



# SECARD



MANUEL UTILISATEUR



*Designed in France  
Made in France*

[www.stid-security.com](http://www.stid-security.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](http://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**

# Sommaire

## MANUEL UTILISATEUR - PARTIE 1 – FONCTIONNALITÉS 8

<b>I.</b>	<b>INFORMATIONS</b>	<b>9</b>
	<b>I. 1 - PREREQUIS PC</b>	<b>9</b>
	<b>I. 2 - CONTENU DE LA CLE USB</b>	<b>9</b>
	<b>I. 3 - MATERIEL NECESSAIRE</b> <small>MODIFICATION 3.6</small>	<b>9</b>
	<b>I. 4 - INSTALLATION SOUS WINDOWS</b>	<b>9</b>
	<b>I. 5 - COMPATIBILITE</b> <small>MODIFICATION 3.6</small>	<b>11</b>
	<b>I. 6 - DEMARRAGE DU LOGICIEL</b>	<b>13</b>
	<b>I. 7 - GENERALITES</b>	<b>14</b>
<b>II.</b>	<b>PARAMETRES SECARD</b>	<b>15</b>
	<b>II. 1 - ENCODEUR</b>	<b>15</b>
	<b>II. 2 - DROITS UTILISATEUR</b>	<b>18</b>
	<b>II. 3 - FICHIERS</b>	<b>19</b>
	<b>II. 4 - CREDITS BLUETOOTH®</b>	<b>22</b>
<b>III.</b>	<b>CONFIGURATION LECTEUR - SCB / OCB</b>	<b>26</b>
	<b>III. 1 - ASSISTANT SCB : PARAMETRES LECTEURS</b>	<b>31</b>
	SCB – ETAPE 1	32
	SCB – ETAPE 2	33
	SCB – ETAPE 3 <small>AJOUT FONCTIONNALITE 3.6</small>	35
	SCB – ETAPE 4	41
	SCB – ETAPE 5	43
	SCB – ETAPE 6 <small>AJOUT FONCTIONNALITE 3.6</small>	45
	SCB – ETAPE 7 <small>AJOUT FONCTIONNALITE 3.6</small>	52
	SCB – ETAPE 8	57
	SCB – ETAPE 9 <small>AJOUT FONCTIONNALITE 3.6</small>	66
	<b>III. 2 - ASSISTANT SCB : CLES DE SECURITE LECTEUR</b>	<b>69</b>
	<b>III. 3 - ASSISTANT OCB : PARAMETRES LECTEURS</b>	<b>73</b>
	OCB – ETAPE 1	74
	OCB – ETAPE 2	76
	OCB – ETAPE 3 <small>AJOUT FONCTIONNALITE 3.6</small>	79
	OCB – ETAPE 4	85
	OCB – ETAPE 5 <small>AJOUT FONCTIONNALITE 3.6</small>	86
	OCB – ETAPE 6	88
	OCB – ETAPE 7	90
	OCB – ETAPE 8 <small>AJOUT FONCTIONNALITE 3.6</small>	99
	<b>III. 4 - ASSISTANT OCB : CLES DE SECURITE DU LECTEUR</b>	<b>102</b>
	<b>III. 5 - MIFARE® DESFIRE® : PARAMETRES</b>	<b>105</b>
	<b>III. 6 - MIFARE® DESFIRE® : CLES</b>	<b>115</b>

III. 7 - MIFARE PLUS® SL3 : PARAMETRES.....	124
III. 8 - MIFARE PLUS® SL3 : CLES .....	127
III. 9 - MIFARE® CLASSIC/SL1 : PARAMETRES .....	129
III. 10 - MIFARE® CLASSIC /SL1 : CLÉS .....	132
III. 11 - MIFARE ULTRALIGHT® C : PARAMETRES.....	134
III. 12 - MIFARE ULTRALIGHT® C : CLÉS.....	135
III. 13 - BLUE/NFC MOBILE ID : PARAMETRES .....	137
III.13.1 - STID MOBILE ID® .....	137
III.13.2 - ORANGE™ PACK ID .....	141
III.13.3 - OPEN MOBILE PROTOCOL.....	142
III. 14 - BLUE/NFC MOBILE ID : CLÉS .....	143
III. 15 - 125 KHZ : PARAMETRES.....	144
III.15.1 – SE8.....	144
III.15.2 – SE8M.....	145
III. 16 - CODE MATRICIEL / CODE QR : PARAMETRES <sup>AJOUT FONCTIONNALITE 3.6</sup> .....	148
III. 17 - APPLICATION MULTISERVICES CITOYENNE (AMC) : PARAMETRES <sup>NOUVEAU 3.6</sup> .....	151
III. 18 - NFC-HCE : PARAMETRES .....	156
III. 19 - NFC-HCE : CLES.....	159
III. 20 - CPS3 : PARAMETRES.....	160
<b>IV. CONFIGURATION LECTEUR - SKB</b> .....	<b>161</b>
IV.1 - CREATION EN MODE CLASSIQUE .....	162
IV.2 - CREATION EN MODE « CEREMONIE DES CLES » .....	163
IV.3 - UTILISATION DE CLES INDEXEES DANS LA CONFIGURATION SECARD .....	167
<b>V. CONFIGURATION LECTEUR - SCB R/W</b> .....	<b>171</b>
VI.1 – ASSISTANT DE CONFIGURATION .....	172
VI.2 – CREATION DU SCB R/W .....	179
<b>VI. CREATION BADGES</b> .....	<b>180</b>
VII. 1 - DONNEES.....	180
VII. 2 – ENCODER .....	184
<b>VII. OUTILS</b> .....	<b>190</b>
VIII. 1 - MAD.....	190
VIII. 2 - SECTEUR.....	193
VIII. 3 - CONTENU.....	194
VIII. 4 - NIVEAUX .....	196
VIII. 5 - DESFIRE.....	197
VIII. 6 - VERROUILLAGE.....	199
VIII. 7 - BCA .....	200
VIII. 8 - FICHIERS ESE/PSE .....	202

VIII. 9 - MISE A JOUR.....	203
VIII. 10 - UHF CONFIG.....	210

<b>MANUEL UTILISATEUR - PARTIE 2 - TECHNIQUE</b>	<b>211</b>
<b>T1 - LECTEURS CONFIGURABLES PAR SECARD</b>	<b>212</b>
T1.1- CONFIGURABLE PAR SCB .....	212
T1.2- CONFIGURABLE PAR OCB .....	212
T1.3- CONFIGURABLE PAR SCB R/W .....	212
<b>T2 - AU SUJET DES LECTEURS</b>	<b>213</b>
T2.1 - MISE SOUS TENSION DES LECTEURS LECTURE SEULE .....	213
T2.2 - CONFIGURATION DES LECTEURS .....	214
T2.3 - LECTEUR ARC1 .....	214
<b>T3 - AU SUJET DES PUCES</b>	<b>215</b>
T3.1 - ORGANISATION DE LA MEMOIRE DES PUCES MIFARE® CLASSIC ET MIFARE PLUS® .....	215
T3.2 - ORGANISATION DE LA MEMOIRE DES PUCES MIFARE® DESFIRE® ET MIFARE® DESFIRE® EVX.....	218
T3.3 - ORGANISATION DE LA MEMOIRE DES PUCES MIFARE ULTRALIGHT® ET ULTRALIGHT® C .....	219
<b>T4 - AU SUJET DES PROTOCOLES DE COMMUNICATION TTL</b>	<b>221</b>
T4.1 - PROTOCOLE ISO2 CLOCK&DATA .....	221
T4.2 - PROTOCOLE WIEGAND .....	224
T4.3 - PROTOCOLE WIEGAND CHIFFRE .....	228
T4.4 - PROTOCOLE PAC / PAC64 .....	228
<b>T5 - AU SUJET DES PROTOCOLES DE COMMUNICATION SERIE</b>	<b>229</b>
T5.1 - MODE DE COMMUNICATION UNIDIRECTIONNEL .....	229
T5.2 - MODE DE COMMUNICATION BIDIRECTIONNEL .....	230
<b>T6 - AU SUJET DES LECTEURS CLAVIER</b> <small>AJOUT FONCTIONNALITE 3.6</small>	<b>238</b>
T6.1 - LECTEURS TTL - R31 - BADGE OU TOUCHE .....	238
T6.2 - LECTEURS TTL - R31 – TOUCHE ET BADGE.....	241
T6.3 - LECTEURS TTL - R31 - BADGE OU TOUCHE - MODE 26-BITS WIEGAND <small>NOUVEAU 3.6</small> .....	241
T6.4 - LECTEURS TTL - S31 - BADGE ET TOUCHE.....	242
T6.5 - LECTEURS TTL - S31 - BADGE OU TOUCHE .....	242
T6.6 - LECTEURS RS232 / RS485 - R32/S32/R33/S33 - BADGE OU TOUCHE .....	243
T6.7 - LECTEURS RS232 / RS485 - R32/S32/R33/S33 - BADGE ET TOUCHE.....	244
<b>T7 - GESTION DE LA BIOMETRIE</b>	<b>245</b>
T7.1 – FORMAT DES EMPREINTES BIOMETRIQUES .....	245

T7.2 - DEROGATION BIOMETRIQUE .....	245
<b>T8 - GESTION DE LA BIOMETRIE + CLAVIER</b>	<b>246</b>
<b>T9 - SIGNAL DE VIE</b>	<b>247</b>
T9.1 - LECTEUR TTL .....	247
T9.2 - LECTEUR SERIE BIDIRECTIONNEL .....	249
T9.3 - LECTEUR SERIE UNIDIRECTIONNEL .....	249
<b>T10 - SIGNAL D'ARRACHEMENT</b>	<b>250</b>
T10.1 - LECTEUR TTL.....	250
T10.2 - LECTEUR SERIE BIDIRECTIONNEL .....	250
T10.3 - LECTEUR SERIE UNIDIRECTIONNEL .....	250
<b>T11 - ID D'ARRACHEMENT</b>	<b>251</b>
<b>T12 - SIGNAL DE VIE / ARRACHEMENT MUTUALISES</b>	<b>251</b>
<b>T13 - LIGNE DE COMMANDE</b>	<b>252</b>
T13.1 - DESCRIPTION .....	252
T13.2 - UTILISATION .....	252
T13.3 - CONSOLE DE COMMANDE.....	254
T13.4 - FICHIER BATCH.....	256
T13.5 - APPLICATIONS TIERCES .....	257
T13.6 - FICHIER D'IMPORT DE CONFIGURATION .....	258
T13.7 - SECURISATION DU MODE LIGNE DE COMMANDE .....	273
<b>T14 - RECOMMANDATIONS SUR LA SAUVEGARDE DES FICHIERS PSE</b>	<b>275</b>
T14.1 - DEFINITION.....	275
T14.2 - UTILISATION .....	275
T14.3 - RECOMMANDATIONS .....	275
<b>T15 - LEXIQUE</b>	<b>276</b>
<b>SECARD V3.6 EVOLUTIONS – VERSION FIRMWARE Z17 / OSDP-Z11</b>	<b>278</b>
<b>REVISION</b>	<b>279</b>

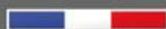


# SECARD



## MANUEL UTILISATEUR

Partie 1 : Description détaillée de toutes les fonctionnalités



*Designed in France  
Made in France*

[www.stid-security.com](http://www.stid-security.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.
- 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.
- MorphoCBM Driver.

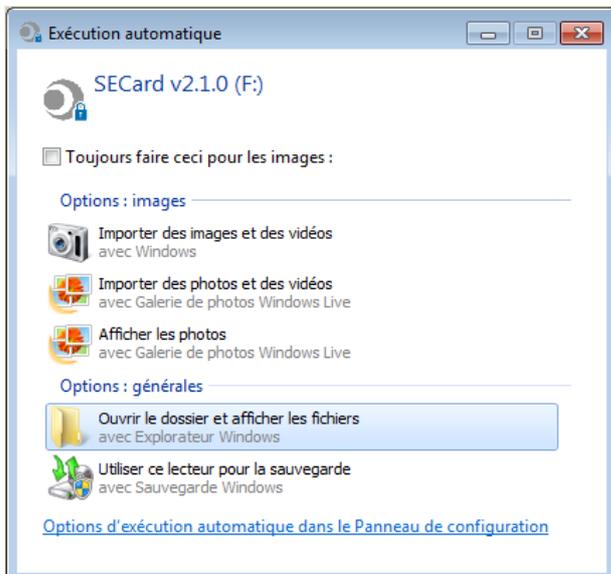
### I. 3 - Matériel nécessaire *Modification 3.6*

Encodeur USB 13,56 MHz et Bluetooth® STid : Réf. ARCS-W35-E-BT1-5AA-1.  
Version de firmware Z10 minimum (visible sur l'étiquette au dos de l'encodeur).

Pour créer les badges SCB / OCB : MIFARE® DESFire® EV2/EV3 8ko non verrouillé en mode EV2

### 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.

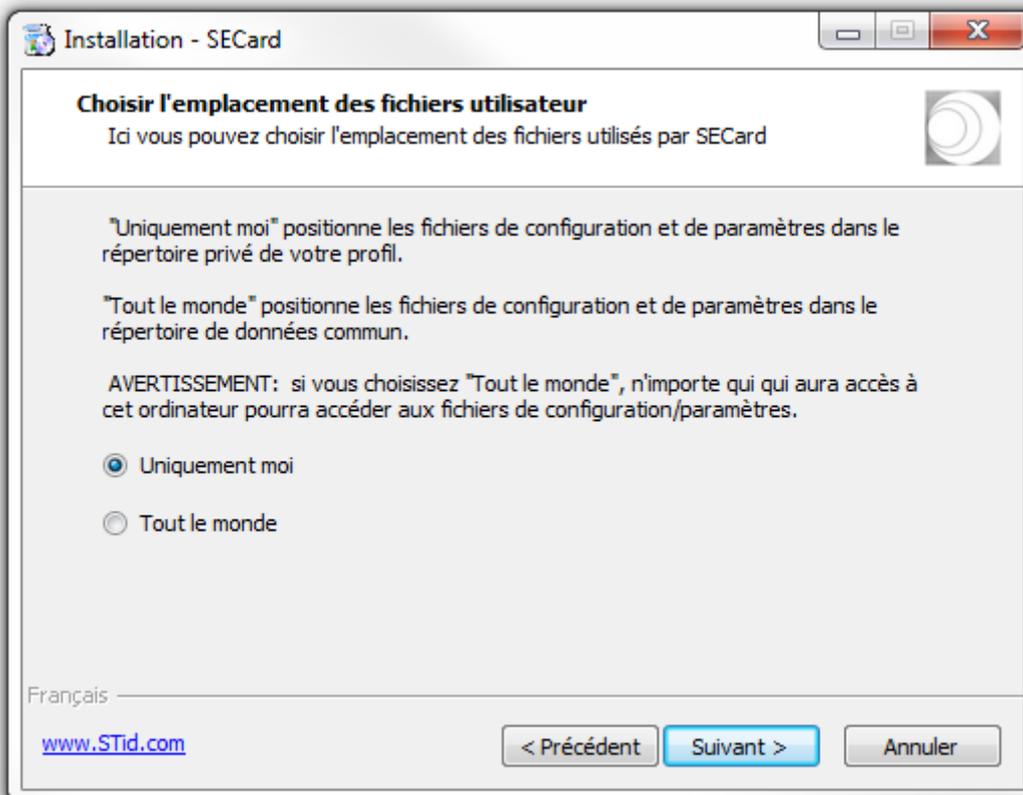
#### **Remarques :**

**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 *Modification 3.6*

### ➤ Firmware / version de SECard

Le logiciel SECard (V3.6.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 encastrables WAL\* et Architect® avec le même logiciel SECard.

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
V3.2.x	V12	≥ Z08
V3.3.x	V13	≥ Z11
V3.4.x	V14	≥ Z14
V3.5.x	V15	≥ Z16
V3.6.x	V16	≥ Z17

Version de SECard	Version du OCB	Version du Firmware
V3.3.x	OCBv3	≥ Z05
V3.4.x	OCBv4	≥ Z08
V3.5.X	OCBv5	≥ Z09
V3.6.X	OCBv6	≥ Z11

\* Pour configurer les lecteurs standards STid et les lecteurs WAL de firmware SZ188F21, utiliser une version de SECard < v3.3.x et se reporter au Manuel Utilisateur SECard v6.4.

### **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®, module QR Code / Matrix) 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.

➤ **Badge de configuration** *Nouveau 3.6*

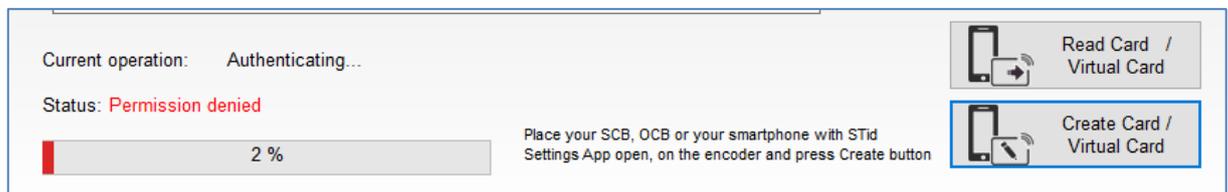
A partir de la version SECard 3.6, l'encodage des badges de configurations est modifié.

Conséquences :

Badge SCB v16 : ré-encodage dans une version antérieure de SCB IMPOSSIBLE

Badge OCB v06 : ré-encodage dans une version antérieure de OCB IMPOSSIBLE

Message d'erreur lors de l'encodage d'un SCB v16 en SCB v15 ou inférieur :

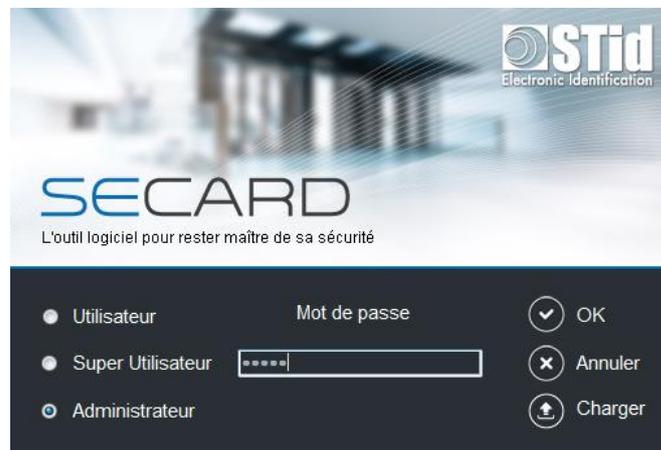


## I. 6 - Démarrage du logiciel

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 apparié à SECard, contacter le service commercial.

