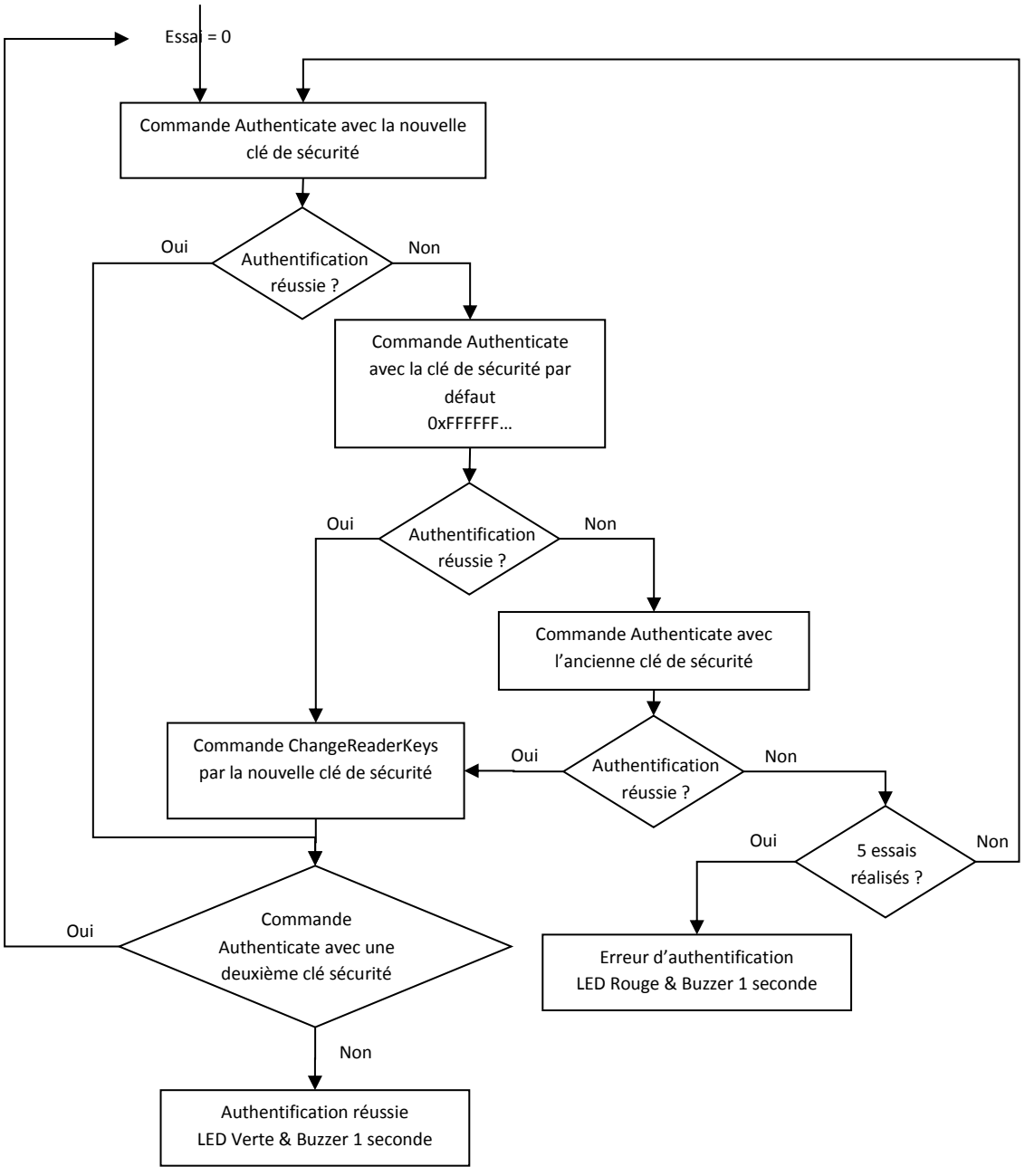
T5.2.5 Modification des clés utilisateurs

Les valeurs des clés utilisateurs de chiffrement et de signature peuvent être changées dans SECard.
La modification de ces clés sera effectuée par une commande lecteur spéciale ***ChangeReaderKeys*** (décrite dans les spécifications protocoles *SSCP*) transmise signée et chiffrée.

Cette procédure est envoyée au système par le lecteur lorsque celui-ci détecte via le badge *SCB* une demande de changement de clés.

La clé de sécurité correspond à :
- ✓ la clé de Chiffrement si la communication est configurée en mode *Chiffré*
- ✓ la clé de signature si la communication est configurée en mode *Signé*

Dans le cas d'une communication en mode *Chiffré et Signé* le processus d'authentification sera fait deux fois, une fois pour chaque clé.



T6 - Au sujet des lecteurs Clavier

T6.1 - Lecteurs TTL - R31 - Badge OU Touche

Le lecteur fonctionne en mode Badge OU Touche. Cela signifie qu'en cas de présentation d'un badge, son identifiant est immédiatement transmis suivant le protocole en cours, suivi d'un acquittement sonore.
En cas de frappe d'une touche, et suivant le format des données du code choisi (1, 2 ou 3), sa valeur est immédiatement transmise suivant le protocole en cours, suivi d'un acquittement sonore.

Concernant le type 4 d'encodage, une séquence de touches est saisie, validée par un appui sur la touche **'★'** pour être alors transmise suivant le protocole en cours, suivi d'un acquittement sonore. Au-delà d'un timeout de 6 secondes entre 2 touches saisies, l'opération en cours est annulée, signalée par un clignotement de la LED rouge et d'un bip sonore. Toute la saisie est alors à recommencer.

Types de formats des touches clavier

- **'1' : « 4 bits trame »**
  4 bits correspondants à la valeur de la touche pressée, envoyés au sein d'une trame selon le protocole de sortie.

Format ISO2 LSB … MSB		
'0'	0000	0x00
'1'	1000	0x01
'2'	0100	0x02
'3'	1100	0x03
'4'	0010	0x04
'5'	1010	0x05
'6'	0110	0x06
'7'	1110	0x07
'8'	0001	0x08
'9'	1001	0x09
'#'	1101	0x0B

Dans ce format, les 4 bits sont envoyés LSB First au sein d'une trame correspondante au protocole en cours. Se référer à la spécification de chacun de ces protocoles pour le détail.

Exemple : envoi de la touche seule '5' au format 4 bits et suivant le protocole ISO2 / 2b.

000…	1101 0	1010 1	1111 1	xxxx x	000…
Zéros	**Start**	**'5'**	**End**	**LRC**	**Zéros**

Format WIEGAND MSB … LSB		
'0'	0000	0x00
'1'	0001	0x01
'2'	0010	0x02
'3'	0011	0x03
'4'	0100	0x04
'5'	0101	0x05
'6'	0110	0x06
'7'	0111	0x07
'8'	1000	0x08
'9'	1001	0x09
'#'	1011	0x0B

Dans ce format, les 4 bits sont envoyés MSB First au sein d'une trame correspondante au protocole en cours. Se référer à la spécification de chacun de ces protocoles pour le détail.

Exemple : envoi de la touche seule '5' au format 4 bits et suivant le protocole Wiegand / 3i.

0	0000	0000	0000	0000	0000	0101	1
Parité	**'0'**	**'0'**	**'0'**	**'0'**	**'0'**	**'5'**	**Parité**

✓ **'2'** : **« 4 bits »**

4 bits correspondants à la valeur de la touche pressée, envoyés seuls.

Format ISO2 LSB … MSB		
'0'	0000	0x00
'1'	1000	0x01
'2'	0100	0x02
'3'	1100	0x03
'4'	0010	0x04
'5'	1010	0x05
'6'	0110	0x06
'7'	1110	0x07
'8'	0001	0x08
'9'	1001	0x09
'#'	1101	0x0B

Dans ce format, les 4 bits sont envoyés LSB First avec les timings du protocole en cours. Se référer à la spécification de chacun de ces protocoles pour le détail.

Exemple : envoi de la touche seule '4' au format 4 bits et suivant le protocole ISO2 / 2b.

0010
'4'

Format WIEGAND MSB … LSB		
'0'	0000	0x00
'1'	0001	0x01
'2'	0010	0x02
'3'	0011	0x03
'4'	0100	0x04
'5'	0101	0x05
'6'	0110	0x06
'7'	0111	0x07
'8'	1000	0x08
'9'	1001	0x09
'#'	1011	0x0B

Dans ce format, les 4 bits sont envoyés MSB First avec les timings du protocole en cours. Se référer à la spécification de chacun de ces protocoles pour le détail.

Exemple : envoi de la touche seule '4' au format 4 bits et suivant le protocole Wiegand / 3i.

0100
'4'

✓ **'3'** : **« 8 bits »**

8 bits correspondants à la valeur de la touche pressée, envoyés seuls (configuration par défaut).

Format ISO2 LSB … MSB		
'0'	11110000	0xF0
'1'	01111000	0xE1
'2'	10110100	0xD2
'3'	00111100	0xC3
'4'	11010010	0xB4
'5'	01011010	0xA5
'6'	10010110	0x96
'7'	00011110	0x87
'8'	11100001	0x78
'9'	01101001	0x69

Dans ce format, les 8 bits sont envoyés LSB First avec les timings du protocole en cours. Se référer à la spécification de chacun de ces protocoles pour le détail.

Exemple : envoi de la touche seule '4' au format 8 bits et suivant le protocole ISO2 / 2b.

11010010
'4'

Format WIEGAND MSB … LSB		
'0'	11110000	0xF0
'1'	11100001	0xE1
'2'	11010010	0xD2
'3'	11000011	0xC3
'4'	10110100	0xB4
'5'	10100101	0xA5
'6'	10010110	0x96
'7'	10000111	0x87
'8'	01111000	0x78
'9'	01101001	0x69

Dans ce format, les 8 bits sont envoyés MSB First avec les timings du protocole en cours. Se référer à la spécification de chacun de ces protocoles pour le détail.

Exemple : envoi de la touche seule '4' au format 8 bits et suivant le protocole Wiegand / 3i.

10110100
'4'

✓ **‘4’** : **« X touche Trame »**

4 bits – x touches au sein d’une trame, 4 bits correspondants à la valeur de la touche pressée, envoyés au sein d’une trame selon le protocole de sortie.

Format ISO2 LSB … MSB		
‘0’	0000	0x00
‘1’	1000	0x01
‘2’	0100	0x02
‘3’	1100	0x03
‘4’	0010	0x04
‘5’	1010	0x05
‘6’	0110	0x06
‘7’	1110	0x07
‘8’	0001	0x08
‘9’	1001	0x09

Dans ce format, les 4 bits des x touches sont envoyés LSB First au sein d’une trame correspondante au protocole en cours. Se référer à la spécification de chacun de ces protocoles pour le détail.

Seules les touches ‘0’ à ‘9’ sont possibles.

‘★’ Valide la fin de la séquence de touches. Dans le cas où x=8, la procédure est automatiquement validée et les 8 touches sont envoyées.

‘#’ Annule la séquence en cours.

Exemple : dans ce mode, si l’utilisateur saisit au clavier ‘4’ ‘5’ ‘9’ ‘★’, la trame envoyée sera au format 4 bits et suivant le protocole ISO2 / 2b.

000…	1101 0	0010 0	1010 1	1001 1	1111 1	xxxx x	000…
Zéros	**Start**	**‘4’**	**‘5’**	**‘9’**	**End**	**LRC**	**Zéros**

Format WIEGAND MSB … LSB		
‘0’	0000	0x00
‘1’	0001	0x01
‘2’	0010	0x02
‘3’	0011	0x03
‘4’	0100	0x04
‘5’	0101	0x05
‘6’	0110	0x06
‘7’	0111	0x07
‘8’	1000	0x08
‘9’	1001	0x09

Dans ce format, les 4 bits des x touches sont envoyés MSB first, au sein d’une trame correspondante au protocole en cours. Se référer à la spécification de chacun de ces protocoles pour le détail.

Seules les touches ‘0’ à ‘9’ sont possibles.

‘★’ Valide la fin de la séquence de touches. Dans le cas où **(x=8)***, la procédure est automatiquement validée et les 8 touches sont envoyées.

‘#’ Annule la séquence en cours

Exemple : dans ce mode, si l’utilisateur saisit au clavier ‘4’ ‘5’ ‘9’ ‘★’, la trame envoyée sera, au format 4 bits et suivant le protocole Wiegand 3i.

0	0000	0000	0000	0100	0101	1001	1
Parité	**‘0’**	**‘0’**	**‘0’**	**‘4’**	**‘5’**	**‘9’**	**Parité**

Remarque

✓ *Nombre de touches maximum = 8.*

✓ ***xmax** = 6 touches maximum pour le protocole Wiegand 3i. Dans ce cas les valeurs des touches ne sont pas envoyées automatiquement, il faut valider la séquence en cours.*

T6.2 - Lecteurs TTL - R31 - Badge ET Touche

Dans ce mode, la séquence de touches doit être saisie au clavier et validée par l'identifiant RFID.
Une séquence de touches est saisie au clavier (1 à 9 touches suivant la configuration).
Seules les touches **'0'** à **'9'** peuvent être saisies.