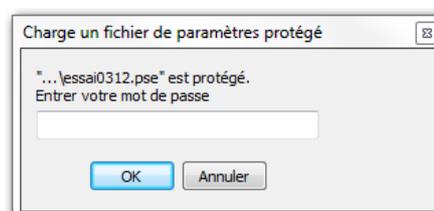


Lors du démarrage du logiciel, une fenêtre apparaît pour la saisie des identifiants de connexion ou le chargement d'un fichier de configuration spécifique.

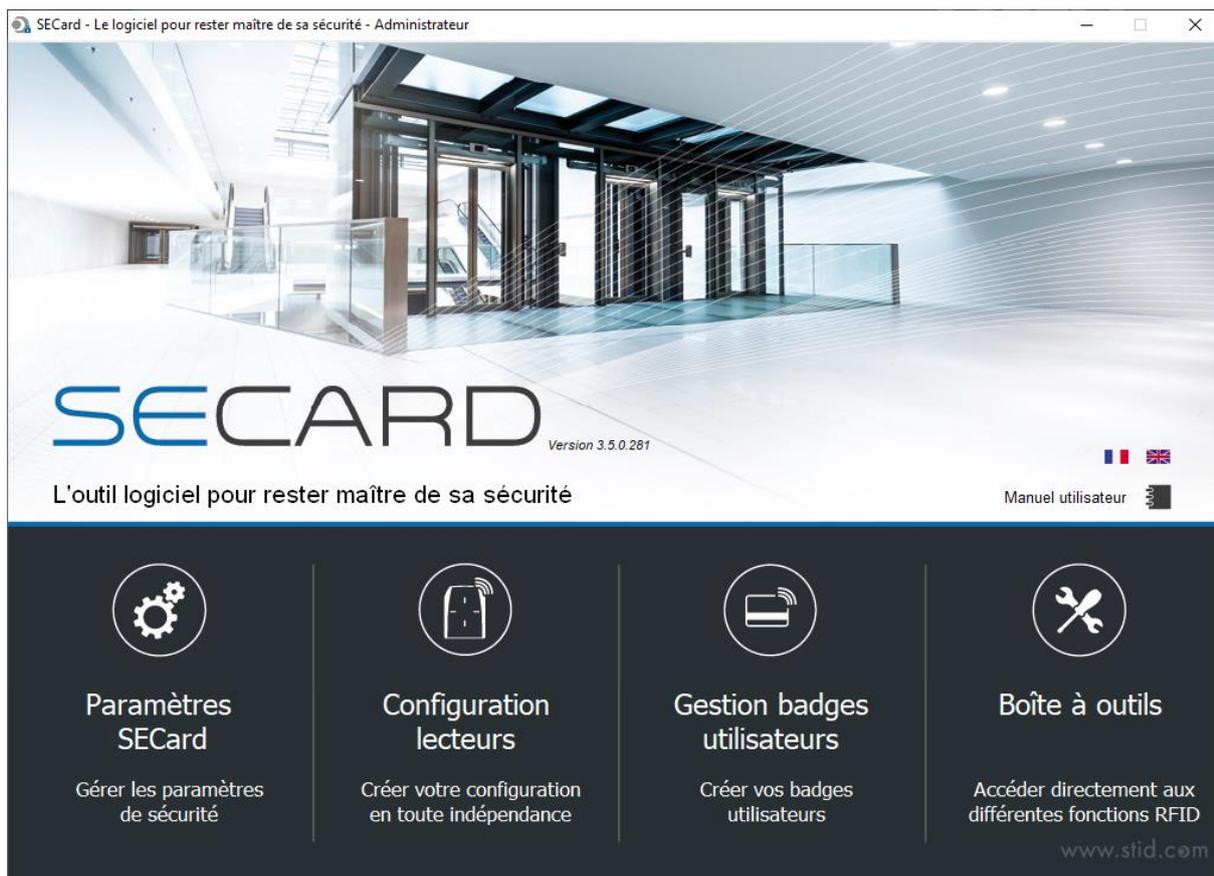
Il y a trois niveaux d'accès, gérant différentes autorisations au sein du logiciel. Ces mots de passe sont sauvegardés dans le fichier de configuration.

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 apparaît 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.



Accueil



Paramètres



Encodeur



Droits utilisateur



Fichiers



Configuration lecteur



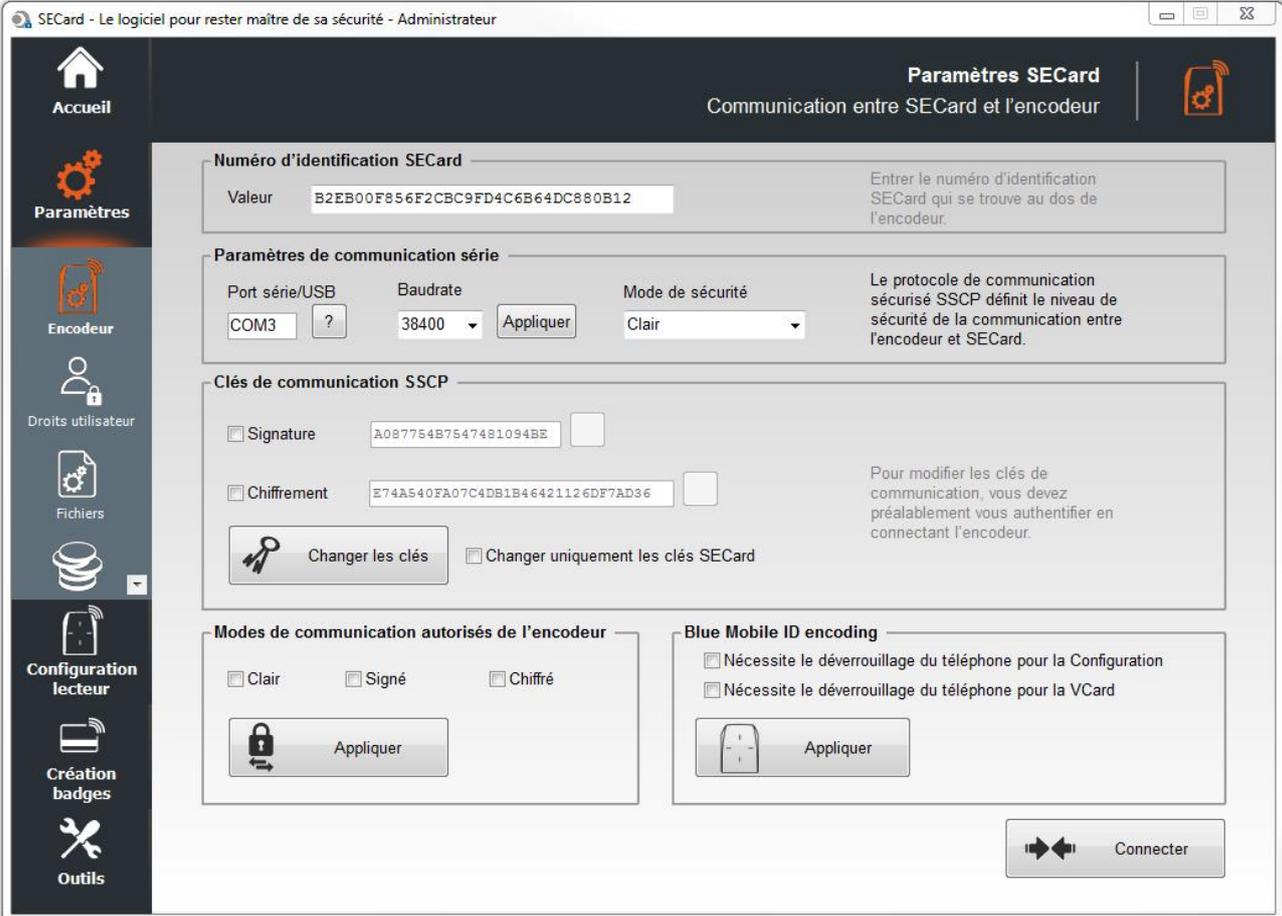
Création badges



Outils

## 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.



Accueil



Paramètres



Encodeur



Droits utilisateur



Fichiers



Configuration lecteur



Création badges



Outils

- ❖ 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® ( Secure & Smart Communication 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.

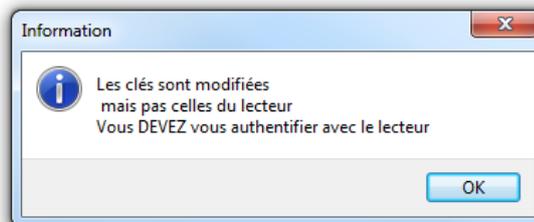
Lorsque la communication est signée et/ou chiffrée, le logiciel SECard et l'encodeur utilisent les clés utilisateurs par défaut suivantes :

Clé de signature : A087754B7547481094BE  
 Clé de chiffrement : E74A540FA07C4DB1B46421126DF7AD36

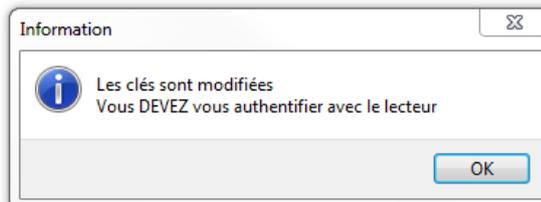
Afin de changer les valeurs de ces clés, il suffit de cocher les cases « Signature » et/ou « Chiffrement », de renseigner la nouvelle valeur. Puis de cliquer sur le bouton « Changer les clés ».

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.



Accueil



Paramètres



Encodeur



Droits utilisateur



Fichiers



Configuration  
lecteur



Création  
badges



Outils

## 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

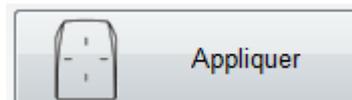
Si le mode « *En clair* » n'est plus autorisé **et** que les clés utilisateurs sont perdues, il ne sera alors plus possible de communiquer avec l'encodeur.

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

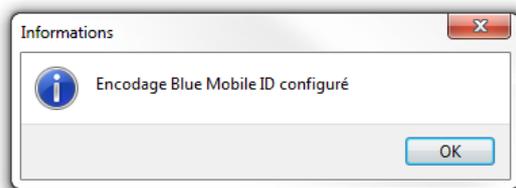
## Encodage Blue Mobile ID

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.



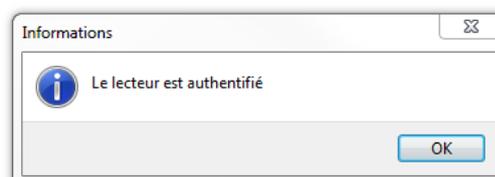
Valider le choix en cliquant sur le bouton :



## Connecter

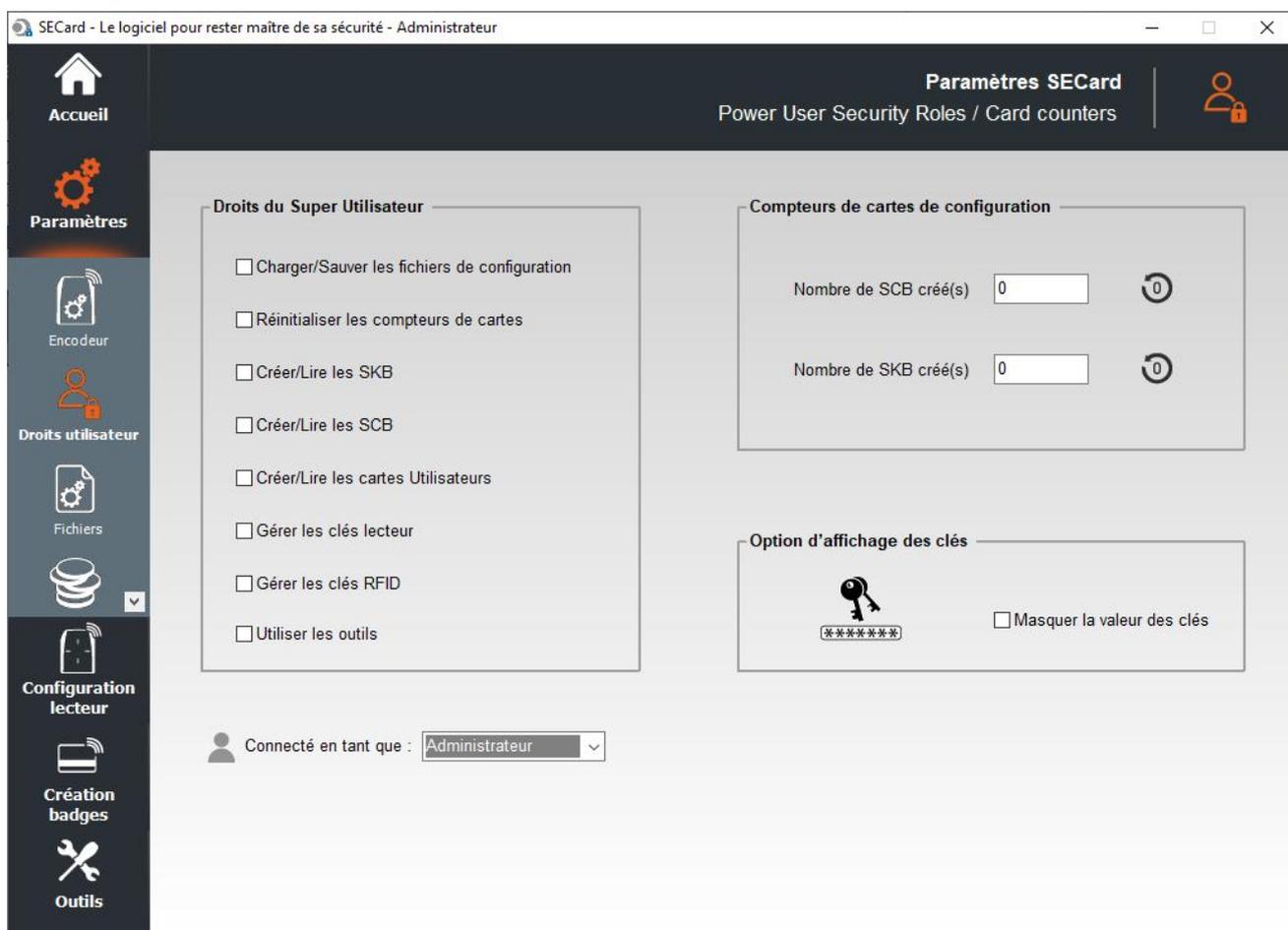
Lors de l'alimentation du lecteur encodeur, celui-ci allume la LED blanche et émet un bip sonore.

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'acquiescement apparaîtra à l'écran.





## II. 2 - Droits Utilisateur



### 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.

### Se loguer en tant que :

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.



Accueil



Paramètres



Encodeur



Droits utilisateur



Fichiers



Configuration lecteur

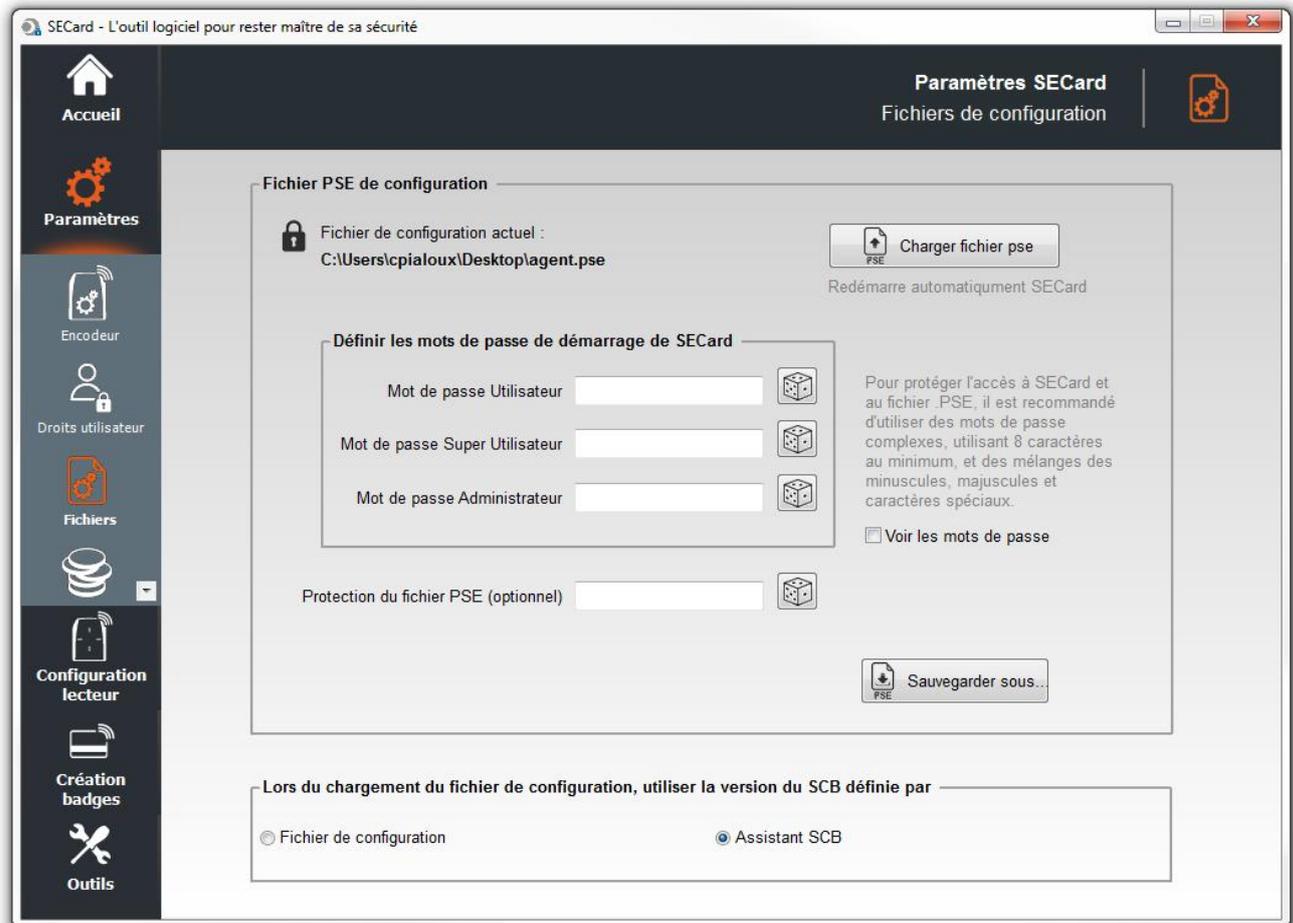


Création badges



Outils

## 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 choisit 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 fichier .pse.