Les touches **'★'** et **'#'** annulent l'opération en cours et toute la saisie est à recommencer. Il en est de même au-delà d'un timeout de 6 secondes entre 2 touches saisies.

Lorsque la séquence de touches est complète, le lecteur attend un identifiant pendant un délai de 6 secondes (émission d'un bip sonore pour indiquer l'attente d'un identifiant + LED orange).
Au-delà de ce timeout, le lecteur annule l'opération en cours, signalé par un clignotement rouge et d'un bip sonore. Toute la séquence 'saisie touche(s) + badge' est à recommencer.
L'ensemble est transmis suivant le protocole en cours, avec en premier dans la trame la séquence de touches saisies au format 4 bits :

Touche n°1 *Format 4 bits*	Touche n°2 *Format 4 bits*	…	Identifiant *Format n bits* *(taille du protocole)*

Exemple :
Trois touches : 7, 8, 9 / Identifiant 0x11223344 en hexadécimal soit 287454020 en décimal
Protocole Wiegand 3Cb ➔ ouput = 0x**789***0011223344*(+LRC)
Protocole Iso 2b ➔ output = **789***0000287454020*

T6.3 - Lecteurs TTL - S31 - Badge ET Touche

Les touches et l'UID/Id seront envoyés dans des trames qui se suivent.
Le format des trames chiffrées sera :

Data ***12 octets***	***Valeur aléatoire*** ***2 octets***	***CRC*** ***2 octets***

Trame touches

+

Data ***12 octets***	***Valeur aléatoire*** ***2 octets***	***CRC*** ***2 octets***

Trame1

Data ***12 octets***	***Valeur aléatoire*** ***2 octets***	***CRC*** ***2 octets***

Trame 2

Data ***12 octets***	***Valeur aléatoire*** ***2 octets***	***CRC*** ***2 octets***

Trame …

T6.4 - Lecteurs TTL - S31 - Badge OU Touche

Les trames touches chiffrées et les trames UID/Id chiffrées AES avec la clé de chiffrement renseignée dans « Clé AES de chiffrement de la sortie » sont envoyées indépendamment.

Data ***12 octets***	***Valeur aléatoire*** ***2 octets***	***CRC*** ***2 octets***

Trame1chiffrée
ou Trame
Touche chiffrée

Data ***12 octets***	***Valeur aléatoire*** ***2 octets***	***CRC*** ***2 octets***

Trame 2 chiffrée

Data ***12 octets***	***Valeur aléatoire*** ***2 octets***	***CRC*** ***2 octets***

Trame …chiffrée

Exemple pour touche 1 appuyée

Format 4 bits au sein d'une trame correspondante au protocole de sortie
Data (12o) = 0x10 00 00 00 00 00 00 00 00 00 00 00

Format 4 bits seuls avec chronogrammes correspondants au protocole de sortie
Data (12o) = 0x10 00 00 00 00 00 00 00 00 00 00 00

Format 8 bits seuls avec chronogrammes correspondants au protocole de sortie
Data (12o) = 0xE1 00 00 00 00 00 00 00 00 00 00 00

Exemple pour touches 1, 5, 7 appuyées

Format 4 bits – n touches au sein d'une trame correspondante au protocole de sortie
Protocole W3i : Data (12o) = 0x00 01 57 00 00 00 00 00 00 00 00 00
Protocole W3Ca : Data (12o) = 0x00 00 01 57 00 00 00 00 00 00 00 00
Protocole ISO2B : Data (12o) = 0x00 00 00 01 57 00 00 00 00 00 00 00

T6.5 - Lecteurs RS232 / RS485 - R32/S32/R33/S33 - Badge OU Touche

Les touches seront codées au format 8 bits comme représenté ci-dessous :

Valeur de la touche pressée MSB … LSB		
'0'	11110000	0xF0
'1'	11100001	0xE1
'2'	11010010	0xD2
'3'	11000011	0xC3
'4'	10110100	0xB4
'5'	10100101	0xA5
'6'	10010110	0x96
'7'	10000111	0x87
'8'	01111000	0x78
'9'	01101001	0x69

Mode unidirectionnel

Se référer à *T5.1 - Mode de communication unidirectionnel* pour plus de détails concernant les options d'empaquetage possibles de la trame.

La structure de la trame sera de la forme :

1 octet	***1 octet ****	***1 octet***	***1 octet***	***1 octet***	***1 octet***
STX	*Code Touche*	*LRC*	*0x0D*	*0x0A*	*ETX*

** Multiplié par deux si l'option ASCII est activée.*

Mode bidirectionnel

Se référer à *T5.2 - Mode de communication bidirectionnel* pour plus de détails sur la communication bidirectionnelle du lecteur.

En mode Badge Ou Touche, la récupération des données de l'identifiant est réalisée via la commande ***Output_Protocol***. Les **données du clavier** sont récupérées via la commande décrite ci-dessous :

Output_Keyboard

Description

Cette commande est générée par le lecteur lors de l'appui sur une touche clavier en mode Badge OU Touche.

Lecteur : CTRL CommandCode AAh 55h L_{out} $Data_{out}$

CommandCode *2 octets :* 01h 07h

L_{out} *2 octets :* 00h 03h

$Data_{out}$ *3 octets :* 00h 01h + Valeur de la touche lue récupérée au format 8 bits.

Système : ACK L_{in} 00h 00h

ACK *2 octets :* 01h 07h
L_{in} *2 octets :* 00h 00h

Exemple pour la touche 0 et un lecteur a l'adresse RS485 0:
Lecteur : 02 00 0B 01 00 00 00 01 07 AA 55 00 03 00 01 F0 03 75.
Réponse système : 02 00 04 01 00 01 07 00 00 46 7C.

T6.6 - Lecteurs RS232 / RS485 - R32/S32/R33/S33 - Badge ET Touche

L'encodage des touches se fait au format 8bits, le nombre de touches à appuyer est configuré par le badge de configuration SCB.

Mode unidirectionnel

Se référer au chapitre *T5.1 - Mode de communication unidirectionnel* pour plus de détails concernant les options d'empaquetage possibles de la trame.

Concernant la configuration *Badge Et Touche*, la structure de la trame sera de la forme :

1 octet	***X octets***	***X octets***	***1 octet***	***1 octet***	***1 octet***	***1 octet***
STX	*Code touches**	*Données**	*LRC*	*0x0D*	*0x0A*	*ETX*

* *Multiplié par deux si l'option ASCII est activée.*

Exemple en mode *Badge ET Touche* :

- ✓ 3 Touches : *7, 8 et 9*
- ✓ Identifiant : 0x11223344 en hexadécimal et 287454020 en décimal.
- ✓ Taille du protocole : 5 octets
- ✓ Format de sortie hexadécimal : 0x*87786911223344*
- ✓ Format de sortie décimal : *8778690000287454020*

Mode bidirectionnel

Se référer au chapitre *T5.2 - Mode de communication bidirectionnel* pour plus de détails sur la communication bidirectionnelle du lecteur.

En mode Badge ET Touche, la récupération des données (code clavier et code carte) est réalisée via la commande ***Output_Protocol***.

T7 - Gestion de la biométrie

T7.1 – Format des empreintes biométriques

L'information contenant les empreintes digitales est contenue dans un fichier (MIFARE® DESFire® EV1/2) ou dans les secteurs 32 à 39 (MIFARE Plus® Level 3) définis dans les paramètres biométriques.

- ✓ A sa création, SECard définit une taille égale à : Nombre de doigts * 170 octets.
- ✓ Les templates biométriques sont écrits au format Morpho Sagem (PK_COMP).
- ✓ Mapping du fichier MIFARE® DESFire® EV1/2 ou secteur(s) MIFARE Plus® Level 3 :

MSB *LSB*

[**LenTotale**] | [**Nb Template**] | [**LenTemplate$_x$** | **Template$_x$**] ^{n}

- ✓ **LenTotale** est la longueur totale à écrire dans la puce MIFARE® DESFire® EV1 ou Plus® Level 3 sur 2 octets.
- ✓ **Nb Template** est le nombre de template (max 5), sur 1 octet.
- ✓ **LenTemplate$_x$** est la longueur du Xème template sur 1 octet.
- ✓ **Template$_x$** est le Xème template de longueur **LenTemplate$_x$**.
- ✓ n est le nombre de templates donc le nombre de doigts.

La taille maximale totale est donc de 2+5*(1+170)=857 octets car le nombre de doigts maximum est 5 et la taille maximale des templates est 170 octets (cf. Morpho Sagem).

Le nombre de secteurs écrits dans le cas d'une MIFARE Plus® Level 3 dépend du nombre de doigts.

T7.2 - Dérogation biométrique

A partir de la version 3.1, il est possible d'activer une empreinte de dérogation dans les badges compatibles biométrie. L'utilisateur ne sera pas invité à coder ses empreintes, un modèle de dérogation sera encodé à la place.
Cela permet d'autoriser ou non le lecteur à prendre en compte les badges utilisateurs qui utilisent cette dérogation.

Le motif de dérogation est défini par :

$$\mathrm{TemplateDerogation} = \mathrm{SHA2}(\mathrm{salt} \,|\mathrm{UID}, \mathrm{UIDLen})$$

- ✓ **salt** valeur fixe privée de 16 octets
- ✓ **UID** le numéro de série de la puce
- ✓ **UIDLen** longueur de l'UID

De plus les badges utilisateurs programmés en utilisant un motif de dérogation biométrique en lieu et place d'une vraie empreinte issue du capteur bio, peuvent être encodé ou pas à la volée à chaque encodage.

T8 - Gestion de la biométrie + Clavier

T8.1 - Biométrie avec les empreintes dans le badge utilisateur

Mode 1 : Touche **OU** (Badge **ET** biométrie)

Le fonctionnement est identique à celui d'un Badge OU Touche, avec ajout de la lecture de l'empreinte digitale après la lecture du badge.

Mode 2 : Touche **ET** (Badge **ET** biométrie)

Le fonctionnement est identique à celui d'un Badge ET Touche, avec ajout de la lecture de l'empreinte digitale après la lecture du badge.

T8.2 - Biométrie avec les empreintes dans le lecteur

Mode 1 : Touche **OU** Biométrie.

Mode 2 : Touche **ET** Biométrie.

T9 - Biométrie dans le lecteur

Dans ce mode, les empreintes sont stockées le module biométrique Sagem.

Le module fait la comparaison des empreintes lues avec les empreintes enregistrées dans base de données du module.
Ce mode est compatible avec tous les types de puces disponibles dans SECard.

Le nombre d'utilisateurs maximum est fixé à 500 avec deux doigts par utilisateur.

Rappel : Trois badges sont nécessaires pour gérer le lecteur dans ce mode. La clé maître de ces trois badges sera la même valeur que la clé entreprise SCB mais sera diversifiée.

Attention

La taille maximum de l'ID privé qui peut être sauvegardé dans le module est 24 octets.

La première étape avant d'initialiser la base de donnée est de présenter le badge de configuration SCB au lecteur afin de le configurer en mode « Données bio dans le lecteur ».

Initialiser la base de données utilisateur

Ce badge est utilisé pour initialiser la base de données dans le module.

Mode opératoire

Avec un lecteur écran tactile le texte est :		Sans écran tactile :
	- *Initialisation de la base utilisateurs en cours*. - *Initialisation de la base utilisateurs réussie*	La LED rouge est activée et le buzzer émet deux BIP longs indiquant la prise en compte du badge.
Si une erreur survient durant la procédure :		
	- *Echec de l'initialisation de la base utilisateurs* - *Capteur biométrique non détecté ou désactivé.*	La LED rouge et le buzzer sont activés durant 1s. Le lecteur repasse alors en mode de fonctionnement normal.

Attention

L'initialisation de la base de données efface la base actuelle et donc le contenu actuel du module.

Ajouter un utilisateur

Ce badge permet d'ajouter un utilisateur dans la base de données du module biométrique. Le template d'un utilisateur est associé à son ID utilisateur (UID ou ID privé).

Lorsqu 'un badge « Ajout un utilisateur » est détecté par le lecteur, celui-ci passe en mode enrôlement pendant 6 secondes et attends un badge utilisateur.

Si le badge utilisateur est compatible avec la configuration du site, le lecteur lit l'ID utilisateur et le module biométrique s'allume pour enrôler deux doigts de l'utilisateur.

Les deux empreintes sont enregistrées dans la mémoire du module, et associées à l'ID utilisateur.

Mode opératoire

Avec un lecteur écran tactile le texte est :	Sans écran tactile :
Lorsque le badge « Ajout utilisateur" est détecté par le lecteur	
Présentez le badge utilisateur à ajouter	La LED blanche s'allume.
Lorsque le badge utilisateur est lu	
Scannez 2 doigts *2 secondes par doigt* *3 fois chaque doigt*	La LED verte s'allume et le buzzer est activé durant 400ms, ensuite la LED blanche s'allume et l'utilisateur doit alors présenter son premier doigt trois fois puis son second doigt trois fois. (le module bio s'allume et s'éteint successivement pour la saisie de chaque doigt).
Lorsque l'enrôlement est fini :	
Enrôlement réussi	La LED verte et le buzzer sont activés durant 400ms.
Si une erreur survient durant la procédure :	
Echec de l'enrôlement	La LED rouge et le buzzer sont activés durant 1s. Le lecteur repasse alors en mode de fonctionnement normal.

Effacer un utilisateur

Ce badge permet de supprimer un utilisateur de la base de données.

Lorsqu'un badge "Effacer un utilisateur" est détecté par le lecteur, celui-ci passe en mode suppression pendant 6 secondes et attend un badge utilisateur. Si le badge utilisateur est compatible avec la configuration du site, le lecteur supprime l'utilisateur correspondant à l'ID utilisateur lu.

Avec un lecteur écran tactile le texte est :	Sans écran tactile :
Lorsque le badge « Effacer utilisateur" est détecté par le lecteur :	
 *Présentez le badge utilisateur à supprimer*	La LED blanche s'allume.
Lorsque le badge utilisateur est lu :	
	La LED verte et le buzzer sont activés durant 400ms, puis la LED blanche est activée durant l'effacement en mémoire des empreintes (trop rapide pour être pour visible).
Lorsque l'effacement est fini :	
 *Utilisateur supprimé*	La LED verte et le buzzer sont activés durant 400ms.
Si une erreur survient durant la procédure :	
 *Echec de la suppression*	La LED rouge et le buzzer sont activés durant 1s. Le lecteur repasse alors en mode de fonctionnement normal.

Autre textes pour le lecteur avec écran tactile :

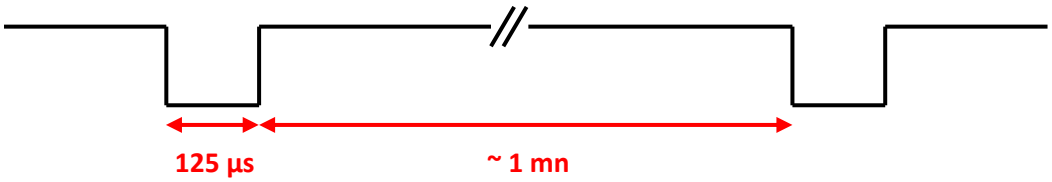
Indiquer que la base de données est vide	*Attention, la base Utilisateurs est vide*
Indiquer que la base de données est pleine	*Attention, la base Utilisateurs est pleine*
Indiquer que la base de données n'existe pas	*Base utilisateurs inexistante*
Indiquer que l'ID du badge est déjà présent dans la base de données	*Badge utililisateur déjà enregistré*
Indiquer que les empreintes sont déjà présentes dans la base de données	*Empreintes déjà enregistrées*

T10 - Signal de vie

T10.1 - Lecteur TTL

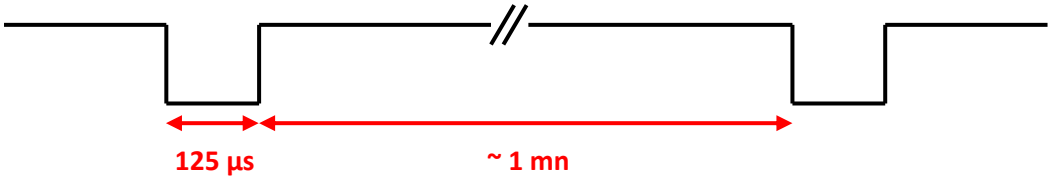
Lorsque cette fonction est activée, le lecteur émet un signal environ toutes les minutes sur les lignes Data/DATA1.
Le signal de vie peut être activé de façon générique (*Generic life signal – un signal de vie commun à tous les lecteurs*) ou spécifique (*Specific life signal – signal de vie différent pour chaque lecteur*).

Signal de vie générique *:*

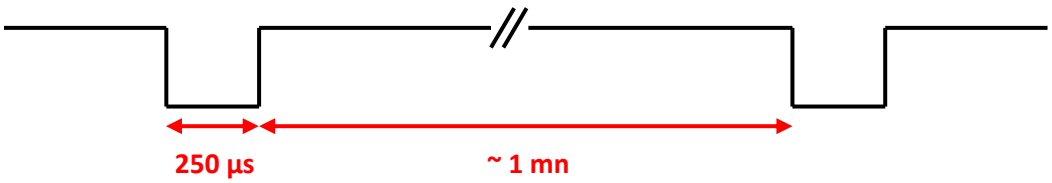


Signal de vie spécifique *:*

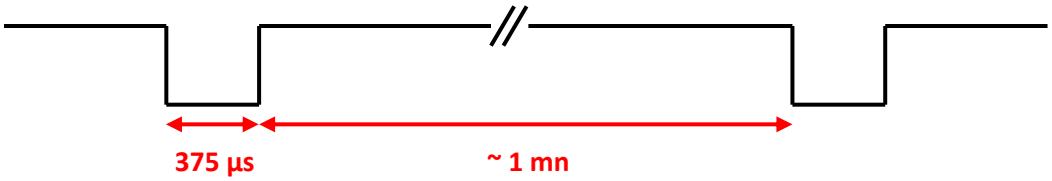
LXS-R31 & LXS-S31 & MXS-R31 & MXS-S31 & ATX-R31 & ATX-S31



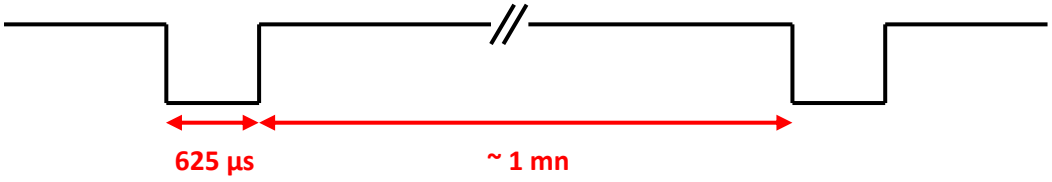
LX1-R31 & LX1-S31



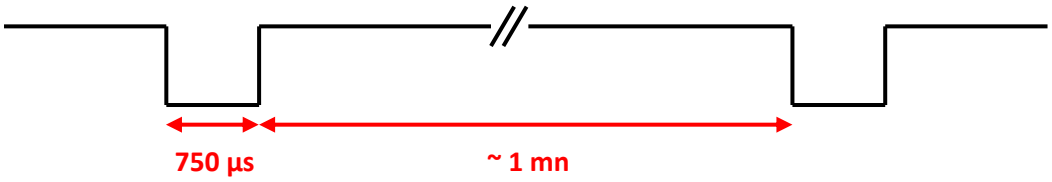
MS-R31 & MS-S31 & LDS-R31 & LDS-S31



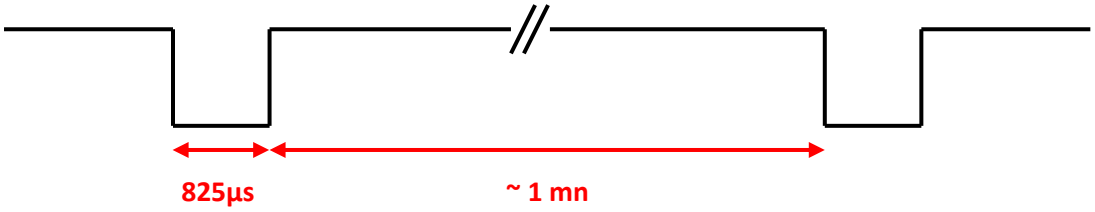
LXE-R31 & LXE-S31



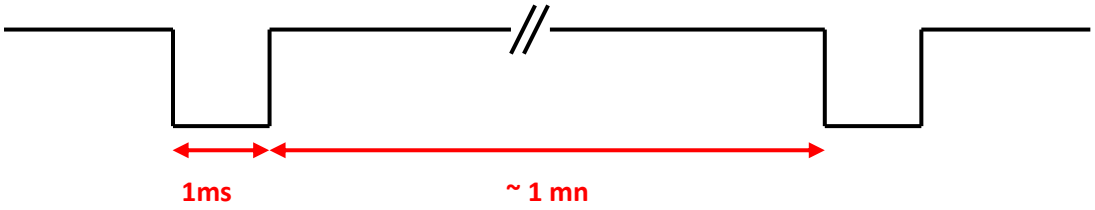
CLA-R31 & LXC-R31 & CLA-S31 & LXC-S31



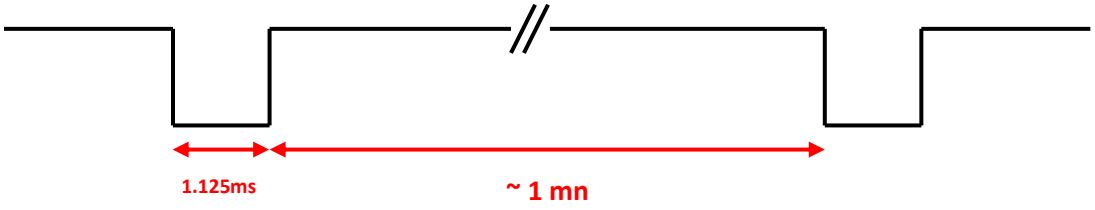
WAL-R31 & WAL-S31



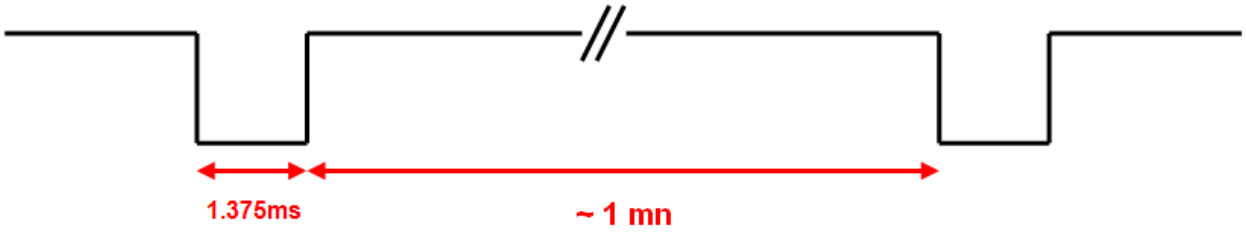
ARC-R31 & ARC-S31



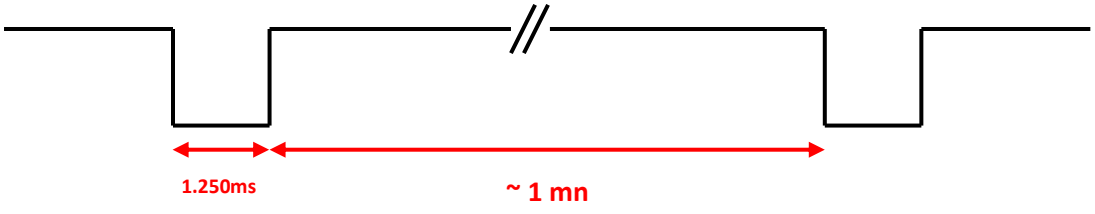
ARC1-x31



ARC1S-x31



ARCS-x31



T10.2 - Lecteur série bidirectionnel

Le lecteur envoie en clair sur la série le code commande 0x0102.

Donnée = x * 125us (exemple: pour ARC-R32/R33, x = 8)

T10.3 - Lecteur série unidirectionnel

Le lecteur envoie sur la série le code commande:

Generique: 0x50

Specifique:

ARC-R32/R33= 0x61

ARC1-R33 = 0x62

ARCS-R33 = 0x63

ARC1S-R33 = 0x64

Specifique Gamme E:

LXS-R32/R33= 0x50

MS-R31 = 0x52

LXE-R32/R33 = 0x54

LXC-R32/R33 = 0x55

WAL-R32/R33 = 0x56

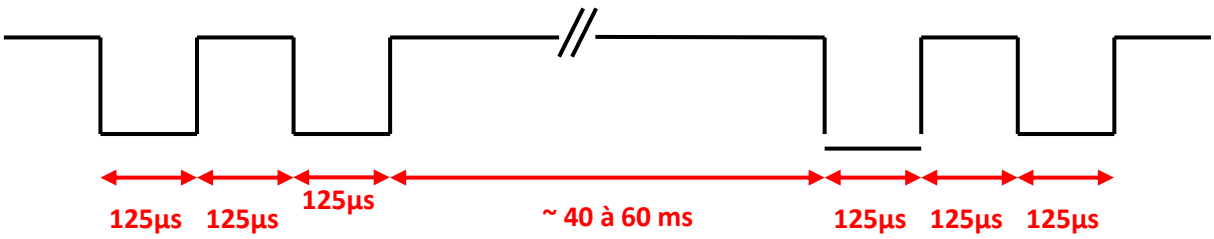
T11 - Signal d'arrachement

Lorsque cette fonction est activée, le lecteur mémorise au démarrage l'état initial de son entrée « ***Switch*** » ou de l'accéléromètre.