Recommandations sur la sauvegarde des fichiers de configuration .pse (cf. [T14 - Recommandations sur la sauvegarde des fichiers PSE](#))



Accueil



Paramètres



Encodeur



Droits utilisateur



Fichiers



Configuration lecteur



Création badges



Outils

## Sauver sous...

- Mots de passe pour le login de SECard.

**Définir les mots de passe de démarrage de SECard**

Mot de passe Utilisateur

Mot de passe Super Utilisateur

Mot de passe Administrateur



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

**Générateur de mot de passe**

Taille  Majuscules [A..Z]  
 Minuscules [a..z]  
 Nombres [0..9]  
 Symboles | <>,&"(-..

11

**Exemple**

xyi0wURkNnJ

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



- Protection du fichier PSE (optionnel)

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 :



Accueil



Paramètres



Encodeur



Droits utilisateur



Fichiers



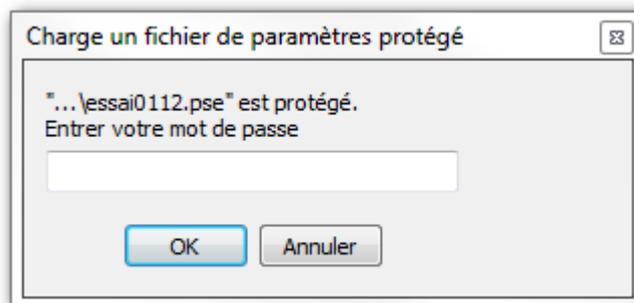
Configuration lecteur



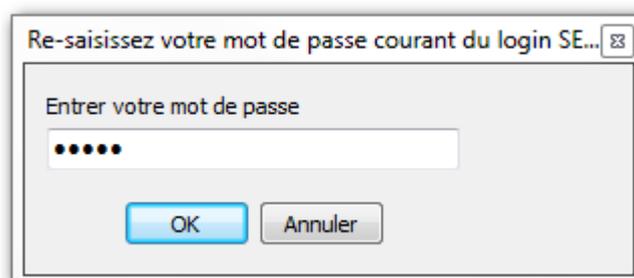
Création badges



Outils



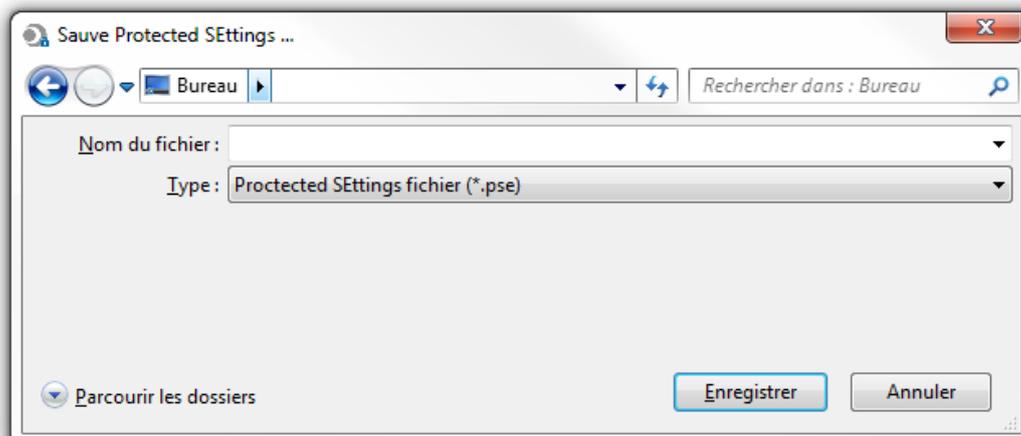
- Lorsqu'on clique sur le bouton Sauver sous... une fenêtre apparaît demandant de saisir le mot de passe **administrateur pour le login de SECard** courant :



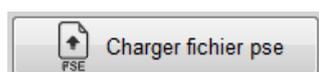
Par exemple STidA, si c'est le fichier SECard.pse par défaut qui a été chargé.

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®

- Accueil
- Paramètres
- Droits utilisateur
- Fichiers
- Crédit
- Configuration lecteur
- Création badges
- Outils

The screenshot shows the 'Paramètres SECard' window with the following sections:

- Requête de crédits:**
  - Text: "Vous pouvez directement envoyer votre demande de crédits par email ou générer un fichier texte que vous devez envoyer à votre revendeur avec votre bon de commande."
  - Radio buttons for credit amounts: 50, 100 (selected), 500, 1000, 200, and "Autre montant" (with a text input field containing "100").
  - Information: "1 Badge STid Mobile ID+ = 1 crédit", "1 Badge d'accès virtuel = 5 crédits".
  - Buttons: "Requête Email" and "Générer fichier texte".
  - Warning: "Important: vous pouvez uniquement faire UNE demande de crédits à la fois. Toutes les demandes suivantes remplaceront la première tant qu'aucune n'est chargée dans l'encodeur".
- Chargement des crédits:**
  - Text: "Pour charger des crédits dans l'encodeur, vous devez simplement coller votre code de licence dans ce champ, ou charger le fichier .txt que vous avez reçu."
  - Text input field: "Copier / Coller le code de licence".
  - Button: "Chargement crédits".
- Supprimer votre badge d'accès virtuel et récupérer vos crédits:**
  - Text input field: "myConfigName" with a long string of zeros.
  - Button: "Suppression VCard".

**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.



STid propose trois badges d'accès :

STid Mobile ID	STid Mobile ID+	Card name
iD: #428F3478	iD: #428F3478	Configuration name Site code 1234 iD: #1231458903
<p><b>CSN STid Mobile ID° free</b></p> <ul style="list-style-type: none"> <li>▶ Numéro unique fourni à l'installation de l'application</li> <li>▶ Modes autorisés :</li> </ul>	<p><b>CSN+ STid Mobile ID°+</b></p> <ul style="list-style-type: none"> <li>▶ Numéro unique fourni à l'installation de l'application</li> <li>▶ Modes autorisés :</li> </ul>	<p><b>Virtual access card Secure+</b></p> <ul style="list-style-type: none"> <li>▶ ID privé</li> <li>▶ Sécurité entièrement paramétrable</li> <li>▶ Modes autorisés :</li> </ul>



Accueil



Paramètres



Droits utilisateur



Fichiers



Crédit



Configuration lecteur



Création badges



Outils

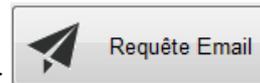
## Demande de Crédits

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

Deux méthodes sont proposées :

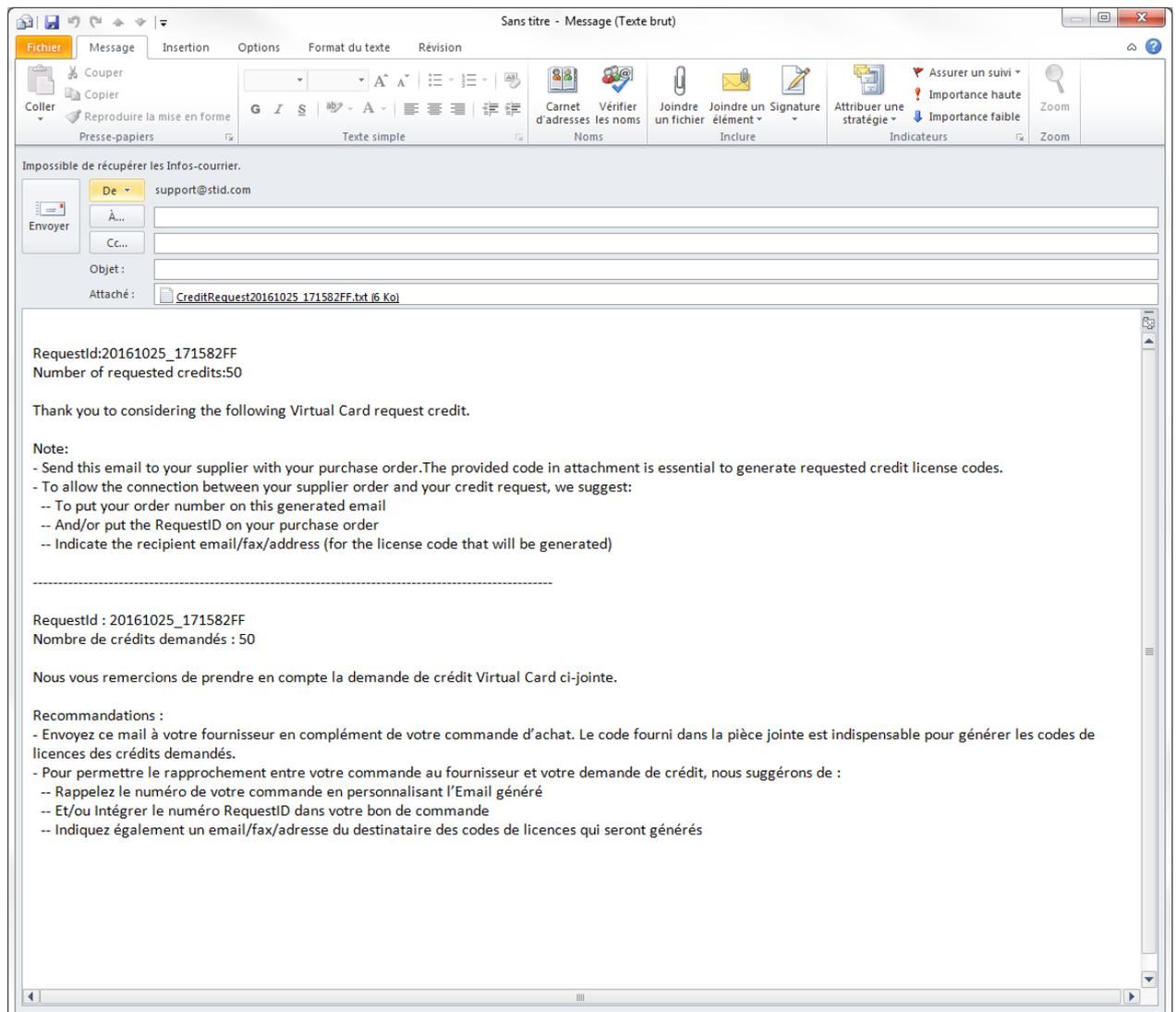
- « Demande par mail » si le poste sur lequel est installé SECard a une connexion internet et un logiciel de messagerie actif
- « Générer un fichier texte » qui pourra être envoyé par mail ou tout autre moyen.

## 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.



Accueil



Paramètres



Droits utilisateur



Fichiers



Crédit



Configuration lecteur



Création badges



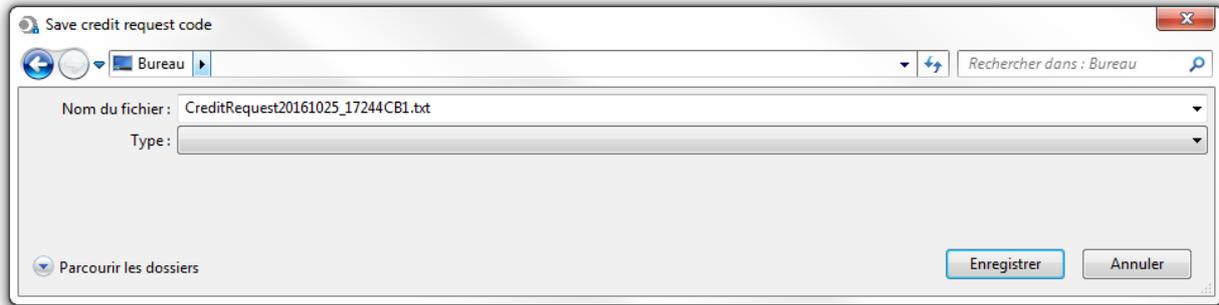
Outils

## Générer un fichier texte

Générer 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)

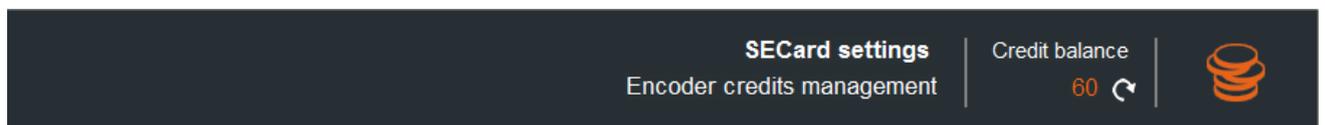
## Chargement des crédits

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

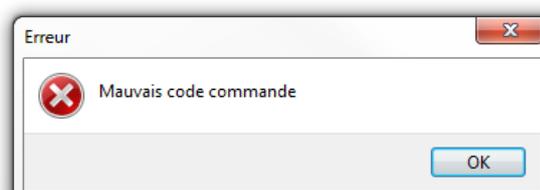
- 3- Cliquer sur

## Solde de crédits

Permet de connaître 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 :





### III. Configuration lecteur - SCB / OCB

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCF
- Création badges
- Outils

SECard - Le logiciel pour rester maître de sa sécurité - Administrateur

Accueil
Configuration Lecteur

Créer votre configuration du lecteur en toute indépendance

**Démarrer ma configuration lecteur**

Compatible avec :  
Architect®, Architect® One, Architect® Blue,  
WAL2, MS2 & MS2S Blue

Configurations courantes :

**Famille du lecteur courant = Architect®, Architect® One, Architect® Blue, WAL, MS2 and MS2S Blue**  
Version SCB = 14

Les paramètres Lecteur sont configurés

Pas de configuration MIFARE Classic ou Plus niveau 1 active  
Pas de configuration MIFARE Plus niveau 3 active  
Pas de configuration MIFARE DESFire EV1 active  
Pas de configuration MIFARE Ultra Light C active  
Pas de configuration CPS3 active  
Pas de configuration 125kHz/3,25MHz active  
Pas de configuration NFC\_HCE active  
Pas de configuration Blue Mobile ID active  
Aucune configuration valide de code matriciel disponible

Opération en cours : Aucune

État :

Configuration détaillée
 Sauvegarder

Imprimer
 Effacer le contenu

Charger une configuration avec le câble

Lire badge / Badge virtuel
 Créer badge / Badge virtuel

<p><b>Démarrer ma configuration lecteur</b></p> <p>Compatible avec : Architect®, Architect® One, Architect® Blue, WAL2, MS2 &amp; MS2S Blue</p>	Permet d'ouvrir l'assistant de configuration pour les lecteurs
	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.
Assistant SCB	Permet de charger la configuration dans le lecteur par la communication série.
Assistant OCB Nouveau 3.6	Permet de charger la configuration dans le lecteur par la communication série ou de créer le fichier de configuration.
Lire badge / Badge virtuel	Permet de lire un badge de configuration SCB/OCB RFID. <b>Utilise la clé entreprise SCB/OCB définie dans l'assistant de configuration.</b>
Créer badge / Badge virtuel	Permet de créer un badge de configuration SCB/OCB RFID / virtuel selon les paramètres définis dans l'assistant de configuration.

Cette version de SECard permet de créer la configuration des lecteurs de la gamme WAL, de la gamme Architect® (ARC, ARC One, ARCS et ARCS Blue) et des modules OEM MS2, MS2S.

Assistant SCB

### Assistant de configuration SCB

Pour les modèles : Architect®, Architect® One, Architect® Blue, WAL, MS2 et MS2S Blue

Sélectionner votre type de SCB Paramètres complets

Configuration lecteur	<span>Lecteur sécurisé (SCB)</span>	<span>Paramètres</span>	<span>Clés</span>	<input checked="" type="checkbox"/>
MIFARE DESFire	<span>Mode manuel</span>	<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
MIFARE Plus SL3	<span>Mode manuel</span>	<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
MIFARE Classic/SL1	<span>Mode manuel</span>	<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
MIFARE UltraLight/C		<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
Blue/NFC Mobile ID		<span>Paramètres</span>	<span>Clés</span>	<input checked="" type="checkbox"/>
125 kHz		<span>Paramètres</span>		
Code matriciel / code QR		<span>Paramètres</span>		
Application Multiservices Citoyenne (AMC)		<span>Paramètres</span>		<input type="checkbox"/>
NFC-HCE		<span>Paramètres</span>	<span>Clés</span>	

Fermer

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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## SCB-Charger une configuration avec le câble

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

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

- 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 « Charger une configuration avec le câble » 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).

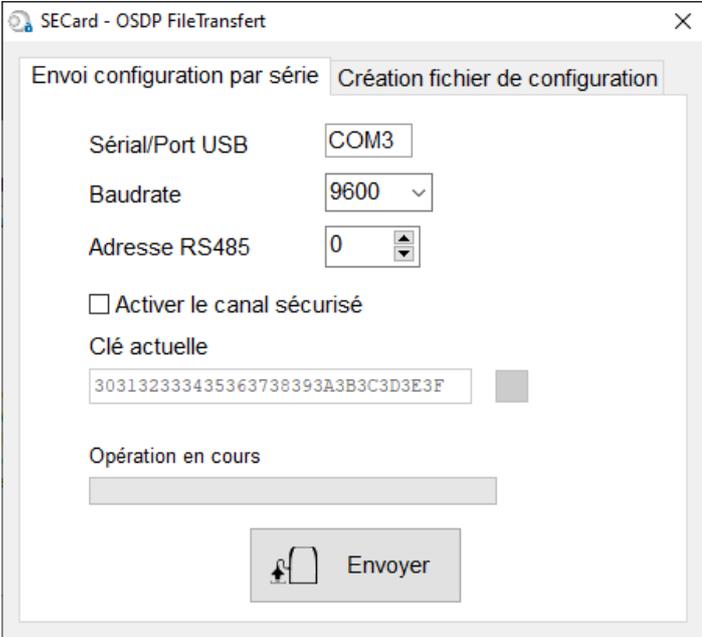
## OCB-Charger une configuration avec le câble ou créer un fichier de configuration Nouveau 3.6

A partir de la version 3.6.0, la configuration OCB, créée dans SECard, peut être chargée soit :

- directement avec SECard dans le lecteur via sa liaison série
- en utilisant la commande `osdp_FileTransfer` et le fichier de configuration créé avec SECard.

### ➤ Envoi configuration par série :

- 1- Quand tous les paramètres ont été renseignés dans l'assistant de configuration OCB cliquer sur 



- 2- Connecter le lecteur W33-XX-7OS à configurer via un câble convertisseur au PC.
- 3- Choisir le numéro de port de communication / le Baudrate (par défaut 9600) / l'adresse RS485 (par défaut 0) du lecteur.
- 4- Si le lecteur est utilisé en Secure Channel : sélectionner « Activer le canal sécurisé » et renseigner la valeur de la clé.
- 5- Cliquer sur Envoyer.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



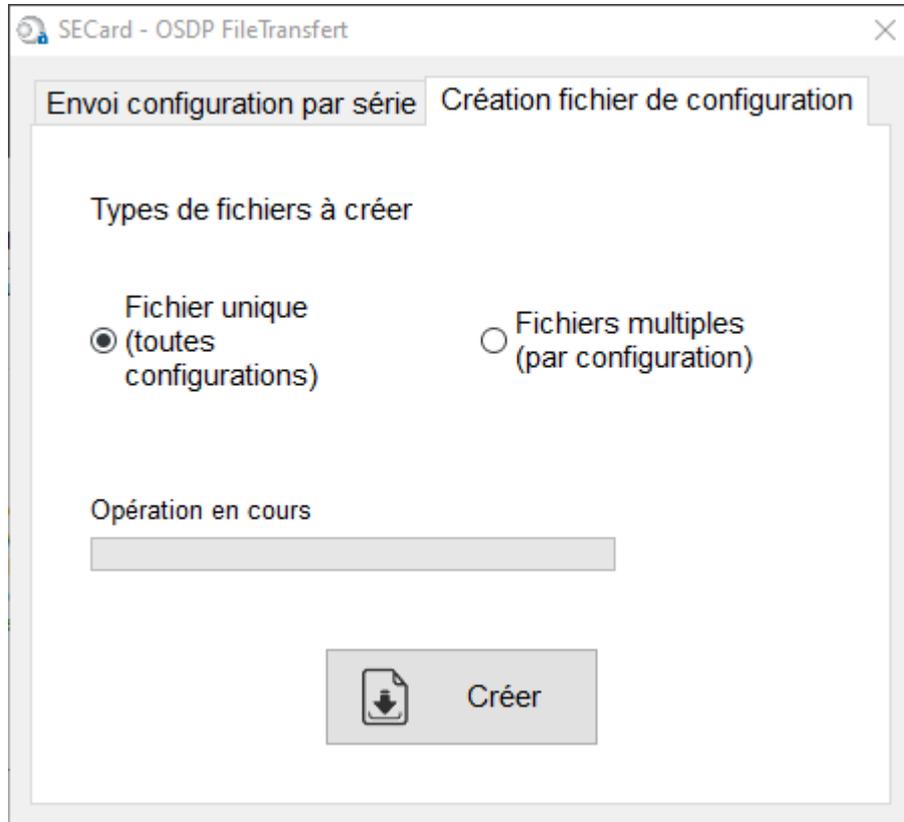
Création badges



Outils

➤ **Création fichier de configuration :**

- 1- Quand tous les paramètres ont été renseignés dans l'assistant de configuration OCB cliquer sur 



2- Type de fichiers à créer :

Fichier unique : toutes les configurations sont enregistrées dans un même fichier.

Fichiers multiples : chaque configuration est enregistrée dans son propre fichier :

- MUSECARDmulti\_125kHz.ftd
- MUSECARDmulti\_AMC.ftd
- MUSECARDmulti\_AppleWallet.ftd
- MUSECARDmulti\_BT.ftd
- MUSECARDmulti\_Classic.ftd
- MUSECARDmulti\_DESFire.ftd
- MUSECARDmulti\_MatrixCode.ftd
- MUSECARDmulti\_PlusSL3.ftd
- MUSECARDmulti\_ReaderOSPD.ftd
- MUSECARDmulti\_ReaderTexts1.ftd
- MUSECARDmulti\_ReaderTexts2.ftd
- MUSECARDmulti\_ReaderTexts3.ftd
- MUSECARDmulti\_ReaderTexts4.ftd
- MUSECARDmulti\_ReaderTexts5.ftd
- MUSECARDmulti\_ReaderTexts6.ftd
- MUSECARDmulti\_ReaderTexts7.ftd
- MUSECARDmulti\_ReaderTexts8.ftd
- MUSECARDmulti\_ReaderTexts9.ftd
- MUSECARDmulti\_ReaderTexts10.ftd
- MUSECARDmulti\_ReadrBT.ftd
- MUSECARDmulti\_UltralightC.ftd

- 3- Choisir un nom et un dossier pour la sauvegarde du(des) fichier(s).



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## Création des badges RFID SCB/OCB

A partir de la version V3.6.x de SECard, les badges de configuration SCB/OCB doivent être créés avec les technologies de badges ci-dessous :

Type de puce à utiliser
MIFARE® DESFire® EV2/ EV3 non locked 8ko

Il est possible de réutiliser un badge SCB/OCB dès lors que l'on connaît sa clé Maître (cf I. 5 - Compatibilité Modification 3.6)

### Attention

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

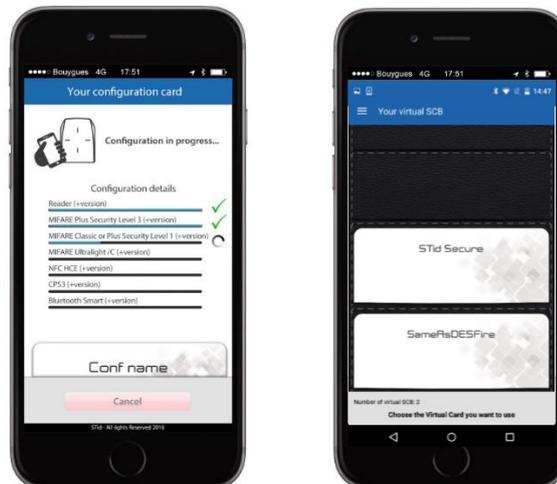
Exemple : un lecteur ARC-R31-E-103-xx ne pourra pas être reconfiguré en ARC-R31-E-PH5-xx.  
Il est nécessaire de retourner le produit en usine pour un changement de référence.

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

A partir de la version V3.6.x de SECard intégrant le paramétrage des lecteurs Bluetooth®, les badges de configuration peuvent être créés en virtuel sur un smartphone.

Un smartphone peut contenir plusieurs badges virtuels de configuration.

L'application STid settings est requise.





Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### III. 1 - Assistant SCB : paramètres lecteurs

#### Niveau SCB

Sélectionner votre type de SCB

- Paramètres complets
- Paramètres complets
- Paramètres Lecteur uniquement
- Paramètres Puces uniquement

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. (non disponible pour la configuration des lecteurs Bluetooth®).
- ❖ 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.

**Configuration lecteur :** Dans le menu déroulant, choisir Lecteur sécurisé (SCB)

Lecteur sécurisé (SCB)

- Lecteur sécurisé (SCB)
- Lecteur OSDP (OCB)

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

	<a href="#">Cliquez-ici</a>	Assistant de configuration / Choix de la version de SECard
	<a href="#">Cliquez-ici</a>	Sélection de la référence du lecteur à configurer
	<a href="#">Cliquez-ici</a>	Protocole de communication du lecteur
	<a href="#">Cliquez-ici</a>	Protections physiques du lecteur
	<a href="#">Cliquez-ici</a>	LED et Buzzer
	<a href="#">Cliquez-ici</a>	Clavier, biométrie et options des lecteurs ARC
	<a href="#">Cliquez-ici</a>	Options écran tactile
	<a href="#">Cliquez-ici</a>	Options Blue/NFC Mobile ID
	<a href="#">Cliquez-ici</a>	Options QR Code / Matrix

## SCB – Etape 1

SCB wizard

### Configuration wizard

Create your SCB reader configuration card

1
2
3
4
5
6
7
8
9

Wizard configuration steps:

- Reader selection
- Reader communication protocol
- Reader physical protections
- LED and Buzzer
- Keypad, biometrics and ARC new options
- Touchscreen options
- Bluetooth® / NFC options
- Matrix code / QR code options and settings

The functions available with the configuration card (SCB) depend on the generation of the reader's firmware.  
You must choose the SECard version corresponding to your reader generation.

[Click to view firmware compatibilities array](#)

**Choose SECard version to use**

SECard v3.6.x - SCB v16

[Click to view compatibilities ARC/ARCS, ARC1/ARC1S, WAL2 and MS2/MS2S](#)

Back
Next
Cancel

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*.

Compatibilités entre les versions de SECard et les firmwares lecteurs

		SECard						
		v3.0.x	v3.1.x	v3.2.x	v3.3.x	v3.4.x	v3.5.x	v3.6.x
ARC-WAL Firmwares	Z05-06	x						
	Z07	x <sup>1</sup>	x					
	Z08-09-10	x <sup>1</sup>	x <sup>1</sup>	x				
	Z11-13	x <sup>1</sup>	x <sup>1</sup>	x <sup>1</sup>	x			
	Z14-15	x <sup>1</sup>	x <sup>1</sup>	x <sup>1</sup>	x <sup>1</sup>	x		
	Z16	x <sup>1</sup>	x					
	>=Z17	x <sup>1</sup>	x					

x Entièrement compatible  
x<sup>1</sup> Fonctions limitées pour assurer la rétro-compatibilité

Compatibilités entre les versions de SECard et les firmwares lecteurs

Les lecteurs ARC1/ARC1S et MS2/MS2S se configurent comme un lecteur ARC/ARCS Blue hormis dans ces trois cas d'usage :

- si le mode Pulse est sélectionné, les LEDs de l'ARC1/ARC1S seront fixes sur la couleur sélectionnée ;
- si le mode ECO est sélectionné, seul le temps de Scan sera impacté (aucun impact sur la luminosité des LEDs) ;
- si les options Biométrie Clavier et/ou Écran tactile sont activées, elles ne seront pas prises en compte.

L'ARC1 Ph1 ne prend en compte que les paramètres MIFARE Classic et les UID des autres puces.

Pour l'ARC1S Blue et MS2S Blue les modes d'identification disponibles sont : Badge, Tap Tap, Remote et Mains-libres.

Pour l'ARCS Blue les modes d'identification disponibles sont : Badge, Slide, Tap Tap, Remote et Mains-libres.

Le lecteur WAL est configuré comme un lecteur ARC excepté dans les cas suivants :

- si le mode Pulse est sélectionné, la LED du WAL sera fixe à la couleur sélectionnée ;
- si le mode ECO est sélectionné, seulement le temps du Scan sera impacté (pas d'impact sur la luminosité de la LED) ;
- si la Biométrie, le Clavier ou l'Écran tactile sont activés alors ils ne seront pas pris en compte ;
- si les fonctionnalités Bluetooth® sont activées, elles ne seront pas prises en compte ;
- si le mode Arc-en-ciel est sélectionné, la LED du WAL restera fixe sur la couleur bleue.

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

## SCB – Etape 2

Assistant SCB

### Sélection du lecteur

Sélectionner le type de lecteur à configurer

1 2 3 4 5 6 7 8 9

#### ID privé et/ou UID (lecteurs PH5/PH1/BT1)

<b>TTL</b>	Wiegand ou Data/Clock (R31) <input checked="" type="radio"/>	Wiegand Chiffré (S31) <input type="radio"/>	
<b>Série</b>	RS232 (R32) <input type="radio"/>	USB (R35) <input type="radio"/>	RS485 (R33) <input type="radio"/>
<b>Série Chiffrée</b>	RS232 (S32) <input type="radio"/>	USB (S35) <input type="radio"/>	RS485 (S33) <input type="radio"/>
<b>Série avec décodeur Easy Secure</b>	RS485/Wiegand ou Data/Clock (R33+INTR33E) <input type="radio"/>		
	RS485 / RS485 (S33+INT-E 7AA/7AB) <input type="radio"/>		
<b>Série avec décodeur Easy Remote</b>	RS485 / Wiegand ou Clock&Data (R33+INTR33F) <input type="radio"/>	<i>Choisir TTL R31</i>	
	RS485 / Wiegand Chiffré (R33+INTS33F) <input type="radio"/>	<i>Choisir TTL S31</i>	

#### UID (lecteurs 103)

TTL  Wiegand ou Data/Clock (R31/103)

#### Activation fonctionnalités

- |   |   |   |   |   |   |
|---|---|---|---|---|---|
|  |  |  |  |  |  |
| <input type="checkbox"/> Clavier  | <input type="checkbox"/> Écran tactile  | <input type="checkbox"/> Blue/NFC Mobile ID   | <input type="checkbox"/> Biométrie  | <input type="checkbox"/> Prox 125 kHz   | <input type="checkbox"/> Matrix code / QR code  |

← Précédent

→ Suivant

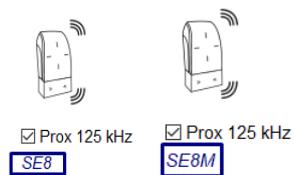
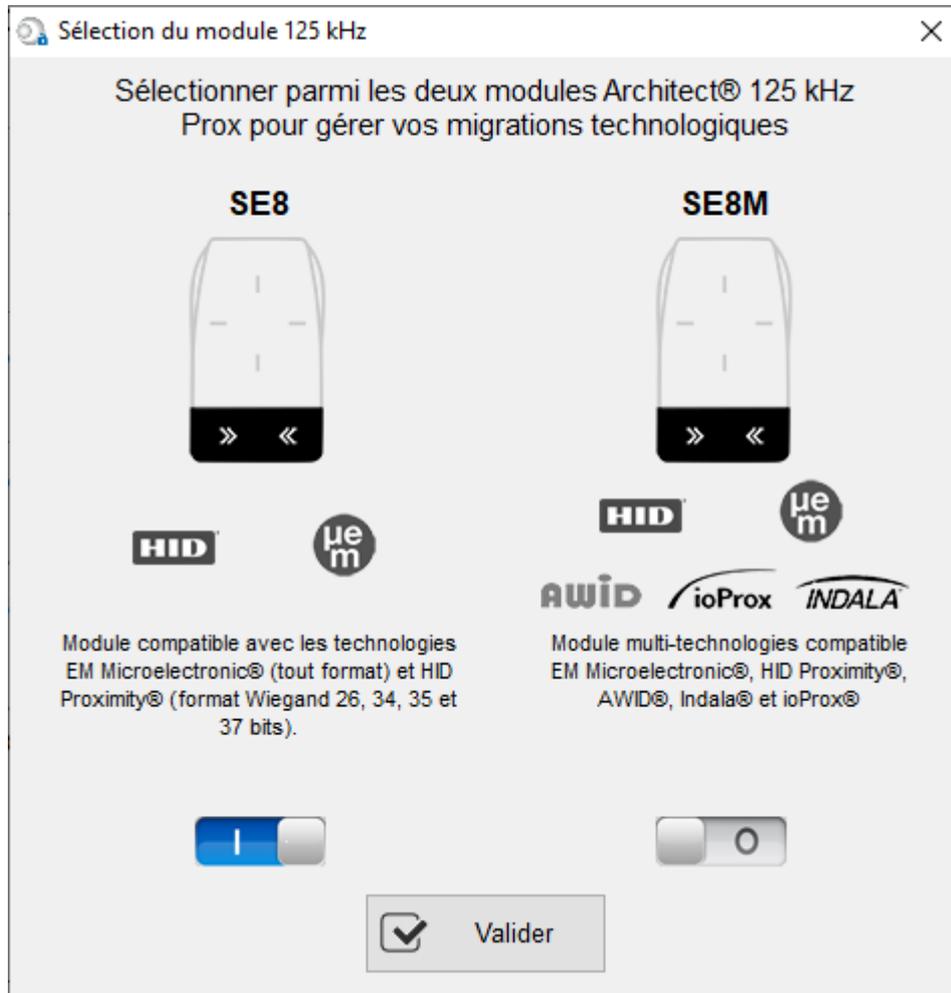
✕ Annuler

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/NFC Mobile ID.
- ❖ D'activer la configuration biométrique.

-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

- ❖ D'activer la configuration du module 125 kHz et de choisir le modèle du module à configurer (SE8 ou SE8M).



Le modèle choisi pour le module apparaît sur l'écran :

**Le module SE8M est uniquement disponible pour les lecteurs R31/S31 et R31/103 en protocole de sortie Wiegand (Wiegand 26bits-3i par défaut).**

Ce choix impacte la fenêtre « Paramètres » du 125 kHz.

- ❖ D'activer la configuration du module code matriciel.

### SCB – Etape 3 Ajout fonctionnalité 3.6

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).



Accueil



Paramètres

Configuration  
lecteur

SCB / OCB



SKB



BCC



SSCP

Création  
badges

Outils

## 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  $\leq$  UID/ID  $\leq$  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 apparaît lorsque le type de lecteur sélectionné à l'étape 2 est en sortie série Modification 3.6 :

Assistant SCB

## Protocole de communication du lecteur

Type de protocole et paramètres

1
2
3
4
5
6
7
8
9

### Sécurité de l'ID privé

Chiffrement authentifié des données

### Options du protocole

Taille  octet(s)

Code site forcé sur l'UID  
 2 octets Valeur

ID-Len  ID-Tag  
Valeurs

### Paramètres de communication série

Baudrate  Adresse RS485

Mode bidirectionnel

Mode de sécurité

#### Format des données

Hexadécimal  Décimal

CR/LF  LRC  
 ASCII  STX+ETX  
 Pas de zéro de bourrage

### ISO14443-3B PUPI / iClass

Autorisé  MSB First

### Intervalle de filtrage ID (LSB)

UID/ID range  à

← Précédent
→ Suivant
✕ Annuler

## 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 apparaît alors soulignée. Cette manipulation ne fonctionne pas pour un encodage mais uniquement pour la relecture d'un identifiant. Uniquement disponible sur les lecteurs séries.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

- ❖ « 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.