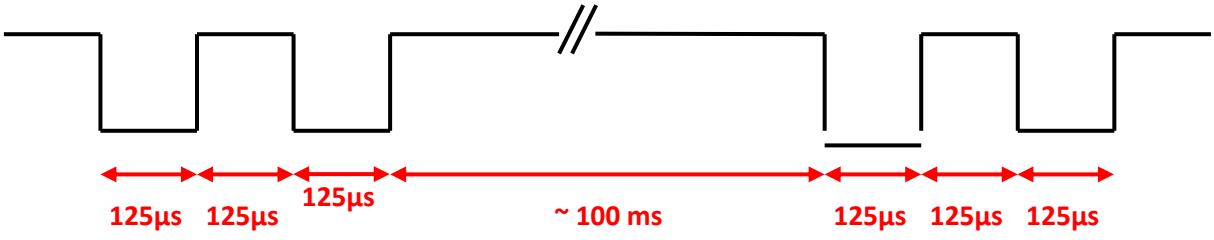
T11.1 - Lecteur TTL

A chaque instant où cet état change, le lecteur émet un signal d'arrachement sur la ligne « ***Data/Data 1*** ». Lors de l'arrachement, par défaut ou si l'option est activée, la forme du signal émis sur la ligne « ***Data/Data 1*** » est :

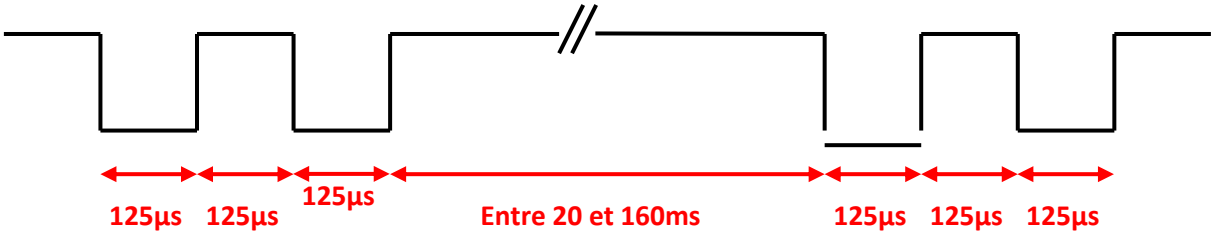
R31-X & S31-X



R33-X + INT-R33-E



R33-X + INT-R33-F



T11.2 - Lecteur série bidirectionnel

Le lecteur envoie en clair sur la série le code commande 0x0103.

T11.3 - Lecteur série unidirectionnel

Le lecteur envoie sur la série le code commande 0xAA.

T12 - ID d'arrachement

Lorsque cette fonction est activée, le lecteur mémorise au démarrage l'état initial de l'accéléromètre.
Une valeur spécifique est envoyée au format du protocole en cours. Cette valeur n'est envoyée qu'une seule fois lorsque l'arrachement est détecté.

Cette valeur peut-être sur :
- 16 octets maximum pour les lecteurs en sortie Wiegand et les lecteurs séries.
- 10 octets maximum pour les lecteurs en sortie ISO.

Remarque : si la taille du protocole en cours est supérieure à cette valeur, le lecteur fera un bourrage à zéro.

T13 - Signal de vie / arrachement mutualisés

Disponible uniquement pour les lecteurs R31/S31 et R33+INTR33E

Lorsque cette option est activée, le lecteur émet chaque seconde la trame signal de vie spécifique.
Le format de la trame dépend du protocole en cours.

Si l'entrée d'arrachement « *Switch* » ou l'accéléromètre change d'état, le signal émis chaque seconde change également.
La donnée « *Arrachement* » est alors envoyée dans la trame spécifique en remplacement de la donnée « *Vie* ».

✓ *Exemple d'un signal de vie (fonctionnement normal) émis chaque seconde :*

- Protocole ISO2 :

  Start Sentinel + Octet de signal de vie + End Sentinel + LRC

- Wiegand :

  Octet de signal de vie + LRC

✓ *Exemple d'un signal d'arrachement (changement d'état du «Switch » ou de l'accéléromètre) émis chaque seconde :*

- Protocole ISO2 :

  Start Sentinel + Octet de signal d'arrachement + End Sentinel + LRC

- Wiegand :

  Octet de signal d'arrachement + LRC

Note :

Cette option n'est pas disponible pour le Wiegand 26 bits 3i.

Si cette option est activée et que le paramètre de clignotement de la LED au repos l'est également, alors le délai du clignotement ne peut pas être inférieur à 400 ms.

T14 - Ligne de commande

T14.1 - Description

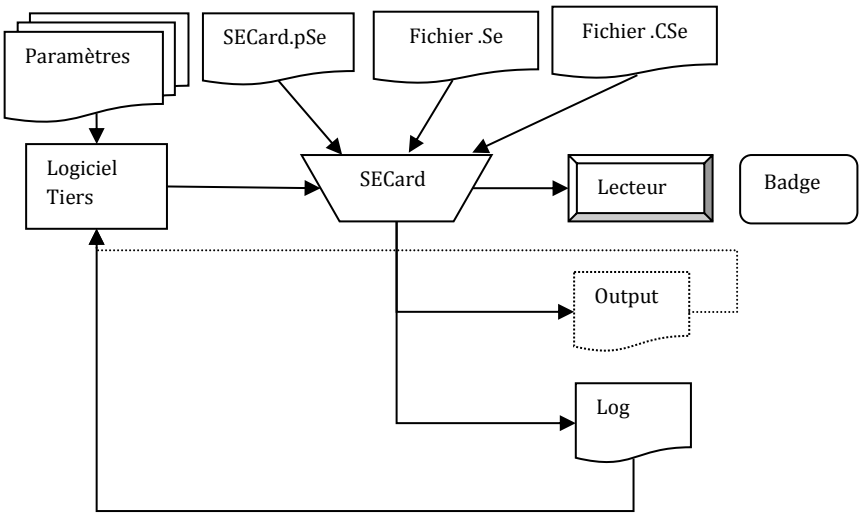
SECard inclus un mode « ligne de commande » permettant une exécution « en tache de fond » (sans aucune interface graphique), ce qui permet de s'interfacer avec une autre application. Cette dernière lancera donc SECard de manière invisible pour l'utilisateur.

SECard permet de :

1. Charger des configurations spécifiques à partir de fichiers de configuration en clairs ou chiffrés.
2. Utiliser la configuration courante.
3. Réaliser des opérations d'encodage et de lecture de tags.
4. Fournir les résultats dans un fichier utilisateur.
5. Enregistrer toutes les opérations réalisées.

Le mode ligne de commande permet donc d'interfacer l'encodage/lecture de tags (ou tout autre opération que SECard peut réaliser), avec une application tierce.
Pour que l'application lance SECard en ligne de commande, un simple appel logiciel avec les bons paramètres suffit.

Le processus est résumé dans le schéma suivant :



T14.2 - Utilisation

Pour exécuter SECard en ligne de commande il suffit :

- soit de lancer l'exécutable dans une fenêtre « Ligne de commande » de Windows avec des paramètres,
- soit de faire un fichier batch contenant une ligne faisant appel à SECard avec des paramètres,
- soit de lancer SECard via une autre application qui permet de renseigner des paramètres.

La ligne de commande est :

secard[.exe] -u userid -p password [-a action] [-i|I config.Se] [-q PSEPassword] [-o outputfile.txt] [-l|L logfile.log] [-d dataTOencode] [-h] -v

Paramètres :

-u : spécifie l'utilisateur qui va lancer SECard, ce paramètre est obligatoire si pas - I
1=Utilisateur
2=Super Utilisateur
3=Administrateur

-p : spécifie le mot de passe utilisé par -u, ce paramètre est obligatoire si pas - I

-q : spécifie le mot de passe utilisé par le fichier pse si verrouillé.

-a : spécifie l'action à réaliser par SECard :

- UEncode encode un badge utilisateur, nécessite -d
- URead lit un badge utilisateur, nécessite -o
- UID lit l'UID d'un badge, nécessite -o
- KEncode encode un badge SKB
- KRead lit un badge SKB, nécessite -o
- CEncode encode un badge SCB
- CRead lit un badge SCB, nécessite –o
- CSe2PSE convertit un fichier CSE en fichier PSE

-b : spécifie la vitesse de communication de l'encodeur
0 : 9600 ; 1 : 19200 ; 2 : 38400 ; 3 : 57600 ; 4 : 115200

-d : spécifie les données utilisateur à encoder, chaîne texte représentant l'ID (hexadécimal/décimal).
Attention, cette chaîne doit être compatible avec le fichier de configuration courant automatiquement chargé par SECard, ou le fichier Se/CSE importé.

-i| I : importe un fichier de configuration en clair (si -i minuscule) .Se, et remplit les paramètres correspondants dans SECard. Exécuté avant l'action définie par -a.
Si le paramètre - I (majuscule) est utilisé alors le fichier d'import de configuration est chiffré, et contient le login et le mot de passe associé (les paramètres -u et -p sont ignorés, de même pour -q).

-o : nom du fichier de résultat contant les opérations réalisées par –a, si l'action réalisée est CSe2PSE le fichier de résultat sera le fichier PSE crée.

-l|L : nom du fichier de log, contenant le statut de toutes les opérations réalisées par -a.
l pour afficher un log minimal (OK|NOK) dans le fichier, ou L pour un log complet.

-v : verbeux log à utiliser avec -l|L. Spécifie si le log doit se faire en mode verbeux, pour cela l'utilisateur qui lance la ligne de commande doit être connecté en tant qu'administrateur ou en power user avec les droits de gestions des clés Lecteur et RFID, sinon le log sera classique. Attention en mode verbeux le log génère un fichier (SECard_VerboseLOG.txt) qui contient les valeurs des clés Lecteurs et RFID.

-h : affiche l'aide dans une fenêtre DOS si lancé depuis DOS et dans une fenêtre Windows si lancé depuis Windows avec IHM, (exclusif, le reste est ignoré).

La ligne de commande SECard n'est pas bloquante, elle rend la main immédiatement.

Par contre, pour qu'il n'y ait pas de problème d'accès au lecteur/configuration, le mode ligne de commande est exclusif, il ne peut pas y en avoir plus d'un en même temps.
Cependant, il peut y avoir un autre SECard classique (pas en ligne de commande) d'exécuté (attention tout de même au partage du port de communication).

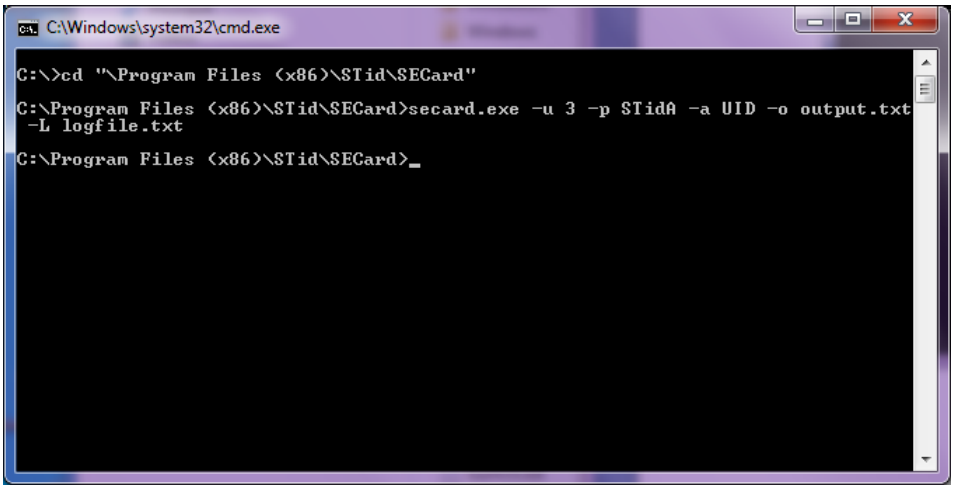
En mode ligne de commande, SECard utilisera automatiquement les paramètres contenus dans le fichier de configuration par défaut ou celui sélectionné par l'utilisateur. Ainsi, il suffira de définir la configuration utilisateur en lançant SECard en mode classique (avec l'IHM) et de sauvegarder cette configuration de manière à ce qu'elle soit chargée automatiquement au lancement de SECard.