### Nouveauté 3.6

En mode Série, il est possible de personnaliser la donnée avant transmission avec les informations suivantes :

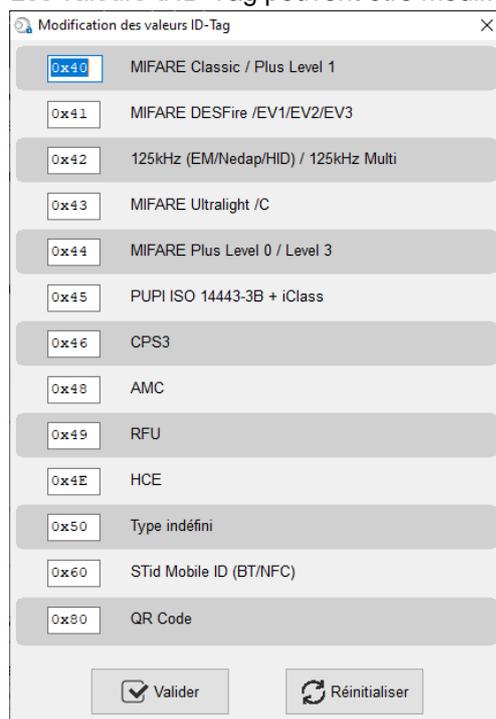
<Prefix><ID-Tag><ID-Len><ID-Number><Suffix>

- ❖ *Prefix* : ajoute un préfixe avant d'envoyer la trame. Valeur hexadécimale sur maximum 5 octets.
- ❖ *Suffix* : ajoute un suffixe avant d'envoyer la trame. Valeur hexadécimale sur maximum 5 octets.

#### ❖ ID-Tag :

Un octet qui identifie le type de « tag » lu et sera ajouté à la trame. L'ID-Tag sera ajouté à un UID ou à un ID privé.

Les valeurs d'ID-Tag peuvent être modifiées dans le tableau ci-dessous :



ID-Tag	Protocole
0x40	MIFARE Classic / Plus Level 1
0x41	MIFARE DESFire /EV1/EV2/EV3
0x42	125kHz (EM/Nedap/HID) / 125kHz Multi
0x43	MIFARE Ultralight /C
0x44	MIFARE Plus Level 0 / Level 3
0x45	PUPi ISO 14443-3B + iClass
0x46	CPS3
0x48	AMC
0x49	RFU
0x4E	HCE
0x50	Type indéfini
0x60	STid Mobile ID (BT/NFC)
0x80	QR Code

Le bouton Reset restaure les valeurs STid par défaut.

- ❖ *ID-Len* : 2 octets indiquant la longueur de ID-Number
  - Pour une donnée en Hexadécimal : ID-Len = nombre d'octets de l'ID-Number
  - Pour une donnée en décimal : ID-Len = nombre de caractères de l'ID-Number

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

**Exemple 1 :**  
Paramétrages :

**Private ID security**

Data authenticated encryption

**Protocol options**

Data size  byte(s)

Forced site code on UID

2 bytes Value

Prefix  Suffix

ID-Len  ID-Tag See values

**Serial communication parameters**

Baudrate  RS485 Address

Bidirectionnal mode

Security mode

**Data format**

Hexadecimal  Decimal

CR/LF  LRC

ASCII  STX+ETX

No leading zeros

Tag : DESFire  
ID-Number = 0000ABCDEF  
ID-Len = 5

Trame :

STX	Prefix	ID-Tag	ID-Len	ID-Number	Suffix	LRC	0x0D	0x0A	ETX
02	1234	41	0005	0000ABCDEF	5678	LRC <i>calculé sur les données 12344100050000ABCDEF5678</i>	0D	0A	03

**Exemple 2 :**  
Paramétrages :

**Private ID security**

Data authenticated encryption

**Protocol options**

Data size  byte(s)

Forced site code on UID

2 bytes Value

Prefix  Suffix

ID-Len  ID-Tag See values

**Serial communication parameters**

Baudrate  RS485 Address

Bidirectionnal mode

Security mode

**Data format**

Hexadecimal  Decimal

CR/LF  LRC

ASCII  STX+ETX

No leading zeros

Tag : DESFire  
ID-Number = 0000ABCDEF  
ID-Len = 5

Trame :

Prefix	ID-Tag	ID-Len	ID-Number	Suffix	0x0D	0x0A
31323334	3431	30303035	30303030414243444546	35363738	0D	0A



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### Exemple 3 :

Paramétrages :

Tag : DESFire  
ID-Number = 0000ABCDEF

ID-Number en décimal vaut 000011259375, avec l'option « Pas de bourrage », ID-Number=11259375 soit 8 caractères.

Trame :

Prefix	ID-Tag	ID-Len	ID-Number	Suffix	LRC	0x0D	0x0A
1234	41	0008	11259375	5678	LRC	0D	0A

### Exemple 4 : Mode bidirectionnel

Paramétrages :

Tag : DESFire  
ID-Number = 0000ABCDEF

Trame

Len	Prefix	ID-Tag	ID-Len	ID-Number	Suffix
000C	1234	41	0005	0000ABCDEF	5678

## SCB – Etape 4

Assistant SCB

### Protections physiques du lecteur

Options : signaux de vie/arrachement

1 2 3 4 5 6 7 8 9

**Options de protection du lecteur**

Enregistrer les clés utilisateurs en mémoire

Effacer les clés lors de l'arrachement

LED rouge par défaut après arrachement

Signal d'arrachement

ID d'arrachement

0

Signaux d'arrachement et de vie mutualisés

Vie  Arrachement

**Signal de vie**

Désactivé

Générique

Spécifique au lecteur

**Sensibilité de l'accéléromètre**

Normale

### 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 **T10 - 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 **T11 - 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 **T12 - Signal de vie / arrachement mutualisés.**

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



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## Signal de vie

Permet d'activer / désactiver le signal et de choisir le type de signal « Générique » ou « Spécifique ».  
Se reporter à [T9 - Signal de vie](#).

## Sensibilité de l'accéléromètre

Les lecteurs 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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## SCB – Etape 5

Assistant SCB

### LED et Buzzer

Options et paramètres

1 2 3 4 5 6 7 8 9

#### État par défaut de la LED

Mode

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

Couleur



Durée clignotement x100ms

4

Vitesse pulsation  
Moyen

#### Action détection carte

Nb clignotement

0

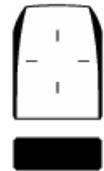
Durée LED x100ms

0

Durée Buzzer x100ms

4

Couleur



Fermeture du relais

1 s

LED à la connexion Bluetooth®

#### Contrôle externe couleur LED

Couleur LED1



Couleur LED2



Couleur LED1+LED2



Volume sonore du Buzzer Fort

Autoriser le contrôle externe LED/Buzzer

Période de requête 1 x100m

Buzzer instantané

← Précédent

→ Suivant

✕ Annuler

### Etat par défaut de la LED

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

Modes disponibles pour les lecteurs ARC :

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

Modes disponibles pour les lecteurs WAL :

- ❖ Fixe
- ❖ Clignotement classique

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



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## 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.
- ❖ 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.
- ❖ Fermeture du relai :  
Pour ARC / ARCS ferme le relais pendant le temps sélectionné, si la carte a été lue (UID ou PrivateID). Si cette fonction est activée, le relais n'est plus utilisé pour les fonctionnalités d'arrachement ou de sonnette.

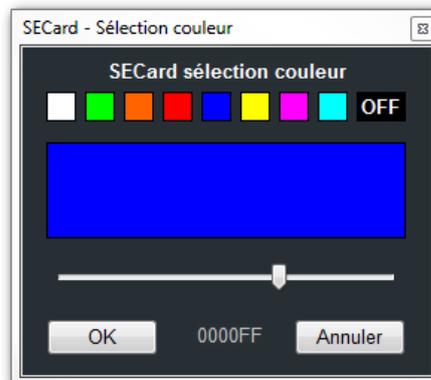
Note : Nb clignotement ou Durée LED définit, pour l'ARC écran, le temps d'affichage de l'état « Image et texte détection badge ».

## Volume sonore du Buzzer

Permet de définir le niveau sonore du buzzer **uniquement pour les lecteurs 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 les lecteurs ARC uniquement, il est possible de 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.

## SCB – Etape 6 Ajout fonctionnalité 3.6

Assistant SCB

### Clavier, biométrie et nouvelles options des ARC

1 2 3 4 5 6 7 8 9

#### Paramètres du lecteur biométrique

Niveau de sécurité	Nombre de doigts à enrôler	Seuil	Détection faux doigt
1	1	5	Désactivée
Nombre de doigts à vérifier			
1	<input type="checkbox"/> Consolidation de la capture des minuties	<input type="checkbox"/> Authentification biométrique sous contrainte	

#### Options clavier

<b>Mode</b> <input checked="" type="radio"/> Badge OU Touche <input type="radio"/> Badge ET Touche <input type="radio"/> Mode 26 bits Wiegand	<b>Appui touche</b> <input type="checkbox"/> Buzzer <input type="checkbox"/> Scintillement
<b>Format</b> <input type="radio"/> 4 bits trame <input type="radio"/> 4 bits <input checked="" type="radio"/> 8 bits <input type="radio"/> X touches trame	<b>Affichage</b> <input checked="" type="radio"/> Clavier <input type="radio"/> Image par défaut <input type="checkbox"/> Clavier aléatoire (Scramble) <input type="checkbox"/> Rétroéclairage <input checked="" type="radio"/> Eclairage permanent <input type="radio"/> Durée d'éclairage
Code site (FC) 255	Nombre de touches 4
	6 s

#### Options ARC

<input type="checkbox"/> Mode Eco (basse consommation)	
<input type="checkbox"/> Atténuation de la LED	
<input type="checkbox"/> Couper la configuration UHF	
<input type="checkbox"/> Mode silencieux	

← Précédent

→ Suivant

✕ Annuler

### 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 entraîne 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.



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

- ❖ Authentification biométrique sous contrainte : L'UID ou ID privé retourné par le lecteur sera modifié pour y inclure le numéro du doigt en MSB avec lequel l'utilisateur s'est authentifié. Cette fonctionnalité est prioritaire sur le code site si utilisé.

Exemple : ID du badge 0x1122334455 / 73 588 229 205 (décimal)

Détection du doigt numéro 2 : ID envoyé par le lecteur 0x**0**222334455 / 9 163 719 765.

Note : non disponible en protocole Wiegand 3T, le 1<sup>er</sup> octet étant utilisé pour le type puce.

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

- ❖ Détection faux doigt : Désactive / Active la détection de faux doigts avec un niveau de détection spécifié

Désactivée	▼
Désactivée	
Faible / FRR=0.5%	
Moyen / FRR=1.5%	
Haut / FRR=5%	
Critique / FRR=15~20%	



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges

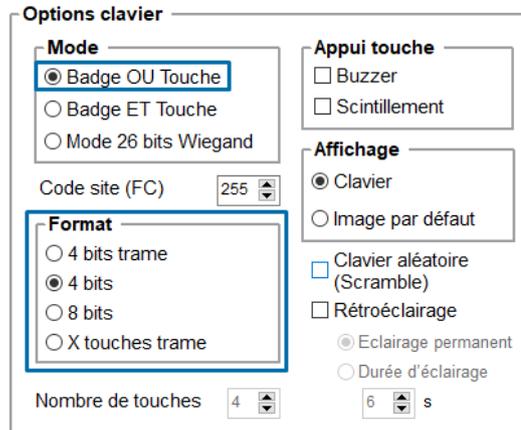


Outils

## Options clavier

Pour plus de détail, sur le fonctionnement et les formats, se reporter à [T6 - Au sujet des lecteurs Clavier](#). Permet de choisir entre les modes « Badge OU Touche », « Touche ET Badge » et « Mode 26 bits Wiegand »

- ❖ Badge OU Touche + choix du format :

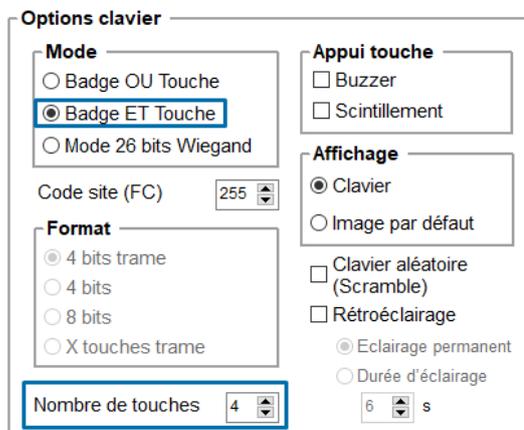


The screenshot shows the 'Options clavier' configuration window. The 'Mode' section has 'Badge OU Touche' selected. The 'Appui touche' section has 'Buzzer' and 'Scintillement' unchecked. The 'Affichage' section has 'Clavier' selected, 'Image par défaut' unchecked, 'Clavier aléatoire (Scramble)' unchecked, and 'Rétroéclairage' unchecked. The 'Format' section has '4 bits' selected. The 'Code site (FC)' is set to 255. The 'Nombre de touches' is set to 4. The 'Durée d'éclairage' is set to 6 seconds.

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.

- ❖ Touche et Badge + nombre de touches :



The screenshot shows the 'Options clavier' configuration window. The 'Mode' section has 'Badge ET Touche' selected. The 'Appui touche' section has 'Buzzer' and 'Scintillement' unchecked. The 'Affichage' section has 'Clavier' selected, 'Image par défaut' unchecked, 'Clavier aléatoire (Scramble)' unchecked, and 'Rétroéclairage' unchecked. The 'Format' section has '4 bits' selected. The 'Code site (FC)' is set to 255. The 'Nombre de touches' is set to 4. The 'Durée d'éclairage' is set to 6 seconds.

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

La séquence 'saisie touches + badge' est envoyé selon le protocole en cours (sauf W3i, W3EB, W3V, W3W, W3y, W3z).

-  Accueil
-  Paramètres
-  Configuration lecteur
-  SCB / OCB
-  SKB
-  BCC
-  SSCP
-  Création badges
-  Outils

❖ Mode 26 bits Wiegand *Nouveau 3.6* :

**Options clavier**

**Mode**

Badge OU Touche

Badge ET Touche

Mode 26 bits Wiegand

Code site (FC)

**Format**

4 bits trame

4 bits

8 bits

X touches trame

**Appui touche**

Buzzer

Scintillement

**Affichage**

Clavier

Image par défaut

Clavier aléatoire (Scramble)

Rétroéclairage

Eclairage permanent

Durée d'éclairage

Nombre de touches   s

Ce mode active le format Wiegand 26 bits uniquement pour la donnée clavier.

Les autres identifiants (MIFARE® DESFire®, Bluetooth®, 125...) seront remontés selon le protocole défini à l'étape 3.

Dans ce mode, le code clavier est envoyé au système sous la forme d'un identifiant badge accolé à un code site défini dans le champ « Code site (FC) ».

# : valide la saisie du code PIN.

\* : annule la saisie du code PIN entrée précédemment, le lecteur émet 4 bip pour indiquer la prise en compte.

bit 1	bit 2 ... bit 9	bit 10 ... bit 25	bit 26
<i>Parité paire sur bit 2 ... bit 13</i>	<i>Code site FC (0 à 255) Se configure dans SECard bit 2 = MSB</i>	<i>Code PIN (0 à 65 535) bit 10 = MSB</i>	<i>Parité impaire sur bit 14 ... bit 25</i>



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

#### ❖ Affichage :

##### Affichage

- Clavier  
 Image par défaut

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.
- Wiegand 26-bits :
  - après la lecture d'un badge valide.
  - toutes les 30 secondes.
  - à la suite de l'appui de la touche #.

#### ❖ Appui touche :

##### Appui touche

- Buzzer  
 Scintillement

Buzzer : permet d'activer / désactiver le Buzzer lorsqu'un utilisateur appuie sur une touche du clavier.

- ❖ **Rétroéclairage** : permet d'activer / désactiver le rétroéclairage du clavier. Options disponibles :

Eclairage permanent : Rétroéclairage permanent du clavier.

Durée d'éclairage : Rétroéclairage du clavier lors d'un appui touche et pendant un temps configurable.

Scintillement : en fonction du mode rétroéclairage choisi, permet de faire flasher ON ou OFF les LEDS du rétroéclairage du clavier lorsqu'un utilisateur appuie sur une touche du clavier.

<p><b>Appui touche</b></p> <p><input type="checkbox"/> Buzzer</p> <p><input type="checkbox"/> Scintillement</p> <p><b>Affichage</b></p> <p><input checked="" type="radio"/> Clavier</p> <p><input type="radio"/> Image par défaut</p> <p><input type="checkbox"/> Clavier aléatoire (Scramble)</p> <p><input type="checkbox"/> Rétroéclairage</p> <p><input checked="" type="radio"/> Eclairage permanent</p> <p><input type="radio"/> Durée d'éclairage</p> <p>6 s</p>	<p><b>Appui touche</b></p> <p><input type="checkbox"/> Buzzer</p> <p><input type="checkbox"/> Scintillement</p> <p><b>Affichage</b></p> <p><input checked="" type="radio"/> Clavier</p> <p><input type="radio"/> Image par défaut</p> <p><input type="checkbox"/> Clavier aléatoire (Scramble)</p> <p><input checked="" type="checkbox"/> Rétroéclairage</p> <p><input checked="" type="radio"/> Eclairage permanent</p> <p><input type="radio"/> Durée d'éclairage</p> <p>6 s</p>	<p><b>Appui touche</b></p> <p><input type="checkbox"/> Buzzer</p> <p><input checked="" type="checkbox"/> Scintillement</p> <p><b>Affichage</b></p> <p><input checked="" type="radio"/> Clavier</p> <p><input type="radio"/> Image par défaut</p> <p><input type="checkbox"/> Clavier aléatoire (Scramble)</p> <p><input type="checkbox"/> Rétroéclairage</p> <p><input checked="" type="radio"/> Eclairage permanent</p> <p><input type="radio"/> Durée d'éclairage</p> <p>6 s</p>
<p>Pas de rétroéclairage Pas de flash du rétroéclairage sur appui touche</p>	<p>Rétroéclairage activé Pas de flash du rétroéclairage sur appui</p>	<p>Pas de rétroéclairage Flash court ON du rétroéclairage sur appui</p>
<p><b>Appui touche</b></p> <p><input type="checkbox"/> Buzzer</p> <p><input checked="" type="checkbox"/> Scintillement</p> <p><b>Affichage</b></p> <p><input checked="" type="radio"/> Clavier</p> <p><input type="radio"/> Image par défaut</p> <p><input type="checkbox"/> Clavier aléatoire (Scramble)</p> <p><input checked="" type="checkbox"/> Rétroéclairage</p> <p><input checked="" type="radio"/> Eclairage permanent</p> <p><input type="radio"/> Durée d'éclairage</p> <p>6 s</p>	<p><b>Appui touche</b></p> <p><input type="checkbox"/> Buzzer</p> <p><input type="checkbox"/> Scintillement</p> <p><b>Affichage</b></p> <p><input checked="" type="radio"/> Clavier</p> <p><input type="radio"/> Image par défaut</p> <p><input type="checkbox"/> Clavier aléatoire (Scramble)</p> <p><input checked="" type="checkbox"/> Rétroéclairage</p> <p><input type="radio"/> Eclairage permanent</p> <p><input checked="" type="radio"/> Durée d'éclairage</p> <p>6 s</p>	
<p>Rétroéclairage activé Flash court OFF du rétroéclairage sur appui</p>	<p>Rétroéclairage OFF et passe ON sur appui touche pendant un temps configurable puis revient OFF</p>	



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges

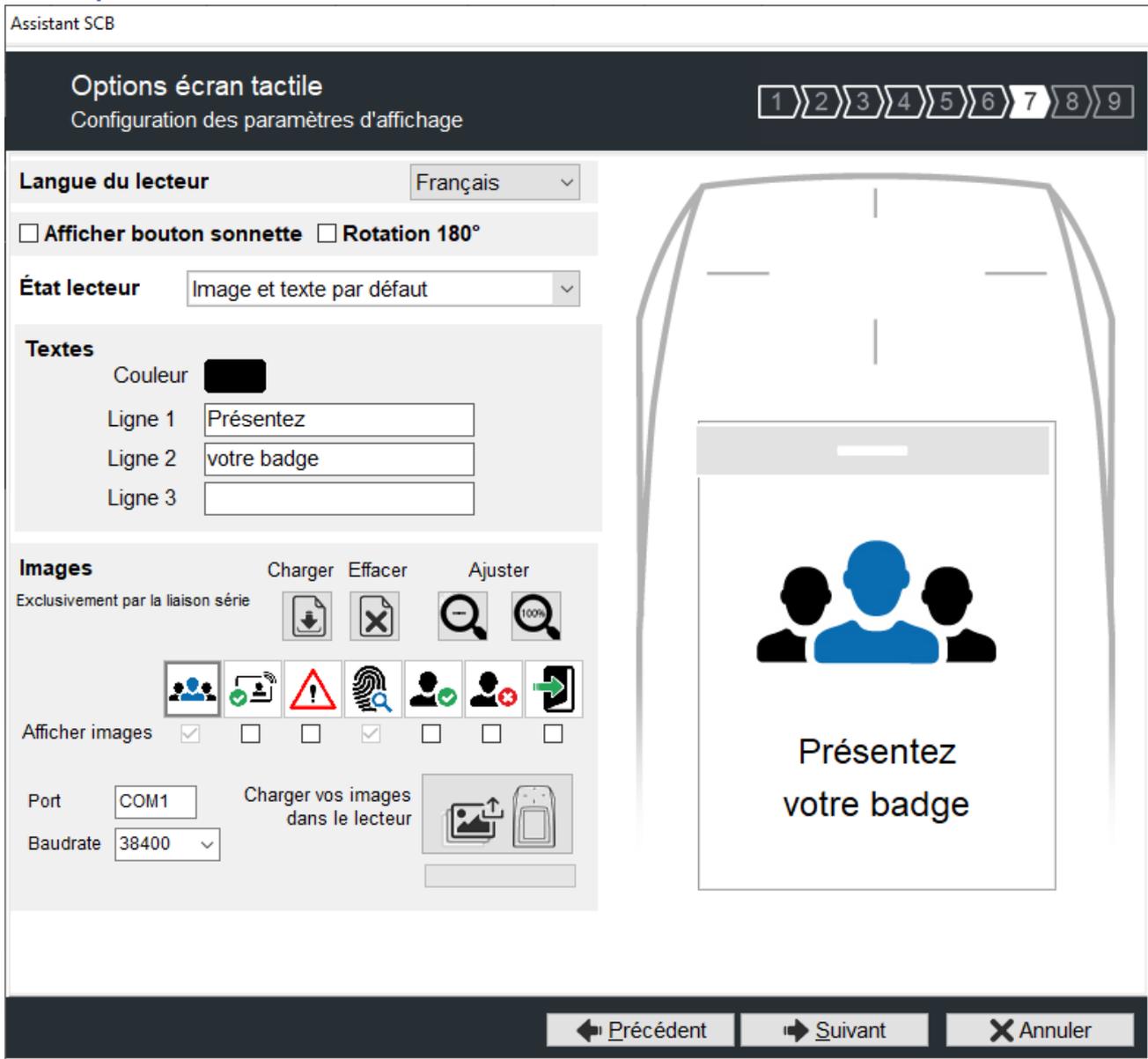


Outils

## ARC options

	<p>Mode Eco (basse consommation)</p> <p>Dans ce mode, l'éclairage est moins intense et les cycles de Scan sont réduits ce qui permet de réduire la consommation du lecteur d'environ 25%.</p>
	<p>Atténuation de la LED</p> <p>Réduit drastiquement l'intensité des LED.</p>
	<p>Couper la configuration UHF</p> <p>Permet de désactiver la puce UHF. Pour plus de détails sur la configuration par UHF, se reporter à <a href="#">VIII. 10 - UHF config</a></p>
	<p>Désactive le buzzer du lecteur.</p>

## SCB – Etape 7 Ajout fonctionnalité 3.6



**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)



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

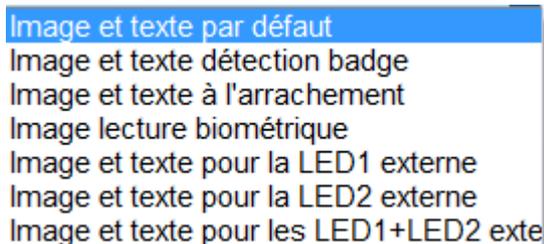
**Rotation 180°** : Permet de faire une rotation de l'image à 180°.

## Langue du lecteur

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

## État 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.

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

**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.

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

## 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

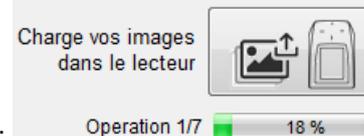
Le chargement des images dans le lecteur se fait par la liaison série du lecteur, pas par le SCB.

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

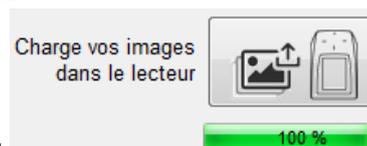
Port	COM1
Baudrate	38400 ▼



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



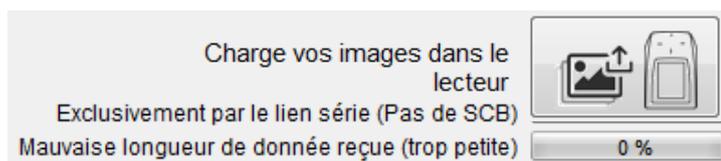
- 3 - L'avancement du chargement est indiqué par la barre de progression : L'opération est répétée pour chaque image, soit sept fois.



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 ».**



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## 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.

## Caractères acceptés :

'SPACE'	0x20
'!'	0x21
'"'	0x22
'#'	0x23
'\$'	0x24
'%'	0x25
'&'	0x26
''''	0x27
'('	0x28
)'	0x29
'•'	0x2A
'+'	0x2B
','	0x2C
'-'	0x2D
'.'	0x2E
'/'	0x2F
'0'	0x30
'1'	0x31
'2'	0x32
'3'	0x33
'4'	0x34
'5'	0x35
'6'	0x36
'7'	0x37
'8'	0x38
'9'	0x39
':'	0x3A
','	0x3B
'<'	0x3C
'='	0x3D
'>'	0x3E
'?'	0x3F
'@'	0x40
'A'	0x41
'B'	0x42
'C'	0x43
'D'	0x44
'E'	0x45
'F'	0x46
'G'	0x47
'H'	0x48
'I'	0x49

'J'	0x4A
'K'	0x4B
'L'	0x4C
'M'	0x4D
'N'	0x4E
'O'	0x4F
'P'	0x50
'Q'	0x51
'R'	0x52
'S'	0x53
'T'	0x54
'U'	0x55
'V'	0x56
'W'	0x57
'X'	0x58
'Y'	0x59
'Z'	0x5A
'['	0x5B
'\'	0x5C
']'	0x5D
'^'	0x5E
'_'	0x5F
''	0x60
'a'	0x61
'b'	0x62
'c'	0x63
'd'	0x64
'e'	0x65
'f'	0x66
'g'	0x67
'h'	0x68
'i'	0x69
'j'	0x6A
'k'	0x6B
'l'	0x6C
'm'	0x6D
'n'	0x6E
'o'	0x6F
'p'	0x70
'q'	0x71
'r'	0x72
's'	0x73

't'	0x74
'u'	0x75
'v'	0x76
'w'	0x77
'x'	0x78
'y'	0x79
'z'	0x7A
'{'	0x7B
' '	0x7C
'}'	0x7D
'~'	0x7E
'*'	0x7F
'\$'	0xA7
'°'	0xB0
'Ä'	0xC4
'Å'	0xC5
'Æ'	0xC6
'Ð'	0xD0
'Ö'	0xD6
'Ø'	0xD8
'þ'	0xDE
'Û'	0xDC
'ß'	0xDF
'à'	0xE0
'â'	0xE2
'ä'	0xE4
'å'	0xE5
'æ'	0xE6
'ç'	0xE7
'è'	0xE8
'é'	0xE9
'ê'	0xEA
'ë'	0xEB
'ì'	0xEE
'í'	0xEF
'ð'	0xF0
'ò'	0xF4
'ö'	0xF6
'ø'	0xF8
'û'	0xFB
'ü'	0xFC
'þ'	0xFE

## SCB – Etape 8

Assistant SCB

### Options Blue/NFC Mobile ID

Affiche les paramètres de configuration

1 2 3 4 5 6 7 8 9

**Mode Blue**

**Désignation**

Nom de configuration (max 14 caractères) \*   STid Mobile ID (CSN)

Code site \*  ⓘ \*Champs obligatoires

**Modes d'identification et distances de communication**

Badge ⓘ **Contact**  Mains-libres Jusqu'à ≈3m

Contact  
iOS: Bluetooth® / Android: NFC

Slide/Détection externe Très proche  Remote Jusqu'à ≈3m

Slide/Détection externe  
Très proche

Détection d'un événement externe via l'entrée lecteur  Remote Bouton télécommande actif

TapTap Jusqu'à ≈3m  Remote 1  Remote 2

**Options lecteur**

Déverrouillage du smartphone requis par le lecteur ⓘ  Ajout de nouvelles valeurs NFC SAK/ATQA

← Précédent    Suivant →    X Annuler

Quatre configurations sont disponibles pour l'authentification Bluetooth® :

Nom de la Configuration	Conf Mobile ID	Conf Mobile ID	SameAsDESFire	Personnalisable
<b>Caractéristiques</b>				
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/NFC

Permet de configurer le lecteur Bluetooth® pour fonctionner avec l'application STid Mobile ID® ou Orange™ Pack ID ou Open Mobile Protocol.

Ce choix a un impact sur les écrans de l'assistant de configuration Etape 8 et Blue/NFC Mobile ID® Paramètres :

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCF
- Création badges
- Outils

Wizard Step 8

Assistant SCB

**Options Blue/NFC Mobile ID**  
Affiche les paramètres de configuration

1 2 3 4 5 6 7 **8** 9

**Mode Blue** STid Mobile ID

**Désignation**

Nom de configuration (max 14 caractères) \* myConfigName  STid Mobile ID (CSN)

Code site \* BF33 ⓘ \*Champs obligatoires

**Modes d'identification et distances de communication**

Badge ⓘ

**Contact**

IOS: Bluetooth® / Android: NFC

Slide/Détection externe

Très proche

TapTap

Jusqu'à ~3m

Mains-libres

Jusqu'à ~3m

Remote

Jusqu'à ~3m

Bouton télécommande actif

Remote 1     Remote 2

**Options lecteur**

Déverrouillage du smartphone requis par le lecteur

Ajout de nouvelles valeurs NFC SAK/ATQA  
000000 000000 000000

← Précédent
→ Suivant
X Annuler

Wizard Blue/NFC Mobile ID settings

Assistant SCB

**Blue/NFC Mobile ID**

STid Mobile ID®

GET IT ON  
 Google Play

Download on the  
 App Store

**Paramètres lecteur**

**Mode de lecture**

ID Privé

Depuis DESFire

ID privé sinon CSN

**Type de clé**

Une clé (RW)

Deux clés (R et W)

**Données**

Taille 5

Décalage 0

Inversé

**Paramètres du badge d'accès virtuel**

Nom du badge d'accès virtuel (max 14 caractères)\*

myVCardName

Aperçu du badge

ID

Code site

Nom de la configuration

Interdire la suppression

Remote 1

Remote 2

Déverrouillage requis

Déverrouillage Bio

✓ Valider
X Annuler

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

Orange™ PAckID

Assistant SCB

1
2
3
4
5
6
7
8
9

**Options Blue/NFC Mobile ID**  
Affiche les paramètres de configuration

**Mode Blue** Orange Pack ID

**Désignation**

Nom de configuration (max 14 caractères) \*   STid Mobile ID (CSN)

Code site \*  ⓘ \*Champs obligatoires

**Modes d'identification et distances de communication**

Badge ⓘ

Contact Jusqu'à ~3m

Slide/Détection externe

Très proche Jusqu'à ~3m

Détection d'un événement externe via l'entrée lecteur

TapTap Jusqu'à ~3m

Mains-libres

Remote Jusqu'à ~3m

Bouton télécommande actif

Remote 1  Remote 2

**Options lecteur**

Déverrouillage du smartphone requis par le lecteur

ⓘ  Ajout de nouvelles valeurs NFC SAK/ATQA

← Précédent → Suivant ✕ Annuler

Assistant SCB
 Pack ID

**Paramètres lecteur**

**Mode de lecture**

ID Privé

Depuis DESFire

ID privé sinon CSN

**Type de clé**

Une clé (RW)

Deux clés (R et W)

**Données**

Taille

Décalage

Inversé

**Paramètres Orange™ Pack ID**

Company Identifier

Service ID

Access ID

TX power (dbm)

✓ Valider
✕ Annuler

Wizard étape 8

Wizard Blue/NFC Mobile ID paramètres

### 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.**

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCF
- Création badges
- Outils

## Open Mobile Protocol

Wizard étape 8

Assistant SCB

### Options Blue/NFC Mobile ID

Affiche les paramètres de configuration

1 2 3 4 5 6 7 8 9

**Mode Blue** Open Mobile Protocol

**Désignation**

Nom de configuration (max 14 caractères) \*   STid Mobile ID (CSN)

Code site \*  ⓘ \*Champs obligatoires

**Modes d'identification et distances de communication**

Badge ⓘ  Contact  Mains-libres Jusqu'à ≈3m

Slide/Détection externe  Remote Jusqu'à ≈3m

Détection d'un événement externe via l'entrée lecteur

TapTap Jusqu'à ≈3m

Bouton télécommande actif  Remote 1  Remote 2

**Options lecteur**

Déverrouillage du smartphone requis par le lecteur

ⓘ Ajout de nouvelles valeurs NFC SAK/ATQA

Wizard Blue/NFC Mobile ID paramètres

Assistant SCB

### Blue/NFC Mobile ID

**OPENMOBILE**  
PROTOCOL

**Paramètres lecteur**

**Mode de lecture**

ID Privé

Depuis DESFire

ID privé sinon CSN

**Type de clé**

Une clé (RW)

Deux clés (R et W)

**Données**

Taille

Décalage

Inversé

**Open Mobile Protocol**

**Mode de communication**

ⓘ Communication sécurisée

Complete local name

Code site

Octets génériques

Puissance émise (dbm)

Identifiant Entreprise

## Compatibilité Blue/NFC Mobile ID et NFC-HCE

Si « STid Mobile ID® » ou « Open Mobile Protocol » est activé alors il n'est pas possible d'activer le NFC-HCE, les paramètres et clés sont grisés. C'est le NFC Mobile ID qui est automatiquement activé.

Assistant SCB ARC

Options Blue Mobile ID  
Affiche les paramètres de configuration

1 2 3 4 5 6 7 8

Mode Blue: STid Mobile ID

Désignation

Nom de configuration (max 14 caractères) \* myConfigName  STid Mobile ID (CSN)

Code site \* 65F8 ⓘ \*Champs obligatoires

OU

Assistant SCB ARC

Options Blue Mobile ID  
Affiche les paramètres de configuration

1 2 3 4 5 6 7 8

Mode Blue: Open Mobile Protocol

Désignation

Nom de configuration (max 14 caractères) \* myConfigName  STid Mobile ID (CSN)

Code site \* 65F8 ⓘ \*Champs obligatoires

Assistant de configuration SCB

Pour les modèles : Architect® , Architect® One, Architect® Blue et Architect® Secure  
Sélectionner votre type de SCB Paramètres complets

Lecteur Paramètres Clés

MIFARE DESFire Mode manuel Paramètres Clés

MIFARE Plus SL3 Mode manuel Paramètres Clés

MIFARE Classic/SL1 Mode manuel Paramètres Clés

MIFARE UltraLight/C Paramètres Clés

Blue/NFC Mobile ID Paramètres Clés

NFC-HCE Paramètres Clés

CPS3 Paramètres

125 kHz Paramètres

Fermer

Si « Orange™ Pack ID » est activé alors il est possible d'activer le NFC-HCE, les paramètres et clés sont dégrisés.