T14.3 - Console de commande

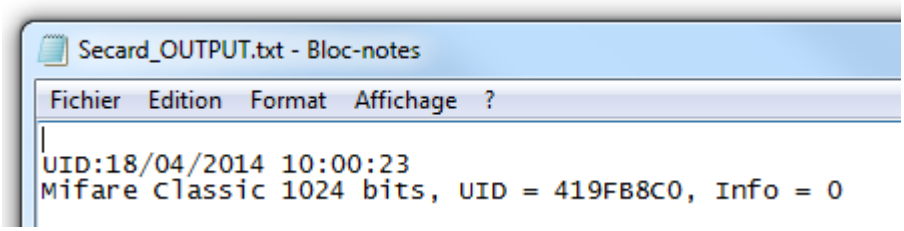
Ouvrir une console de commande Windows : exécuter cmd.exe.
Dans la fenêtre qui s'ouvre, se positionner dans le répertoire d'installation de SECard :

cd \Program Files\STid\Secardvxxx\ ou cd \Program Files (x86)\SECardvxx\

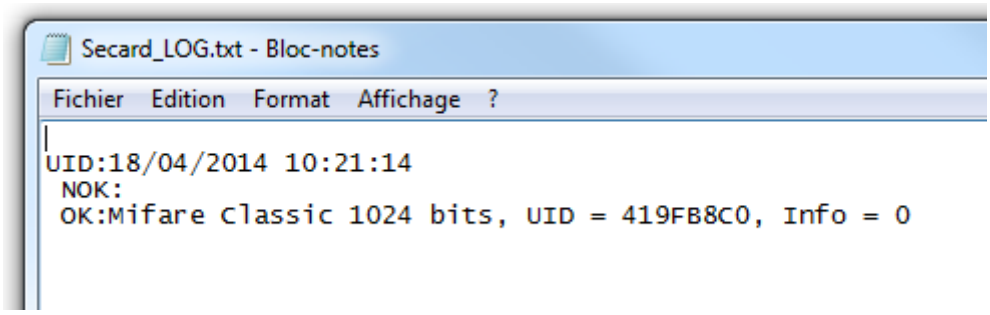
Puis, taper la ligne de commande désirée.
Par exemple, pour récupérer l'UID d'un badge :
Mettre un badge RFID devant le lecteur allumé et configuré dans SECard puis taper :



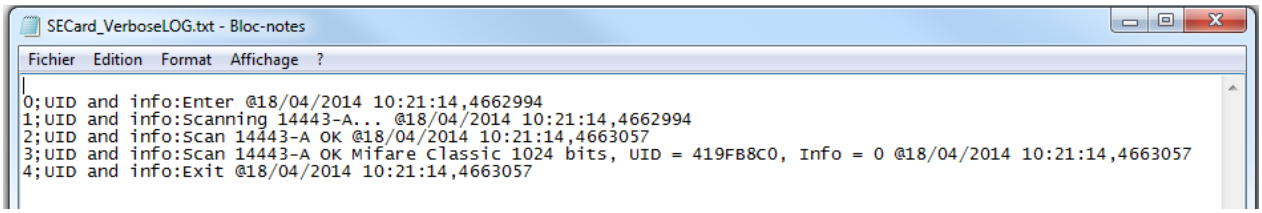
Le résultat de l'opération (donc l'UID du badge présenté au lecteur) est consigné dans le fichier output.txt.



Si l'opération s'est correctement déroulée, cela sera consigné dans le fichier de log logfile.txt.



Si l'option –v verbose est utilisée le fichier de log créé est :



T14.4 - Fichier batch

Grâce aux fichiers batch (exécutable par l'interpréteur de commande de la console de commande Windows) et aux commandes acceptées par SECard, une multitude de scénarios est envisageable.

Par exemple, pour récupérer non pas l'UID d'un seul badge mais l'UID de dix badges, le fichier batch (UIDof10.cmd) est :

```
REM @echo off
for /l %%d in (1,1,10) ^
do (secard.exe -u 3 -p STidA -a UID –o output.txt –L logfile.txt)
```

Les UID des dix badges présentés seront collectés et ajoutés séquentiellement au fichier output.txt.
Attention à être en séquence avec la présentation des différents badges au coupleur RFID. A cette fin, il est possible d'ajouter un sleep de x secondes avec la ligne ping 127.0.0.1 –n x juste après la ligne secard.exe :

```
REM @echo off
for /l %%d in (1,1,10) ^
do (secard.exe -u 3 -p STidA -a UID –o output.txt –L logfile.txt
ping 127.0.0.1 –n 5)
```

De même, pour encoder des IDs contenus dans un fichier texte IDsList.txt (un par ligne), utiliser le fichier batch suivant :

```
@echo off
for /F %%i in (IDsList.txt) ^
do (
echo Presenter le badge a programmer avec %%i
secard.exe -u 3 -p STidA -a UEncode -o output.txt -L log.txt -d %%i
echo 5 secondes pour prendre la badge suivant
ping 127.0.0.1 -n 5 > NUL
)
```

T14.5 - Applications tierces

Paramétrage

Il est possible d'utiliser SECard en ligne de commande dans des applications tierces (par exemple l'impression).

Pour cela, lancer l'application, créer le design de la carte en se référant au manuel de l'application.
Ensuite sélectionner ou activer « Carte à puce » puis sélectionner « Ligne de commande ».
Configurer l'utilisation de la RFID.
Sélectionner l'exécutable de SECard typiquement localisé dans c:\Program Files\STid\SeCard Vx.x.x\SeCard.exe.
Il faut définir l'emplacement du fichier retour, si ce fichier n'existe pas, créer le fichier CMDlineLOG.txt.
Définir ensuite l'accès au champ (soit une valeur statique, soit des valeurs issues d'une base de données).

Pour finir, renseigner les arguments de la ligne de commande de SECard :

Remarque : Si les paramètres -o et/ou -l|L sont utilisés avec des fichiers ayant des noms longs et/ou contenant des espaces ou des caractères spéciaux, il faut les encadrer par des " ".

- -u 3 -p STidA –a UEncode –o "C:\Program Files (x86)\STid\SeCard\output.txt" –l "C:\Program Files (x86)\STid\SeCard\CMDlineLOG.txt"

- -d 11223344 ou –d <valeur du champ de données>

Gestion des erreurs

❖ **L'application tierce n'arrive pas à dialoguer avec SECard**
Vérifier le lancement de SECard par l'application tierce. Pour cela, il suffit de lancer le « Gestionnaire de tâche » de Windows et de vérifier que SECard apparait (au moins un instant) dans la liste des processus. Si ce n'est pas le cas, vérifier la ligne de commande et le chemin d'accès au fichier SECard.exe.

Si SECard est bien lancé mais que ça ne fonctionne toujours pas, lancer SECard avec l'option -L (l majuscule) au lieu de -l (l minuscule) suivit du nom de fichier de log. SECard enregistrera alors toutes les opérations qu'il effectuera avant de se fermer. Relancer l'opération. Vérifier le contenu du fichier de log :

- « *Mauvaise longueur de donnée reçue (trop petite)*» : le port de communication est mal configuré dans SECard.
  Ouvrir SECard classiquement et modifier le port de manière à le faire correspondre avec le coupleur RFID, vérifier la vitesse, enregistrer le fichier de paramètres de SECard en fermant.

- « *Mauvais fichier de paramètre, corrompu ou port de communication invalide* » : le fichier de paramètres courants dans SECard n'est pas enregistré correctement pour le mode ligne de commande. Avec un éditeur de texte ouvrir le fichier SECard.gcf qui se trouve dans le répertoire d'installation de SECard. Chercher la clé « Settings » dans la zone « File », il s'agit du nom du fichier de paramètres courants de SECard. Vérifier que le nom du fichier utilise un chemin absolu, c'est-à-dire de la forme « C:\Program Files (x86)\STid\SECard\SECard.pse » et PAS de la forme « .\SECard.pse » (qui est la configuration par défaut lors de l'installation). Si ce n'est pas le cas, il faut le modifier, pour cela deux possibilités, soit directement dans le fichier SECard.gcf, soit ouvrir SECard classiquement, aller dans le menu « Fichiers » et « Enregistrer » le fichier de paramètres à l'endroit désiré (il est possible d'écraser le fichier de paramètres par défaut si c'est celui utilisé).

❖ **SECard n'arrive pas à dialoguer avec l'application tierce**

La communication entre SECard et l'application se fait grâce au fichier de log. Si la communication est rompue c'est qu'il y a un problème sur le fichier utilisé.
Vérifier que le nom du fichier défini comme étant le fichier de retour dans l'application tierce, soit le même que le nom du fichier de log définit par la ligne de commande de SECard, et vérifier que son nom soit bien encadré par des " " s'il contient des espaces ou des caractères spéciaux. Vérifier les droits d'accès à ce fichier.

T14.6 - Fichier d'import de configuration

Le fichier suivant détermine tous les paramètres compatibles avec l'import de fichier de configuration en clair, et chiffrée lors du lancement de SECard en ligne de commande.
En l'état, ce fichier spécifie tous les paramètres lecteur, SSCP et uniquement les paramètres DESFire.

Si les valeurs ACCESSLevel et Password ne sont pas définies dans le fichier d'import de configuration et que la ligne de commande indique l'option –I alors SECard utilisera les valeurs par défaut, c'est-à-dire ACCESSLevel=3 et Password=STidA.

```
;; SECard command line import configuration file
;; defines all parameters available in SECard command line mode from V3.2.0

[Login]
;Values are ONLY defined if import configuration file is Encrypted (.CSe)
;Access level : 1=User, 2=PowerUser, 3=Administrator
ACCESSLevel=3
;Password for corresponding user
Password=STidA

;If command line action is "CSe2PSE" you have to defined passwords that will be saved in PSE file
PSEUserPassword=STidU_123
PSEPowerUserPassword=STidP_123
PSEAdministratorPassword=STidA_123
;Read (Open) password is unconstrained, default is empty (no password)
PSEReadPassword=


;PowerUser Rights : 1=Enable, else disable
;Load/Save configuration file
LSconf=0
;Reset conf counters
Rcc=0
;Create/Read SKB
CRSKB=0
;Create/Read SCB
CRSCB=0
;Create/Read User cards
CRUserCards=0
;Manage Reader communication keys
MRCKeys=0
;Manage RFID keys
MRFIDKeys=0
```

```
[ReaderFamily]
;0 for LXS family
;1 for ARC family
;2 for WAL family
ReaderFamilyID=1

[CompatibilityVersion]
; Override .gcf compatibility mode

; For LXS family
; 0 = SeCard v1.1.x or Unknown;
; 1 = SeCard v1.2.x
; 2 = SeCard v1.3.x
; 3 = SeCard v1.4.x
; 4 = SeCard v1.4B.x
CompatibilityVersion= 3

; For ARC family
; 0 = SECard v2.0.0
; 1 = SECard v2.1.0
; 2 = SECard v2.2.0
; 3 = SECard v3.0.0
; 4 = SECard v3.1.0
; 5 = SECard v3.2.0
ARCCompatibilityVersion=3

; For WAL family
; 0 = SECard v2.1.0
; 1 = SECard v2.2.0
WALCompatibilityVersion=0


[SSCP]
COMPort=COM3

;Baudrate = 9600,19200,38400,57600,115200
Baudrate=38400

;Security mode, Plain=0, Sign=1, Enc=2, SignEnc=3
SecurityMode=0

;To use SecurityMode>0 we need keys !
;WARNING: if you use SSCP keys, this file should be enciphered to CSe file
SSCPSignKey=A087754B7547481094BE
SSCPEncKey=E74A540FA07C4DB1B46421126DF7AD36




[Reader]
;SCB company key
SCBKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Change=0
SCBNewKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

```
;Reader reference
;0=R31E/103
;1=R31E/Ph5/Ph1
;2=S31E/Ph5
;3=R33E/Ph5 + INT-R33E
;4=R32E,R35E/Ph5
;5=S32E,S35E/Ph5
;6=R33E/Ph5
;7=S33E/Ph5
;8=S33E/Ph5+INT-E-7AA/7AB
ReaderReference=1

;BiometricActivation available for R31E/103,R31E/Ph5/Ph1 and S31E/Ph5  readers
BiometricActivation=0

;Save user keys in memory
SaveEEPROM=0

;Erase keys at tamper switch activation
EraseKeys=0

;Tamper switch signal activation
TamperSwitch=0

;On tamper activation keeps LED red as default
TamperKeepLEDRed=0

;Mutual life signal and Tamper switch signals available for R31E/103,R31E/Ph5/Ph1,S31E/Ph5 and R33/Ph5+INT-R33E readers
Mutual=0
;Life signal 1 byte
Life=0C
;Tamper signal 1 byte
Tamper=1C

;KeyPad activation available for R31E/103,R31E/Ph5/Ph1,S31E/Ph5,R32E,R35E/Ph5,S32E,S35E/Ph5,R33E/Ph5,S33E/Ph5
KeyPadActivation=0

;If keypad activated Badges/keys mode
;MKmode, =0 Badge OR Key, =1 Badge AND Key
BKmode=0

;KeypadFormat 0=4bits framed, =1 4 b, 2=8 b,3=4b Keys framed
KeypadFormat=2

;KeyPad nb keys [1..9]
KeyPadNbKeys=1

;Enable/disable Tagtype
MIFAREClassicTagEnable=0
MIFAREPlusTagEnable=0
MIFAREDESFireTagEnable=1
MIFAREUltraLightTagEnable=0
CPS3TagEnable=0
```

```
MoneoTagEnable=0
125kHzTagEnable=1
NFC_HCEEnable=0

;V3.0.0
;TagType
BlueMobileID=1
;Blue MobileID Configuration Activation
BlueMobileIDActivation=1
;DESFire Confiugration Activation
DESFireConfigurationActivation=1

;PUPI ISO14443-3B
PUPIEnable=1
PUPIMSB=1
PUPISign=0
PUPISignKey=FFFFFFFFFFFFFFFFFFFF

;UID/ID range, From=To=RandgeFrom=00000000=Disabled
RandgeFrom=00000000
RandgeTo=00000000

;SiteCode
ReaderSiteCode=10BF

;Protocol data size
ProtocolSize=5

;For R31/S31/INT-R33E
;ProtocolID 0=W3i (24bits),1=Iso 2H (32bits),2=Iso 2S (32bits),3=Iso 2B (40bits),4=W3Ca (32bits),5=W3Cb (40bits),6=W3La (32bits),7=W3Lb (40bits),8=W3T (64bits),9=Iso custom size,10=Wiegand LRC custom size,12=Wiegand custom size,13=Wiegand 34 bits - 3Eb,14=Wiegand 35 bits - 3W,15=Wiegand 37 bits - 3V
ProtocolID=13

;For R32/S32/R33/S33
;SerialConfiguration
;Baudrate : 0=9600,1=19200,2=38400,3=57600,4=115200
SCBaudrate=0
SCRS485Adr=0
SCBidirectionnal=0
;Radix : 0=Hexa, 1=Decimal
SCBase=0

SCNoLeadingZeros=1
SCASCII=1
SCLRC=0
SCCRLF=1
SCSTXETX=0

;Security mode (SSCP bidirectional) Plain=0, Sign=1, Enc=2, SignEnc=3
SCSecurityMode=0
SCSignKey=FFFFFFFFFFFFFFFFFFFF
SCChangeSignKey=0
SCNewSignKey=FFFFFFFFFFFFFFFFFFFF
SCEncKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

```
SCChangeEncKey=0
SCNewEncKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

;Life signal :0=Disabled, 1=Generic,2=Specific
LifeSignal=0

;Output encipherment AES key for S31 reader
OutEncKey=000102030405060708090A0B0C0D0E0F
OutEncChange=0
OutNewEncKey=000102030405060708090A0B0C0D0E0F

;;For LXS Family
;Default LED action Color: Off=0, Green=1,Red=2,Orange=3
DefActLED=3
DefActLEDBlink=0
DefActLEDBlinkDuration=4
;Card detection action LEd Color: Off=0, Green=1,Red=2,Orange=3
DetActLED=3
;For WAL reader, used only if WALDetectionLEDBlinkTimes=0
DetActLEDDuration=4
DetActBuzzDuration=4

;;For WAL Family, LED Color in RGB, allowed values are only 00 or FF for each byte
;Yellow,use DefActLEDBlink and DefActLEDBlinkDuration to select blinking
WALDefaultLEDColor=FFFF00

;Yellow
WALDetectionLEDColor=FFFF00
; Nb of LED blink at badge detection, cannot be used if DetActLEDDuration >0
; so to use it set DetActLEDDuration to 0 and set blink times here
WALDetectionLEDBlinkTimes=0


;;For ARC Family
;;use SECard selection color window to get RGB code of a color
;Default LED action Color: RGB 3 bytes hexa
;orange
ARCDefLEDColor=FF6400
;0=Off,1=Fixed,2=Blinking,3=Pulse,4=Rainbow
ARCDefLEDMode=1
;Blink duration [1..31] x100ms
ARCDefLEDBlinkDuration=4
;Pulse speed
;Slow=0, Medium=1, Fast=2
ARCPulseSpeed=1
;Card detection action LED Color: RGB 3 bytes hexa
;Green
ARCDetectionLEDColor=00FF00
;BlinkTimes [0..5]
ARCDetectionBlinkTimes=0
;ARCDetection LED duration x100ms
ARCDetectionLEDduration=4
;ARCDetection Buzzer duration x100ms
ARCDetectionBuzzerduration=4
```

```
;Added in V3.0.0 For ARC-S ARC1-S and ARC1 v2, user can select buzzer sound level
;0=Low, 1=Medium, 2=Loud
BuzzerSoundLevel=2

;;External control LED Color available for ARC and WAL series
;For ARC : RGB 3 bytes hexa
;For WAL : RGB 3 bytes hexa, allowed values = FF or 00
;Blue
ExtLED1Color=0000FF
;Yellow
ExtLED2Color=FFFF00
;Pink
ExtLED1LED2Color=FF00FF


;;For ARC and WAL Families AccelerometerSensitivity defines accelerometer sensibility
;0=Low,1=Normal,2=High
AccelerometerSensitivity=1

;Direct buzzer
DirectBuzzer=0
;Enable external LED/Buzzer control
EnableExtBuzzLED=0
;Polling period x100ms
ExtPolPeriod=1


;Biometric settings
; Security level [1..3] 3 is highest security
BioSecurityLevel=1
; Threshold level [0..10]
BioThreshold=5
; Nb of finger to enroll [1..5]
BioNb2Enroll=1
; Nb of finger to check [1..5] <= BioNb2Enroll
BioNb2Check=1
; Minutiae capture consolidation
BioConsolidation=0


;ARC Enable Eco mode
ARCEco=0
;ARC DENY UHF configuration
ARCDenyUHF=0

;;Authenticated Encryption, available for ARC from firmware version Z02
;and WAL from firmware version Z18
;EnableAE = 1 to Enable AuthenticateEncryption and 0 to disable
EnableAE=0
;If AE enabled, enter User key 16bytes
AEKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

;;Touch Screen enable=1, disable=0, available for ARC-C/F with Screen
EnableTS=0
```

;;ARC with screen defines actions and associates texts, images can only be load with SECard in normal mode (no CMDline)
;Enable(1) disable(0) Events
ARCTS_BadgeDetectionEvent=0
ARCTS_TamperingEvent=0
ARCTS_ExtLED1Event=0
ARCTS_ExtLED2Event=0
ARCTS_ExtLED1and2Event=0
;Default Text
;Text colors are in Red/Green/Blue 3 bytes hexa
ARC_TSTextColor0=0000FF
ARC_TSText1_0=Present your
ARC_TSText2_0=credential
ARC_TSText3_0=
;Badge detection text
ARC_TSTextColor1=00FF00
ARC_TSText1_1=Authorized card
ARC_TSText2_1=
ARC_TSText3_1=
;Tamper switch activation text
ARC_TSTextColor2=FF0000
ARC_TSText1_2=Alert
ARC_TSText2_2=Attempted tampering
ARC_TSText3_2=
;Biometric template
;NO TEXT for bio, hard coded in reader
ARC_TSTextColor3=000000
ARC_TSText1_3=Place your finger
ARC_TSText2_3=on the sensor
ARC_TSText3_3=
;External LED1 action text
ARC_TSTextColor4=FF0000
ARC_TSText1_4=Authorized access
ARC_TSText2_4=
ARC_TSText3_4=
;External LED2 action text
ARC_TSTextColor5=FF0000
ARC_TSText1_5=Access denied
ARC_TSText2_5=
ARC_TSText3_5=
;External LED1+LED2 action text
ARC_TSTextColor6=FF0000
ARC_TSText1_6=Free access
ARC_TSText2_6=
ARC_TSText3_6=
;ARC Reader with TS default Language
;0 for French, 1=for English
ReaderLANG=1
;ARC Reader with TS, display Ring
;1 to display
ARCTS_DisplayRing=0
;If keypad is active, you can choose to enable ScramblePad (set to 1)
ARCTS_ScramblePad=0

;Encoding type, used with UEncode command line parameter

; 0 = PId, 1 = PId AND Biometric template, 2 = Only Biometric
; See DESFire settings for Biometric template location and security
EncodingType=0

;ARC TouchScreen Display Option
;Keypad=0, DefaultImage=1
DisplayOption=0

;Blue Mobile ID Reader Configuration
;Configuration name, max 14 chars
BlueMobileIDReaderConfigurationName=AyConfigNameB
;Configuration Site Code 2 hexdecimal bytes
BlueMobileIDReaderConfigurationSiteCode=92AD
;Identification modes, disable=0, enable=1
IdModeBadge=1
IdModeSlide=0
IdModeTapTap=0
IdModeHandsFree=0
IdModeRemote=0
;Identification mode distances
;0=Contact, 1=0.5m
IdModeBadgeDistance=0
;0=Very Low, 1=Low, 2=Medium, 3=High, 4=Very high distance
IdModeSlideDistance=0
;Less than 3m=0, less than 5m=1, less than 10m=2, less than 15m=3
IdModeTapTapDistance=0
;Less than 3m=0, less than 5m=1, less than 10m=2
IdModeHandsFreeDistance=0
;Less than 3m=0, less than 10m=1, less than 15m=2, less than 20m=3
IdModeRemoteDistance=0
;Remote options =0 for Remote 1, =1 for Remote 2
IdModeRemoteOptions=0
;Requires smartphone unlocking to authenticated
;NOT required=0, required=1
BlueMobileIDReaderConfigurationRequiresUnlocking=0
;STid Mobile ID CSN configuration activation, 0 =disable, 1=enable
STidMobileIDCSN=0

;;Added in SECard V3.1.0, begin

;TamperSwitchAsProtocol define the tamper signal a the protocol, 1 to enable
;Can be selected only if Classic Tamper switch is NOT selected and if Common frame for Tamper and Life signal is NOT selected
TamperSwitchAsProtocol=0

;If TamperSwitchAsProtocol=1, the TamperSignalValue must be set
;1 to 16 hexa bytes or 1 to 10 digits decimal, radix is defined by the current Reader's protocol
TamperSignalValue=0A0B0C0D0E

;Rotation of the screen of the ARC with Touchscreen, set to 1 to enable
ARCTS_Rotation=0

;ARC keypad backlight, set to 1 to enable

```
ARCKeypadBacklight=0
;ARC on keypad pressed Buzzer, set to 1 to enable
ARCOnKeypadPressedBuzz=0
;ARC on keypad pressed flicker, set to 1 to enable
ARCOnKeypadPressedFlicker=0

;ARC Bluetooth LED flashes at BT connection, set to 1 to enable
ARCBlueLightAtBTConnection=0
;If ARCBlueLightAtBTConnection=1, change the LED color, RGB 3 bytes hexa, default=FFFFFF=White
ARCBlueBTConnectionColor=FFFFFF
;ARC Bluetooth Mode/Algo, 0=STid Mobile ID, 1=Orange PackID, 2=STid Open API
ARCBlueMode=0

;;Added in SECard V3.1.0, end


;;Added in SECard V3.2.0, begin
;Affect the LED brightness, 0=Normal brightness, 1=subdued light
ARCSubduedLED=0
;;Added in SECard V3.2.0, end



[DESFire]
;Detection type: 0=UID, 1=PrivateID, 2=Private ID but UID
DetectionType=1

;Key mode: 0=One key per file (RW), 1=Two keys per file (R and W)
KeyMode=0

;Crypto mode: 0=3DES, 1=AES, 2=AES but 3DES
CryptoMode=0

;Card Master Key
;change : 0=No change, 1=Change with NewCMK
CMK=00000000000000000000000000000000
ChangeCMK=0
NewCMK=00000000000000000000000000000000

;Application Master Key
;change : 0=No change, 1=Change with NewAMK
AMK=00000000000000000000000000000000
ChangeAMK=0
NewAMK=00000000000000000000000000000000

;Diversification
;3DES diversification key
;Enablediv=0 NO div , = 1 div enabled
;alsoCMK also diversify CMK , =0 No, =1 Enable
;NXP diversification 32 bytes padding, =0 No NXP, =1 NXP enable

Enablediv=0
3DESdivK=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
alsoCMK=0
NXP=0
```

;Added in SECard V2.2.0
;NXP Padding, active if NXP=1, 20 bytes of padding data
;If you want to read/encode French CIMS card your have to set to 80000000000000000000000000000000000000000
NXPPadding=00000000000000000000000000000000000000000

;Added in SECard V2.2.0
;If NXP diversification is selected you can also modify the MSB/LSB read direction of AID to compute diversified key
;If you want to read/encode French CIMS card your have to set to 1
AIDreversed=0

;Added in SECard V2.2.0
;FID1 Data type 0=RAW classical type and can be encoded, 1=ASCII Decimal value cannot be encoded
FID1DataType=0

;Added in SECard V3.0.0
;For NXP diversification (NXP=1), consider data as input or padding, and determine to use K1 or K2 of CMAC sub keys
;0 for padding (K2), 1 for input (K1)
InputPadd=0

;Added in SECard V3.0.0
;In case of RandomID DESFire, allow user to specify a key nb/value to get the real UID using the GetUID DESFire function
;GetUIDKeyNb=0 means AMK
GetUIDKeyNb=0
GetUIDCurrentKeyValue=00000000000000000000000000000000
ChangeGetUIDKeyValue=0
GetUIDNewKeyValue=00000000000000000000000000000000

;Format DESFire card before encoding, need CMK
;=1 Format , =0 NOT format
Format=0

;RandomID, =0 no RandomID, =1 Configure DEFire to RandomID
RandomID=0

;MSB first, =0 No, =1 Yes, Most Significant Byte First
MSBFirst=0

;Free Application Directory allowed=1 (No authentication required), no=0 (need authentication)
FreeAppDir=0

;Added in SECard V3.0.0
;Free Creation/deletion of AID's files
FreeCD=0
;DESFire Communication mode, 0=Plain, 1=MACed and 2=FullyEncphered (default value)
CommMode=2