Assistant SCB ARC

Options Blue Mobile ID  
Affiche les paramètres de configuration

1 2 3 4 5 6 7 8

Mode Blue: Orange PackID

Désignation

Nom de configuration (max 14 caractères) \* myConfigName  STid Mobile ID (CSN)

Code site \* 65F8 ⓘ \*Champs obligatoires

Assistant de configuration SCB

Pour les modèles : Architect® , Architect® One, Architect® Blue et Architect® Secure  
Sélectionner votre type de SCB Paramètres complets

Lecteur Paramètres Clés

MIFARE DESFire Mode manuel Paramètres Clés

MIFARE Plus SL3 Mode manuel Paramètres Clés

MIFARE Classic/SL1 Mode manuel Paramètres Clés

MIFARE UltraLight/C Paramètres Clés

Blue/NFC Mobile ID Paramètres Clés

NFC-HCE Paramètres Clés

CPS3 Paramètres

125 kHz Paramètres

Fermer

## Compatibilité NFC Mobile ID et « ISO14443-3B PUPI / iClass »

Il est possible d'activer à la fois « NFC Mobile ID » et « ISO14443-3B PUPI », le « NFC Mobile ID » s'effectuant en ISO14443-A.

Assistant SCB ARC

Protocole de communication du lecteur  
Type de protocole et paramètres

1 2 3 4 5 6 7 8

Sécurité de l'ID privé

Chiffrement authentifié des données

Protocole ID

Sélectionner le protocole de votre choix

Clock&Data 40 bits - Iso 2B

Variante 2B

Décodage Décimal (BCD)

40 bits Données 13 caractères

Options du protocole

Taille 5 octet(s)

Code site forcé sur l'UID  2 octets Valeur AB

ISO14443-3B PUPI / iClass

Autorisé  MSB First



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges

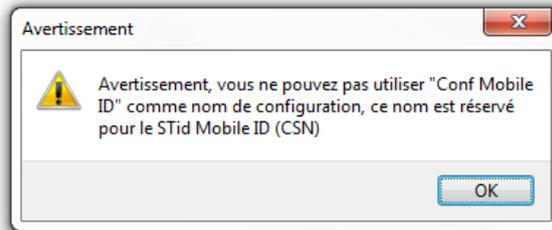


Outils

## 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.



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## 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/ Détection externe :



Slide : Fonctionne en effleurant le lecteur de la main sans présenter le téléphone au lecteur.



Détection externe : Fonctionne en changeant le niveau de l'entrée LED2. (voir plus bas)

- 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



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

#### ❖ Bouton télécommande actif

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

#### 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.

#### ❖ Détection d'un événement externe via l'entrée lecteur

L'information de présence main est donnée par le capteur capacitive ou le niveau d'entrée LED2 sur les ARCS.

Si active : l'information est donnée par le niveau de la LED2.

- LED2 non connectée ou connectée à un niveau haut = Main non présente
- LED2 connectée à la masse (GND) = Main présente.

Par exemple : connecter un système de détection à la LED2. Lorsque des personnes sont détectées, la lecture du smartphone est activée.

#### ❖ Déverrouillage du smartphone requis par le lecteur : 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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### ❖ Ajout de Nouvelles valeurs NFC SAK/ATQA

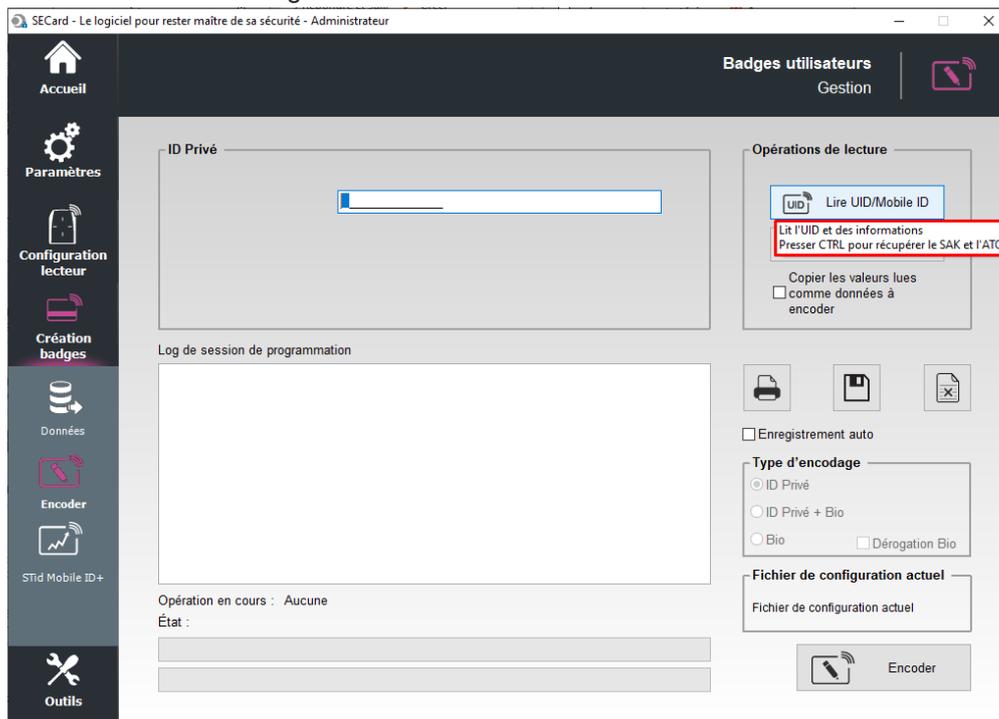
En RFID une puce est identifiée par deux paramètres ATQA et SAK. Ces paramètres doivent être connus des lecteurs pour que les identifiants soient lus.

Les smartphones en NFC répondent à cette même règle. Un certain nombre d'ATKA+SAK sont d'ores et déjà implémenté dans les lecteurs STid.

Pour assurer la compatibilité des lecteurs avec la lecture de nouveaux smartphones en mode NFC, ces champs permettent de renseigner jusqu'à trois valeurs de ATQA et SAK.

### Comment connaître ces valeurs pour votre smartphone:

- ❖ Activer le NFC du smartphone
- ❖ Aller dans Création badges



- ❖ Présenter le smartphone à l'encodeur SECard, en maintenant la touche CTRL + clic sur Lire UID

❖ Résultat **Current operation: SAK=20, ATQA=0004**

- ❖ Entrer cette valeur dans le champ :

**Options lecteur**

Déverrouillage du smartphone requis par le lecteur

Ajout de nouvelles valeurs NFC SAK/ATQA

### Remarques :

- L'activation du NFC-HCE pour "NFC Mobile ID" n'est pas une option dans SECard mais une option au niveau de l'application STid Mobile ID® (activé par défaut). Cette option n'est disponible que pour les smartphones Android.
- "NFC Mobile ID" n'est pas compatible avec l'application STid Settings.

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

Assistant SCB

### Code matriciel / code QR

Options et paramètres

1
2
3
4
5
6
7
8
9

#### Sélection du type de code matriciel

**Code 2D**

Data Matrix

Code QR

Aztec code

**Code 1D**

Code 39

Code 128

#### Eclairage ambiant

Mode Eco ?

Mode normal / Jour et nuit ?

Mode luminosité intense ?

**Paramètres avancés**

Luminosité du faisceau d'éclairage

Intense

Luminosité du faisceau cible

Haute

Sensibilité de détection

Normale

← Précédent
✓ Valider
✗ Annuler

❖ **Sélection du type de code matriciel**  
Sélectionner les types de code à lire.

Data Matrix	QR Code	Aztec code	Code 128	Code 39
123456	123456	123456	123456	123456



Home



Settings



Reader configuration



SCB / OCB



SKB



BCC



Create user cards



Tools

### ❖ Format du code matriciel

Sélectionner le format du code matriciel à lire.

La taille maximale du code dépend du format choisi :

Format	Taille en caractères	Octets
Hexadécimal	96	48
Décimal	25	10
ASCII	192	48

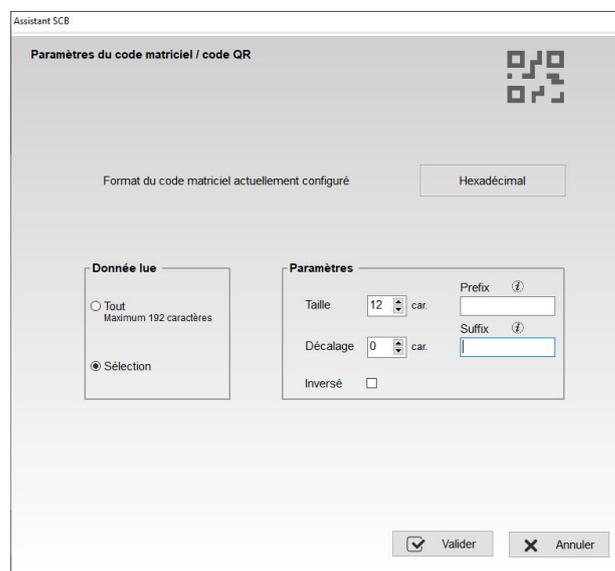
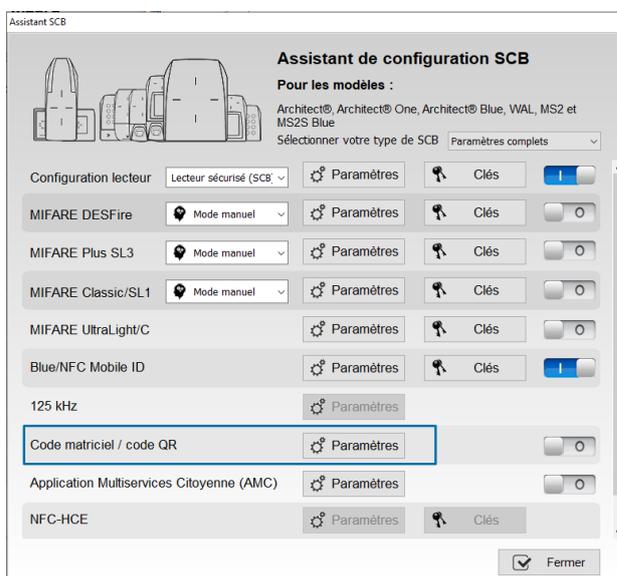
De 0 à 1208925819614629174706175  
0x0 à 0xFFFFFFFFFFFFFFFFFFFFFFFF

Remarque : seuls les caractères listés ci-dessous sont autorisés en ASCII :

Valeur	ASCII caractère	Valeur	ASCII caractère	Valeur	ASCII caractère
30	0	38	8	61	a
31	1	39	9	62	b
32	2	41	A	63	c
33	3	42	B	64	d
34	4	43	C	65	e
35	5	44	D	66	f
36	6	45	E		
37	7	46	F		

Remarque : si le code à lire n'est pas dans le type de code défini dans l'assistant, le code n'est pas lu. Par exemple, si le type décimal est défini et que le code à lire contient une lettre, le code ne sera pas lu.

Pour lire une partie spécifique du code, utiliser les paramètres Code matriciel :





Home



Settings



Reader configuration



SCB / OCB



SKB



BCC



SSCP



Create user cards



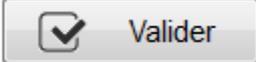
Tools

❖ Paramètres

- Mode Eco : Luminosité faible à modérée.
- Mode normal / Jour et nuit
- Mode luminosité intense : Luminosité très forte.

❖ Paramètres avancés

Luminosité du faisceau d'éclairage	Contrôle la puissance du spot qui éclaire le code	Normal		Intense
Luminosité du faisceau cible	Contrôle la puissance du laser qui cible le code	Basse	Normale	Haute
Sensibilité de détection	Contrôle la sensibilité du déclencheur pour commencer à scanner le code	Faible	Normal	Max

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

-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

### III. 2 - Assistant SCB : clés de sécurité lecteur

Assistant SCB

#### Clés de sécurité du Lecteur

Garder le contrôle de votre sécurité. Définir/modifier vos clés.

##### Clé entreprise SCB

Actuelle	<input type="checkbox"/> Nouvelle
<input type="text" value="FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"/>	<input type="text" value="00000000000000000000000000000000"/>

##### Clés de communication série

Signature	<input type="text" value="FFFFFFFFFFFFFFFF"/>	Chiffrement	<input type="text" value="FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"/>
<input type="checkbox"/> Nouvelle	<input type="text" value="FFFFFFFFFFFFFFFF"/>	<input type="checkbox"/> Nouvelle	<input type="text" value="FFFFFFFFFFFFFFFF"/>

##### Easy Secure ou clé AES de chiffrement du Wiegand

Actuelle	<input type="text" value="FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"/>
<input type="checkbox"/> Nouvelle	<input type="text" value="FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"/>

##### Protection configuration UHF ARC

Clé d'écriture	<input type="text" value="FFFFFFF"/>
<input type="checkbox"/> Nouvelle	<input type="text" value="FFFFFFF"/>

##### PUPI ISO14443-3B

<input type="checkbox"/> Signature	Clé	<input type="text" value="FFFFFFFFFFFFFFFF"/>
------------------------------------	-----	---

##### Chiffrement authentifié

Clé
<input type="text" value="FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"/>

Changer automatiquement la clé de communication (liaison série avec interface)

Valider      Annuler

#### 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

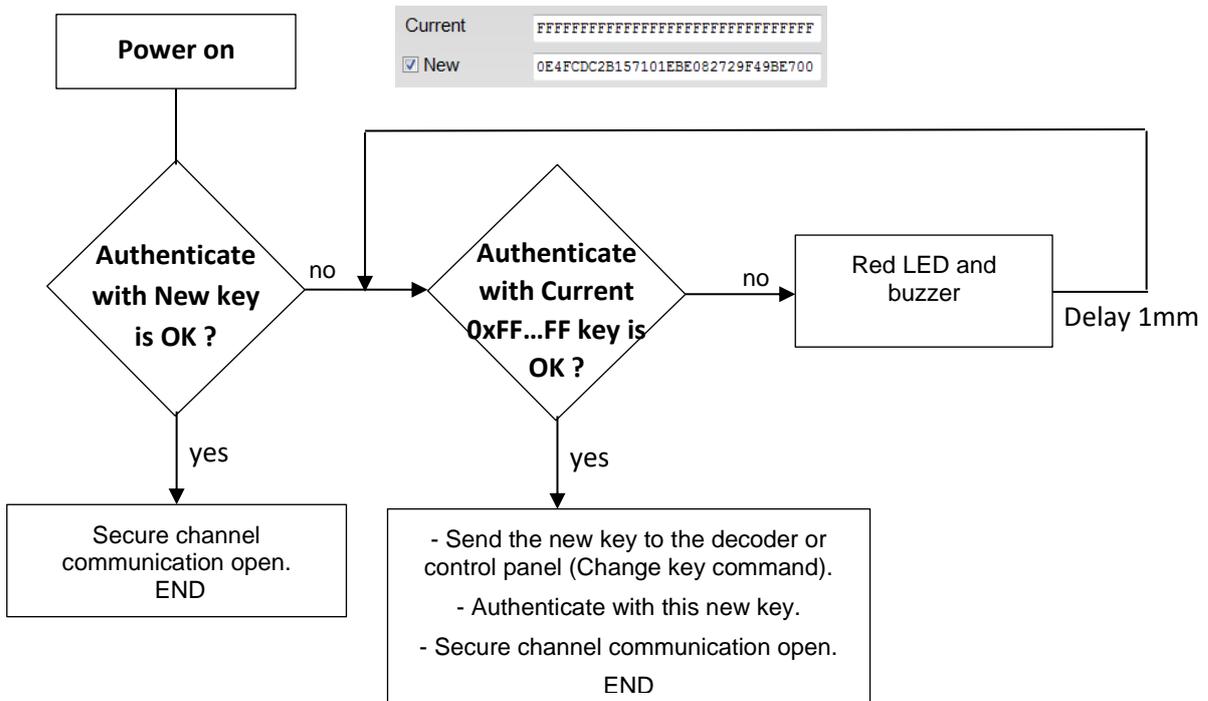
Permet de modifier la clé d'écriture de la configuration UHF si elle est activée. Il est recommandé de la modifier afin de protéger la configuration en écriture dans la puce.

### Chiffrement authentifié (AtE) :

Permet de renseigner la clé pour le chiffrement authentifié.