;AID 3 bytes application identifier
AID=F51BC0

;Authenticate with Key Itself before Change Key value

```
;0=Use AMK
;1=Use KeyItself
DESFireChangeKeyKeyIDItself=0

;FID1 settings
FID1ID=0
FID1KeyID=0
;AsFID2: to encode FID1 with FID2 settings (keys)
AsFID2=0

;Keys used in KeyMode=0 (One RW key)
FID1RWKey=00000000000000000000000000000000
FID1ChangeRWKey=0
FID1NewRWKey=00000000000000000000000000000000
;+keys used in KeyMode=1 (Two keys R and W)
FID1WKeyID=2
FID1WKey=00000000000000000000000000000000
FID1ChangeWKey=0
FID1NewWKey=00000000000000000000000000000000

;Private ID/UID to encode/read
FID1size=5
FID1offset=0

;FID2 settings
FID2Enabled=0
FID2ID=0
FID2KeyID=3
;Concatenate=1: to encode/read FID1 data+FID2
;First= not Concatenate; to encode/read First FID read (authenticated)
Concatenate=0

;Write =0 NOT write FID2, =1 WRITE FID2 after (but in the same process) FID1
WriteFID2=0

;Keys used in KeyMode=0 (One RW key)
FID2RWKey=00000000000000000000000000000000
FID2ChangeRWKey=0
FID2NewRWKey=00000000000000000000000000000000
;+keys used in KeyMode=1 (Two keys R and W)
FID2WKeyID=4
FID2WKey=00000000000000000000000000000000
FID2ChangeWKey=0
FID2NewWKey=00000000000000000000000000000000

;Private ID/UID to encode/read
FID2size=5
FID2offset=0

;Biometric template location and security
;Biometric template location is forced into PId AID, and the security used is the same crypto as the PId
BioFIDId=2

;BioFIDId Read/Write keys (One key mode)
BioFIDRWKeyId=1
```

BioFIDRWKey=00000000000000000000000000000000
ChangeBioFIDRWKey=0
BioFIDRWNewKey=00000000000000000000000000000000

;BioFIDId Write keys (Two keys mode)
BioFIDWKeyId=2
BioFIDWKey=00000000000000000000000000000000
ChangeBioFIDWKey=0
BioFIDWNewKey=00000000000000000000000000000000

;Added in SECard V3.1.0, Biometric exemption : 0=Disable, 1=Enable exemption
DESFireBioExemption=0

;Added in SECard V3.1.0, Diversification for ID¨Prime MD3811, only used for SCB and NOT for DESFire emulation PrivateID encoding
DESFireIDPrimeDiversification=0

;;Added in SECard V3.2.0, begin
; DESFire EV mode : 0=EV1 mode only, 1=EV2 else EV1 mode, 2=EV2 mode only
DESFireEVMode=0

; If card and selected EV mode is EV2 then user can choose to lock card in EV2 mode only by setting DESFireLockEV2Mode=1
DESFireLockEV2Mode=0

; If card is an EV2 then user can choose to use DESFire EV2 Proximity Check by setting DESFireEV2ProxCheck=1
DESFireEV2ProxCheck=1
; and defines max time to get a response from the chip, in multiple of 100 µs
DESFireEV2ProxCheckRespTime=20

;;Added in SECard V3.2.0, end

[BlueMobileID]
;Added in SECard V3.0.0
;Virtual access card name max 14 characters
BMIDVCardName=AyVCardNamB

;Blue Mobile ID Read mode, 0 = PrivateID, 1=From DESFire configuration
;if From DESFire configuration is selected, all BlueMobileID settings will be ignored and replaced by DESFire configuration
BMIDReadMode=0

;Keytype, 0=one key, 1=two keys
BMIDKeyType=0

;KeyValues, all key are 16 hexa bytes, *Change* = 0 for non change, =1 for changing
BMIDCurrentRWK=00000000000000000000000000000000
BMIDChangeRWK=0
BMIDNewRWK=00000000000000000000000000000000
;Write keys are only used if Keytype=1
BMIDCurrentWriteK=00000000000000000000000000000000

BMIDChangeWriteK=0
BMIDNewWriteK=00000000000000000000000000000000

;Data size/offset/reverse
BMIDDataSize=5
BMIDDataOffset=0
BMIDDataReverse=0

;Display options , 0=disable, 1=enable
BMIDDisplayConfName=1
BMIDDisplaySiteCode=1
BMIDDisplayDisplayID=1
BMIDDisplayDisplayRemote1=1
BMIDDisplayDisplayRemote2=0

;;Added in SECard V3.1.0, begin
; If ARCBlueMode=1=OrangePackID, CompanyId = 2 hexa bytes, ServiceId = 4 hexa bytes, AccessId = 6 hexa bytes, TX power integer value
BTS_OrangePackID_CompanyId=0000
BTS_OrangePackID_ServiceId=00000000
BTS_OrangePackID_AccessId=000000000000
;BTS TXPower in dbm : 0=-16, 1=-12, 2=-8, 3=-4, 4=0, 5=4
BTS_OrangePackID_TXPower=2
;;Added in SECard V3.1.0, end

;;Added in SECard V3.2.0, begin
;If ARCBlueMode=2=STid Open API
;Complete local name, max 5 char
STidOpenAPICLN=ARCoa
;Site Code two hexa bytes
STidOpenAPISiteCode=51BC
;3 General purpose bytes
STidOpenAPIGPBS=44444
;To enable secure communication set to 1
STidOpenAPISecureComm=0

;;Added in SECard V3.2.0, end

T14.7 - Sécurisation du mode ligne de commande

Pour sécuriser le fonctionnement en ligne de commande, il faut sécuriser :

- Le fichier d'import de configuration, chargé par le paramètre -i
- Le login en sécurisant les paramètres –u et –p qui apparaissent en clair.

Remarque : si le fichier d'import de configuration est utilisé en sécurisé, il suffit alors de mettre les paramètres –u et –p en tant que données dans ce fichier.

Modification du fichier .gcf

Le rajout de la sécurisation du mode ligne de commande implique des modifications des données contenues (à titre illustratif) dans le fichier SECard.gcf.

```
[Login]
ACCESSLevel=2

[File]
Settings=.\SeCard.pSe

[Serial Number]
SN=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
PN=xxx…….

[Lang]
;1033=Us
;1036=Fr
LangID=1036


[CompatibilityVersion]
eSe_SCB=1

[CommandLineRSA]
; This section ONLY exhibits values integrated in SeCard, none of them is used.
; This is just to remind the values defined in Manual/Specifications.

; RSA decryption for command line configuration file import
; fixed public exponent e = 010001(hex)
; keyLen : 1=1024bits, 2=2048bits, 4=4096 bits

; Key for RSA 1024 bits
;RSA_pub1=3CA377661F13DE29E51E9C2B94CBB7F58EEE4B40377FA3FE22A0EC37F965E7D810E6
4CC01F33391B7FB6A85AC13CEC7D16EA07B07ACA67934A39C79985D13FC0B1599FEB435721CA4
192A31AB805D8239DC52D1F7F55DED1452DC2309824AB655E719371BD9A103D6AC0308EEEDEA
E57E0B14B978DA47A2DBE73377471132D05
;RSA_priv1=PRIVATE
```

; Key for RSA 2048 bits
;RSA_pub2=E511A50D7CE6C94D37B99EA0206F5CBDB1402C5D20BA92CEFDF29C1D553A645BCA
D3C2D118068F7AF1EB49D577C76E170993291ABA56E1E4DC1119539D8EBA635140DCD51B6F36
A949FA7E885946838796FFC09DC57CD1B1B0649F9B15B5610934EAF62DD0B51BA327F7C65E28E
C400D6380E9F9CA0C3D6C4FAEBB1F6CCA2FFBDB4199A6DDF2E43A761AEA83DFF176909AE772D
C453CFA9D54C24600E3B2B8ABB25749D610B5DC85E9146E59AB46AB07A87B6C1F813A53DDCB5
C6119BB6ABAEAB3788B0F2B23382A6FB8B61777AF67C4F1606AC199A0BDB40A4B0BE5C104D77
3293790D64743028C79C88C61E76C90460696D8CD42AAE7718246DC1B1B38F329
;RSA_priv2=PRIVATE

; Key for RSA 4096 bits
;RSA_pub4=5EE503A29011327ECC85F50144CEB2009663DCE96A1EE2C20E065067DCF5D2585FB4
ECA532EDB213A7859F32398958C37088563A0795E482DFD67929EF5C6195DECE80B9D55E54F06
44C3A90DFEBDCE01D84255B3BA4A4B4499D409F00C82065645D1096B07C0466C8BF52C037CD3
60FB068895D5787825F50FCA1307058087D7BA045517F7BA4C9B4A9357A1C409ED2FB2C3425FE
8F6FCAD6344CF8E798BFB87A417A8327BC443E8D6F32211758F50A74AC56B2E3EFFBA38AE087E
3844AA742864F3C64AB182E6D4A5F2346648F31796146B705A2B5B02EA867247258560DAC206F
4CE9040C458B81197E051A1EB7A40C81A6D3A39A4CCB6EC1667CDCC77F2C0C4D74CE98D9BC0D
A4C3088E7348F4E1B20AC13B9D099ACEF1A720C2CF41B06E7B316DBCBE167A2F0CC69FABED31
5C308307CF8AD7BC2FCA14861E92CC51DD0654A66639766BC2BF42F5D39A72FBB1594CBC20073
AFDEE531226024DF3CAF4790BA147FE71315672751AED93833EFC915B7B8A9DF93876C53B466B
72553F8C7B84B32CD19C00BAF61F9902A346D2F1ABF0223CC21C1EEFC5838B7B4859F983A5301
4693838B45B08CF65F1E9BFB8B5AC420F595ADAEE893F854174D51749F31C074E61A9806080A0
184F1C2C0D11AA82367C8C9B1299D4FB7F3A271BDF5811C8B9A17843288CA390ADCFBD28E7DD
D0C8611B02F959AAB9703BF595FA1B46CF77

;RSA_priv4=PRIVATE

Génération du fichier .Se chiffré en .CSe

Pour la génération du fichier de configuration chiffré, utiliser la DLL SeCmdLineLib.dll.

La DLL, son manuel d'utilisation ainsi que deux exemples d'applications sont disponibles dans le dossier de SECard.

T15 - Recommandations sur la sauvegarde des fichiers PSE

T15.1 - Définition

Les fichiers de configuration .pse sont les fichiers créés par SECard. Ils contiennent tous les paramètres de configuration des lecteurs, le paramétrage des puces RFID et les mots de passe de connexion à SECard. Ces fichiers sont chiffrés en AES-CBC et sont inutilisables sans SECard. De plus, ils peuvent être verrouillés par mots de passe de lecture, celui-ci sera alors demandé à l'ouverture, ce mot de passe utilise une clé de hachage.

T15.2 - Utilisation

Le fichier de configuration .pSe par défaut (livré avec SECard) est le fichier SeCard.pse qui se trouve dans le répertoire d'installation de SECard.
A la première ouverture de SECard, il est nécessaire de remplir les champs concernant la communication avec l'encodeur RFID (STR-xx).

Il est possible d'enregistrer ces paramètres (ainsi que tous les autres) dans un autre fichier .pse en utilisant un nom de fichier et un répertoire différents de ceux par défaut. Le dernier fichier .pse utilisé sera automatiquement chargé à l'ouverture de SECard.

T15.3 - Recommandations

Les fichiers .pse contiennent des données sensibles, il convient donc de les considérer, sauvegarder et archiver comme tels. Il est donc conseillé de suivre les recommandations suivantes :

- Utiliser des fichiers pse verrouillés.
- Limiter la diffusion de ces fichiers.
- Sauvegarder les fichiers pse sur un autre poste que celui qui sert à l'encodage.
- Archiver les fichiers pse sur un média non modifiable (CD/DVD).
- En dernière option l'utilisateur pourra récupérer les paramètres courants et sauvegarder la liste de ces paramètres dans un fichier texte, qui sera protégé par une méthode tierce (ex. le fichier rtf produit pourra être zippé, chiffré et sauvegardé par l'entité en charge de la sécurité).

Les utilisateurs qui ont accès à SECard et qui peuvent ouvrir les fichiers pse ont accès aux données qu'ils contiennent donc aux valeurs des paramètres de sécurité (valeurs des clés, cryptographie utilisée …), attention donc à ce que ces personnes soient formées à l'utilisation de SECard et à ce qu'elles soient de confiance (habilitées..).

T16 - Lexique

- ✓ **AES :** Advanced Encryption Standard. Algorithme de chiffrement public utilisant une clé de 128, 192 ou 256 bits. SECard utilise des clés de 128 bits.
- ✓ **ADF :** Application Dedicated File.
- ✓ **APK:** Android Package file.
- ✓ **Application :** Une application contient des fichiers de données.
- ✓ **Application Master Key (AMK):** Clé Maître de l'application des puces MIFARE® DESFire® et MIFARE® DESFire® Ev1.
- ✓ **Authentification :** Procédure qui permet de vérifier l'identité d'une entité.
- ✓ **BCC :** Octet de vérification de CSN. Utilisé sur les puces MIFARE Ultralight® et MIFARE Ultralight® C.
- ✓ **Card Master Key (CMK) :** Clé Maître de la puce MIFARE DESFire® et MIFARE DESFire® Ev1.
- ✓ **Clé Entreprise :** Clé protégeant le badge « SCB » et les lecteurs configurés par ce dernier.
- ✓ **Crypto1 :** Algorithme de chiffrement privé (NXP) basé sur une clé de 48 bits. Utilisé dans la MIFARE® Classic et MIFARE Plus® Level 1.
- ✓ **CSN :** Numéro de série de la puce.
- ✓ **DF :** Dedicated File
- ✓ **EF :** Elementary file
- ✓ **Encodage :** Ecriture d'un numéro privé dans un plan mémoire d'une puce.
- ✓ **FCP :** File Control Parameter
- ✓ **FID :** File Identifier. Numéro de fichier.
- ✓ **Format :** Formatage d'une puce MIFARE® DESFire® et MIFARE® DESFire® Ev1.
- ✓ **HCE:** Host Card Emulation
- ✓ **Lock Bytes :** Octets de verrouillages. Utilisés sur les puces MIFARE Ultralight® et MIFARE Ultralight® C.
- ✓ **MAD :** MIFARE® Application Directory. Pour plus d'informations, se référer au document NXP AN10787 MIFARE® Application Directory (MAD).pdf.
- ✓ **MIFARE Plus® Levels :** Niveaux de sécurité des puces MIFARE Plus®.
  - **Level 0 :** Niveau de configuration des MIFARE Plus®.
  - **Level 1 :** Niveau de compatibilité MIFARE® Classic. Utilise l'algorithme Crypto1.
  - **Level 2 :** Non utilisé par SECard. Niveau intermédiaire.
  - **Level 3 :** Niveau de forte sécurité. Utilise l'algorithme de chiffrement AES.
- ✓ **NFC: Near Field Communication**
- ✓ **OTP :** One Time Programming. Programmation unique.
- ✓ **Private ID :** Code privé.
- ✓ **PUPI :** Numéro de série de la puce utilisé en 14443-B.
- ✓ **SCB :** Secured Configuration Badge (Badge de configuration des lecteurs).
- ✓ **SSCP :** STid Secure Common Protocol.
- ✓ **SKB :** Secured Key Bundle. Portefeuille de clés AES-3DES-Crypto1, utilisé sur les lecteurs RS232 RS485 et USB pour l'indexage des clés de sécurité.
- ✓ **UID :** Numéro de série de la puce.

- ✓ **3DES :** Triple Data Encryption Standard. Variante de l'algorithme DES se basant sur deux clés de 56 bits.
- ✓ **Diversification des clés -** Pour plus d'informations se référer aux documents NXP suivants :
  - MIFARE® DESFire® EV1 et MIFARE Plus® : AN-165310.pdf Méthode NXP MIFARE® SAM.
  - MIFARE® Classic : P5DF072EV2.pdf §8.6.1
  - MIFARE Ultralight® C : P5DF072EV2.pdf §8.6.2

SECard V3.2 évolution

Date	Description

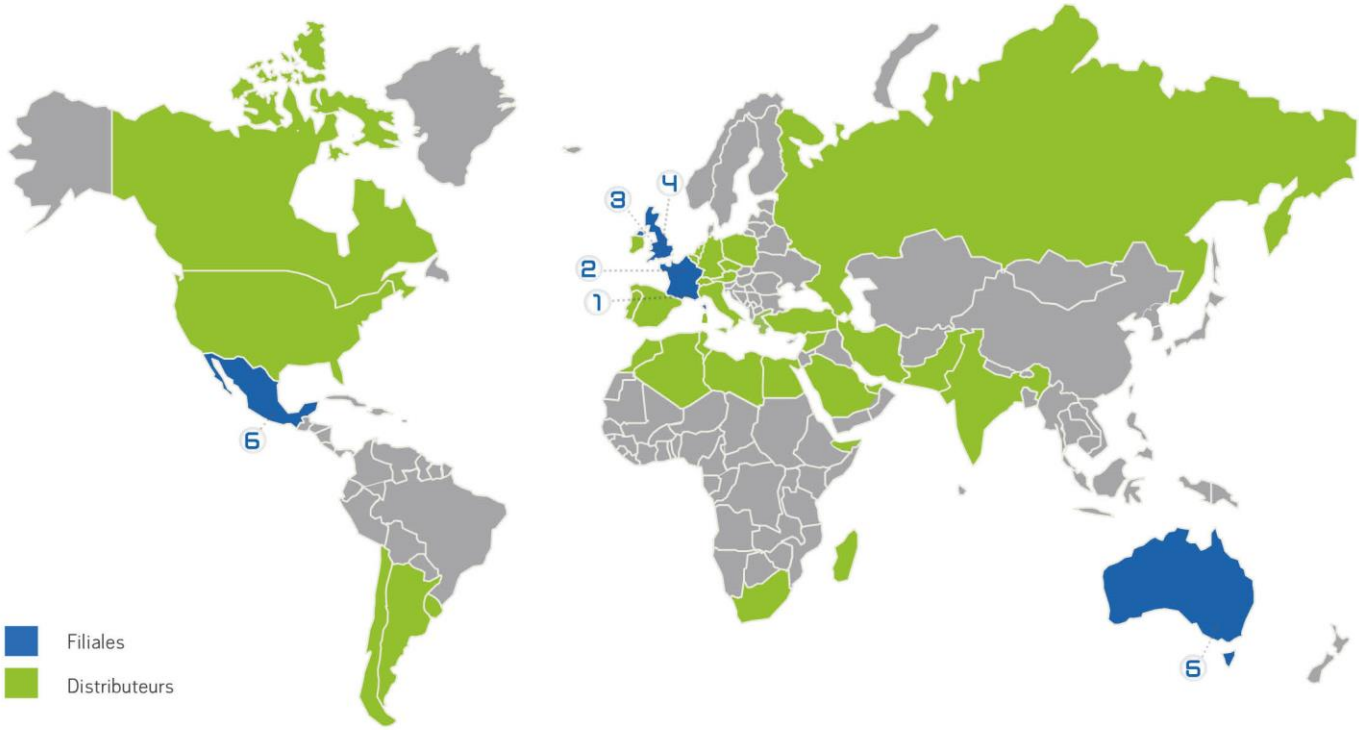
19/03/2018	**Ajout :**
	
	- **Bluetooth :**
	  - 4 Seuils pour le mode badge (au lieu de 2 auparavant)
	  - Open Mobile Protocole
	  - Effacement d'une VCard avec récupération des crédits OFFline
	
	- **DESFire :**
	  - Secure messaging : gestion de la communication en EV2 avec Proximity Check
	  - Encodage et relecture de la DESFire en mode EV2
	  - Outil de verrouillage en mode EV2
	  - Configurations prédéfinis
	
	- **Mifare Classic/SL1 et SL3 :**
	  - Profils de configurations prédéfinis
	
	- **Protocole de communication :**
	  - Wiegand 35bits, 37 bits et 34 bits.
	
	- **125kHz :** Gestion du module SE8- 125kHz
	
	- **LED :** Possibilité de tamiser les LED (luminosité atténuée)
	
	- **Droits du Super Administrateur :** Accés aux Outils SECard
	
	- **Sauvegarde fichier de configuration :** Générateur aléatoire de mot de passe

	Amélioration : - **Compatibilité avec Windows server 2012R2**
	Suppression : - **DESFire : format ASCII des données.**

REVISION

Date	Version	Description
10/03/2014	*5.0*	*Création.*
18/04/2014	*5.1*	*Modification des imprimes écran suite au retrait du point d'interrogation « A propos »* *Ajout « signal de vie et arrachement mutualisés » pour les lecteurs R33+INTR33E (p25, 37, 128)* *Modification du champ Taille données (p22, 24, 34, 36)* *Ajout option –v verbeux en ligne de commande (p130, 132)*
28/11/2014	*5.2*	*Ajout référence encodeur ARC / Ajout installation certificat de sécurité / Modification tableau de compatibilité* *Ajout avertissement sur les droits administrateur /Ajout procédure pas à pas « Enregistrer sous » / Ajout imprime écran Assistant SCB WAL / Ajout tableau sur type de puce pour la création du SCB / Ajout Assistant SCB WAL / Ajout chiffrement authentifié pour ARC / Ajout LED rouge à l'arrachement / Ajout fonction Scramble / Ajout étape 7 de l'assistant SCB ARC / Ajout clé de chiffrement AtE / Ajout précisions sur le formatage DESfire / Ajout ARC-F dans le tableau / Modification du fichier Se. avec ajout WAL, écran et encodage biométrique/ Modification de tous les imprimes écrans.*
02/03/2015	*5.3*	*Modification certificat de sécurité délivré par une autorité de certification de confiance à la place du certificat STid/ Ajout dans le fichier de configuration de la ligne de commande de l'activation des puces*
14/12/2015	*5.4*	*Partie 1 : Mise à jour compatibilité version SECard (p9) / Modification sur les mots de passe (p16-18) / Ajout ARC1(p49) / Ajout dans l'assistant de configuration de l'ARC du mode « Données bio dans le lecteur » (p57-58) / Ajout Type de donnée à lire pour la DESFire FID ID1 (p68) / Ajout du padding et de l'inversion de l'AID dans la diversification NXP (p71) / NHF-HCE ajouté dans les assistants de configuration pour lecteur LXS, WAL et ARC (p85-88) / Création du badge SKB par cérémonie des clés ajouté (p95-98) / Ajout de la Création des badges de configuration BCC (p99-102) /* *Partie 2 : Ajout ARC1 (p126 et p131) / Techno puce HCE ajoutée au protocole Wiegand 3T (p143) / Mode Données bio dans le lecteur (p162-164) / Modification du fichier Se. /* *Modification de tous les imprimes écrans*
19/12/2016	*6.0*	*Part 1 : I.4 Ajout Localisation des fichiers utilisateurs à l'installation // I.6 Compatibilité modifiée // II.2 Ajout Encodage Blue Mobile ID // II.4 Ajout demande de crédit // III.5 SCB ARC assistant: ajout des options Blue Mobile ID // III.7 Paramètres Mifare DESFire: ajout configuration Blue mobile, mode de communication, Free create delete // III.8 Mifare DESFire clés: ajout donnée NXP diversification, ajout d'une clé pour la diversification en RandomID // III.11 Paramètres Mifare Classic: ajout secteur pour la biométrie // III.15 Ajout Paramètres Blue Mobile ID // III.15 Ajout Blue Mobile ID clés // VI.1 Encodage : ajout liste en Random // VI.2 : Ajout encodage // VI.3 ajout configuration en STid Mobile ID+ // VII.9 Mise à jour: ajout d'exemple.* *Part 2 : T2.1 : Modification Mise sous tension // T4.2 : Ajout Protocol 3T BLE // T5.2.2 Correction structure message // T10 Ajout signal de vie spécifique // T11 Ajout signal d'arrachement spécifique // T13.6 Fichier d'import configuration : nouveaux paramètres lecteurs ajoutés. // Ajout du paragraphe SECard Evolution.*
04/08/2017	*6.1*	*Part 1 : I.5 Compatibilité modifiée // III Ajout Chargement de la configuration par la série // III.5 LED à la connexion Bluetooth®// Options clavier // Rotation de l'écran // Orange Pack ID // III.7 /9/11 Option biométrique dérogation // III.8 IDPrime diversification //III.12 MAD clé A // III.15 Mode de lecture Blue // III.17 Ajout algo Orange Pack ID // IV.3 Assignation clés indexées // VI.2 Dérogation bio // VII.5 Suppression fichier*
23/10/2017	*6.2*	*Suppression application et fichier sur badge IDPrime ajouté dans les outils // Ajout paramètres -b en ligne de commande pour spécifier la vitesse de l'encodeur.*
19/03/2018	*6.3*	*Part 1 : I.5 Compatibilité modifiée // II-.2 Droit utilisateurs ajout Utiliser les Outils // II-3 Fichiers ajout Générateur de mot de passe // II-4 Crédits ajout Suppression VCard et compteur de crédits dynamique // III Modification lié à l'IHM // Etape 6 de l'assistant de configuration ajout option d'atténuation des LED // Etape 8 de l'assistant de configuration ajout Open Mobile Protocole // En STidMobileID ajout des 2 nouveaux seuils en mode badge // III-7 Ajout Configurations prédéfinies DESFire Ajout mode EV2 // III-15-Ajout print Open Mobile Protocole // VII-5 Outils DESFire ajout verrouillage EV2* *Partie 2 : T4.2 Ajout Protocol 3Eb 3V 3W // T13.6 Fichier d'import configuration modifié*

CONTACT



1 SIÈGE SOCIAL
20, Parc d'Activités des Pradeaux
13850 Gréasque, France
+33 (0)4 42 12 60 60
+33 (0)4 42 12 60 61

2 AGENCE PARIS - IDF
Immeuble Le Trisalys
416 avenue de la Division Leclerc
92290 Chatenay-Malabry, France
+33 (0)1 43 50 11 43
+33 (0)1 43 50 27 37

3 AGENCE UK
Innovation centre
Gallows Hill, Warwick
CV34 6UW, United Kingdom
+44 (0) 1926 217 884
+44 (0) 1926 217 701

4 AGENCE UK NORD
London, Holborn,
88, Kingsway, WC2B, London
6AA, United Kingdom
+44 (0) 20 7841 1000

5 AGENCE AUSTRALIE - APAC
Levels 5 & 6
616 Harris Street,
Ultimo, Sydney, NSW 2007
New South Wales, Australia
+61 (0)2 92 74 88 53

6 AGENCE AMÉRIQUE
Varsovia 57, Interior 501
Colonia Juárez, CP 06600
Delegación Cuauhtemoc
Mexico, D.F.
+52 (55) 52 56 47 06
+52 (55) 52 56 47 07