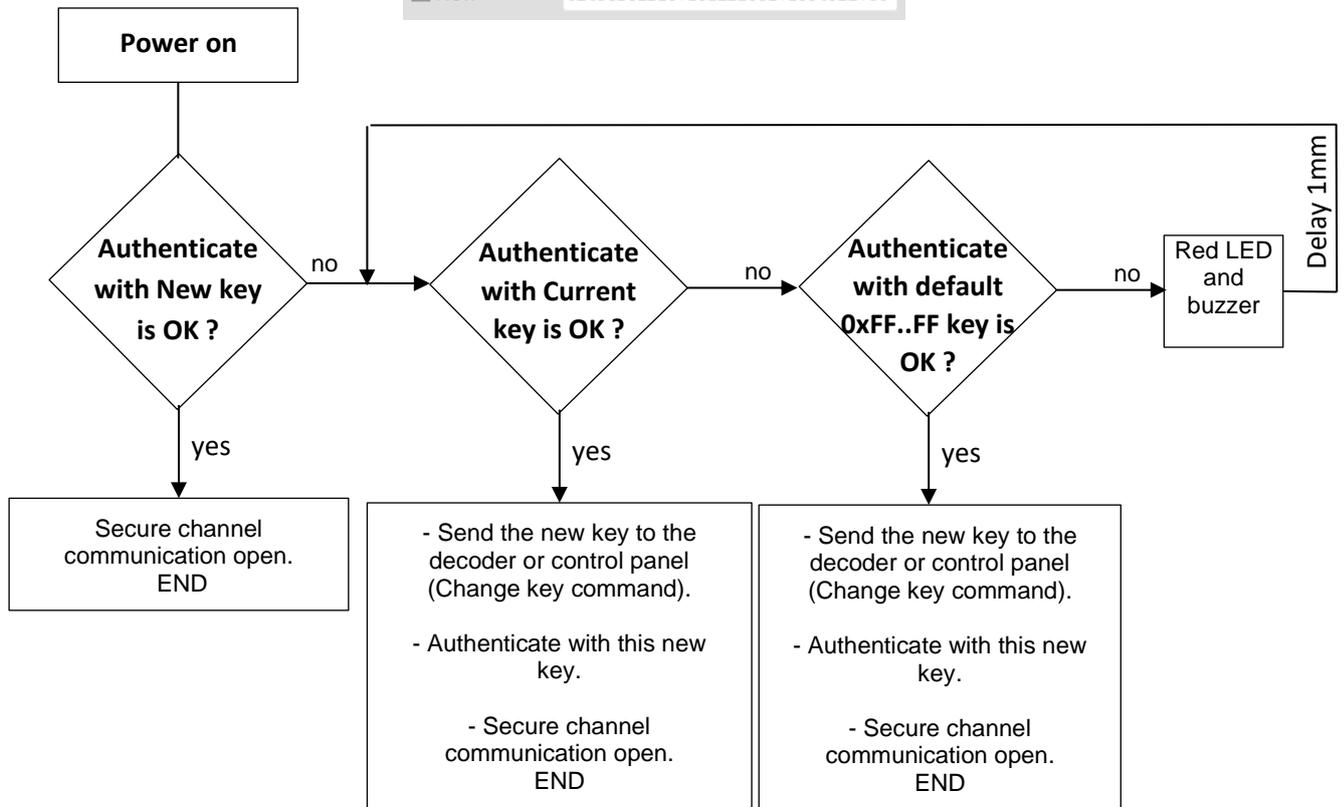
### Change automatiquement la clé de communication : **par défaut sélectionner cette option.**

- ❖ **Activée :**  
Dans SECard <v3.3.x cette option était automatiquement activée. La séquence d'authentification entre le lecteur et le décodeur ou le système est :
- ❖ **1er cas :** La clé courante du décodeur ou du système est la clé par défaut 0xFF...FF.



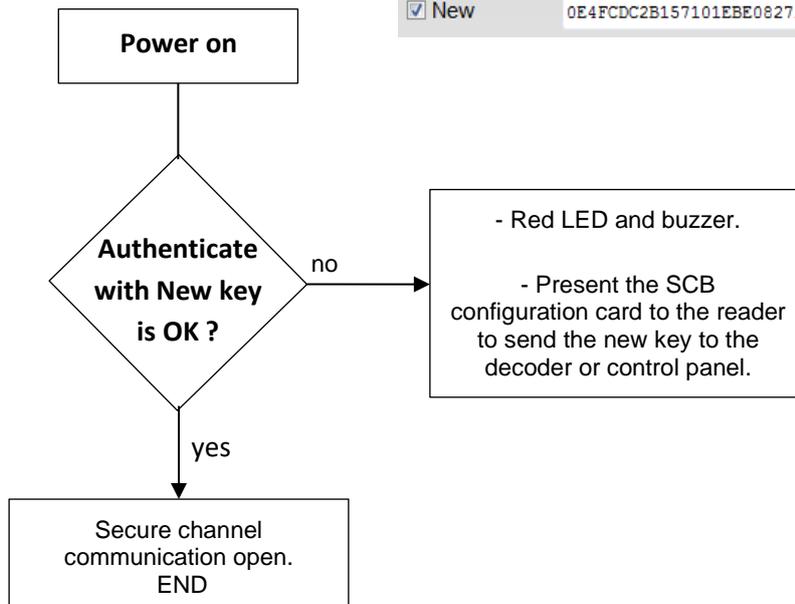
❖ 2<sup>nd</sup> cas : La clé courante du décodeur ou système est différente de la clé par défaut

Current	60827531F39811D39859B88E261E8AEB
<input checked="" type="checkbox"/> New	0E4FCDC2B157101EBE082729F49BE700



❖ Non Activée: la séquence d'authentification est :

Current	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
<input checked="" type="checkbox"/> New	0E4FCDC2B157101EBE082729F49BE700



Si Protocole PAC 64 sélectionné

-  Accueil
-  Paramètres
-  Configuration lecteur
-  SCB / OCB
-  SKB
-  BCC
-  SSCP
-  Création badges
-  Outils

Assistant SCB

### Clés de sécurité du Lecteur

Garder le contrôle de votre sécurité. Définir/modifier vos clés.

**Clé entreprise SCB**

Actuelle   Nouvelle

**Clés de communication série**

Signature  Chiffrement   Nouvelle

**Clé maître du PAC64**

Actuelle   Nouvelle

**Protection configuration UHF ARC**

Clé d'écriture   Nouvelle

**PUPI ISO14443-3B**

Signature Clé

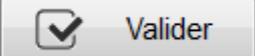
**Chiffrement authentifié**

Clé

Changer automatiquement la clé de communication (liaison série avec interface)

Valider  Annuler

**Clé maître du PAC64** : Permet de renseigner la clé pour le chiffrement du protocole PAC64.

Cliquer sur le bouton  pour terminer la configuration des clés.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



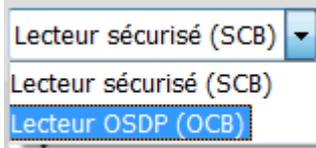
Création badges



Outils

### III. 3 - Assistant OCB : paramètres lecteurs

**Configuration lecteur :** Dans le menu déroulant choisir Lecteur OSDP(OCB).



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

	<a href="#">Cliquez-ici</a>	Assistant de configuration
	<a href="#">Cliquez-ici</a>	Sélection de la référence du lecteur à configurer
	<a href="#">Cliquez-ici</a>	Protocole et options
	<a href="#">Cliquez-ici</a>	LED et Buzzer
	<a href="#">Cliquez-ici</a>	Clavier et biométrie
	<a href="#">Cliquez-ici</a>	Ecran tactile
	<a href="#">Cliquez-ici</a>	Options Blue/NFC
	<a href="#">Cliquez-ici</a>	Code matriciel

## OCB – Etape 1

Assistant OCB

### Assistant de configuration

Créer votre carte de configuration lecteur OCB

1
2
3
4
5
6
7
8

Assistant de configuration pour lecteur OSDP™:

- Sélection lecteur
- Paramètres lecteur (protocoles et options)
- LED et Buzzer
- Claiver et biométrie
- Options écran tactile
- Options Bluetooth® / NFC

Les fonctionnalités disponibles de la carte de configuration OCB dépendent de la version du firmware du lecteur.  
Vous devez sélectionner la version correspondante à votre lecteur.

[Cliquer pour voir le tableau de compatibilité des firmwares](#)

**Sélectionner la version de SECard à utiliser**

SECard V3.5.x OCBv5

**Récupérer la configuration depuis l'assistant SCB**

[Cliquer pour voir les compatibilités ARC/ARCS, ARC1/ARC1S et WAL2](#)

Précédent
➔ Suivant
✕ Annuler

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

Pour assurer la compatibilité entre les différentes versions de OCB 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.*

		SECard			
		V3.3.x OCB v3	V3.4.x OCB v4	V3.5.x OCB v5	V3.6.x OCB v6
ARC-WAL Firmwares	Z05-06-07	x			
	Z08	x*	x		
	Z09-10	x*	x*	x	
	>=Z11	x*	x*	x*	x

x Entièrement compatible  
x\* Fonctions limitées pour assurer la rétro-compatibilité

**SECard et les compatibilités des versions firmwares lecteurs**

Le lecteur ARC1/ARC1S se configure comme un lecteur ARC/ARCS Blue hormis dans les cas d'usage suivants :

- si les options Biométrie, Clavier et/ou Écran tactile sont activées, elles ne seront pas prises en compte ;
- Pour le lecteur ARC1 Ph1, seule la puce sécurisée MIFARE Classic et les UID des autres puces seront pris en compte.

Les modes d'authentification Blue disponibles pour un ARC1S sont : Badge, Tap Tap, Remote et Mains-Libres.  
Les modes d'authentification Blue disponibles pour un ARCS Blue sont : Badge, Slide, Tap Tap, Remote et Mains-Libres.

Le lecteur WAL est configuré comme un lecteur ARC excepté dans les cas suivants :

- si les options Biométrie, Clavier et/ou Écran tactile sont activées, elles ne seront pas prises en compte ;
- si les fonctionnalités Bluetooth® sont activées, elle ne seront pas prise en compte.

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



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



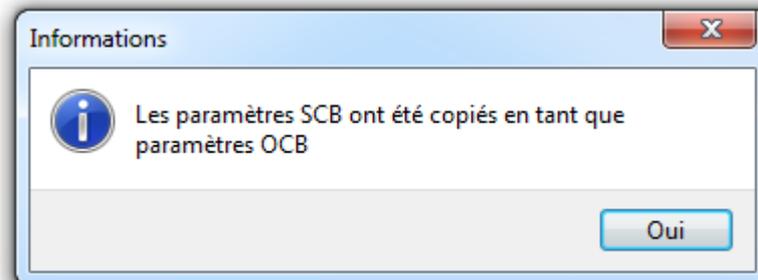
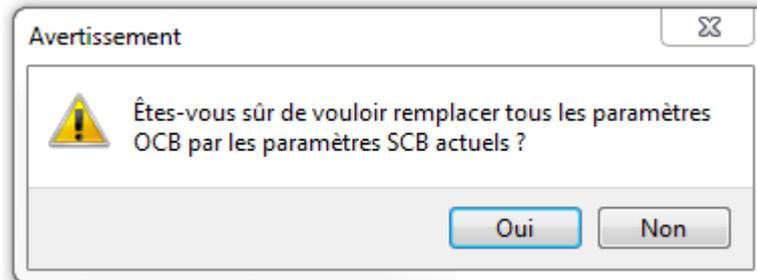
Outils



Récupérer la configuration  
depuis l'assistant SCB



Lorsque vous cliquez sur « Récupérer la configuration depuis l'assistant SCB », tous les paramètres de l'assistant de configuration OCB seront remplacés par les paramètres présents dans l'assistant de configuration SCB.



## OCB – Etape 2

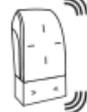
Assistant OCB

### Sélection de la référence du lecteur

Sélectionner le type de lecteur et les options à configurer

1 2 3 4 5 6 7 8

#### Activation des fonctions externes

					
<input type="checkbox"/> Clavier	<input type="checkbox"/> Ecran tactile	<input type="checkbox"/> Blue/NFC Mobile ID	<input type="checkbox"/> Biométrie	<input checked="" type="checkbox"/> Prox 125 kHz SE8	<input checked="" type="checkbox"/> Code matriciel / code QR

#### Options de protection du lecteur

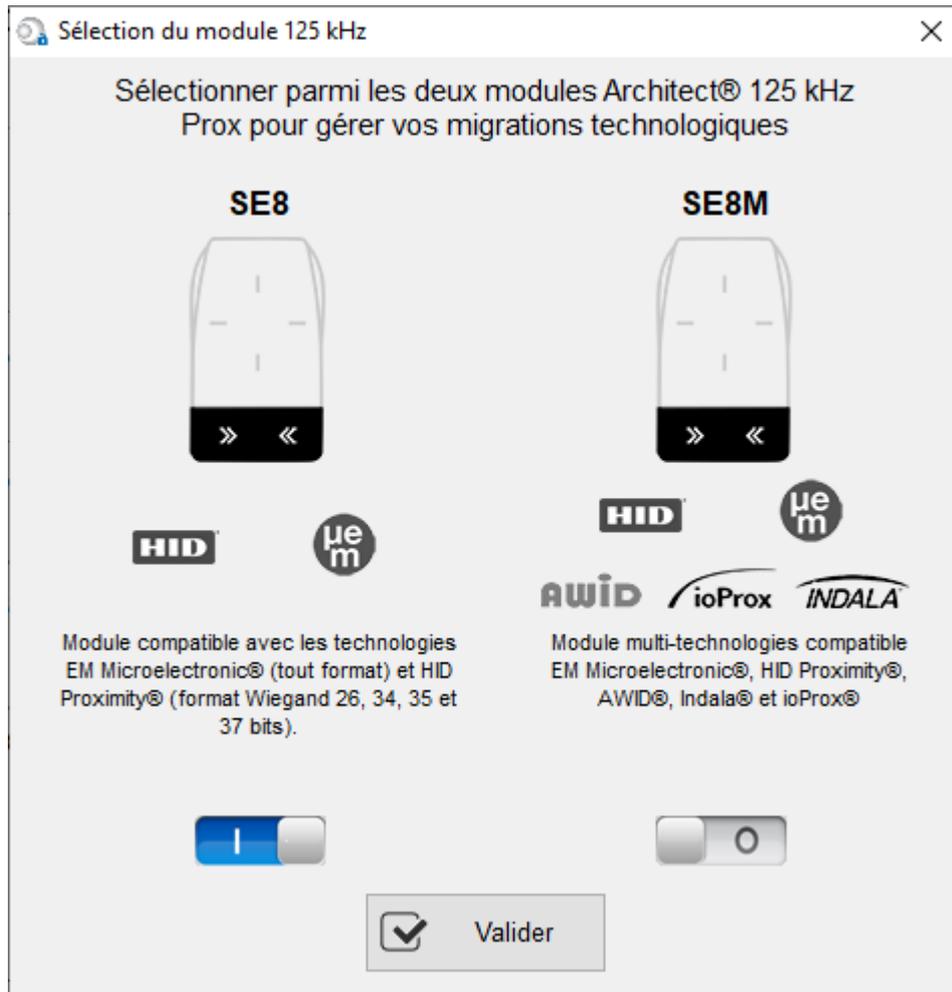
<input checked="" type="checkbox"/> Enregistrer les clés utilisateur en mémoire	<input checked="" type="checkbox"/> Signal d'arrachement
<input type="checkbox"/> Effacer les clés lors de l'arrachement	Sensibilité de l'accéléromètre
<input type="checkbox"/> LED rouge par défaut après arrachement	<input type="range" value="50"/> Normal

← Précédent    → Suivant    ✕ Annuler

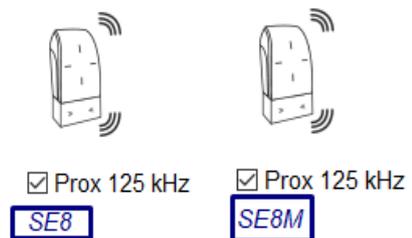
Activation fonctionnalités :

- ❖ D'activer la configuration clavier.
- ❖ D'activer la configuration écran tactile.
- ❖ D'activer la configuration Blue/NFC Mobile ID.
- ❖ D'activer la configuration biométrique.

- ❖ D'activer la configuration du module 125 kHz et de choisir le modèle du module à configurer (SE8 ou SE8M).



Ce choix impacte la fenêtre « Paramètres » du 125 kHz.



Le modèle choisi pour le module apparaît sur l'écran :

- ❖ D'activer la configuration du module code matriciel.



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## 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.
- ❖ Sensibilité de l'accéléromètre :  
Les lecteurs 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.

## OCB – Etape 3 *Ajout fonctionnalité 3.6*

Assistant OCB

### Paramètres lecteur

Options du protocole

1 2 **3** 4 5 6 7 8

#### Sécurité de l'ID privé

Chiffrement authentifié des données

#### Protocoles

##### Type

RAW  Wiegand

Utiliser la taille du protocole  Octet(s)

Rétrocompatibilité

Donnée justifiée à gauche  Donnée justifiée à droite

#### Options du protocole

Code cité forcé sur l'UID

2 octets Valeur

Autoriser le mode en clair après une authentification sur le canal sécurisé

Utiliser l'ACK à la place de la commande Busy

Décalage  bit(s)

Change l'adresse RS485

Baudrate

Wrap texte désactivé  Ancien IEEE

Préfixe   Suffixe

ID-Len  ID-Tag *Valeurs*

#### Intervalle de filtrage ID (LSB)

Intervalle UID/ID  à

#### ISO14443-3B PUP1 / iClass

Autorisé

← Précédent

→ Suivant

✕ Annuler

### ❖ Sécurité de l'ID privé

Les identifiants privés peuvent être chiffrés ET signés avant d'être écrits dans le badge. Le lecteur déchiffre et authentifie 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.

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

## ❖ Protocoles

**[REPLY]: osdp\_RAW – 50h**

SOM	ADDR	LEN	CTRL	REPLY	DATA				CRC / CKSUM	
53h	Physical Reader Address [80h...FEh]	XXh XXh: CKSUM XXh XXh: CRC	XXh	50h: osdp_RAW	Reader number	Format code	Count LSB    MSB		Data	XXh / XXh XXh

**Reader number:** 00h First reader  
1 byte 01h Second reader....

**Format code:** 00h not specified, raw bit array  
1 byte 01h P/data/P (Wiegand)

**Count:** 2-byte size (in bits) of the data at the end of the record  
2 bytes

**Data:** MSB to LSB (left justified)  
n bytes

### Type RAW

- Type Raw + Rétro-compatibilité : “Format code” est fixé à 01h.
- Type Raw: “Format code est fixé à 00h.

Utiliser la taille du protocole : Permet de fixer la taille des données envoyées par le lecteur à la commande OSDP \_RAW (UID et Private ID).

### Type Wiegand

- “Format code” est fixé à 01h.
- 3 protocoles Wiegand sont disponible: Wiegand 26bits, 35 bits et 37 bits.

Pour 13,56 MHz, BLE / NFC et Private ID 125 kHz, possibilité de formater les données envoyées dans osdp\_RAW en conservant les données MSB ou LSB, en ajoutant un remplissage à zéro à gauche ou à droite (justifié à gauche ou justifié à droite) et en ajoutant des bits de parité sur les données lues.

Pour l'UID 125 kHz, le lecteur calcule et ajoute obligatoirement les bits de parité avec la configuration Garder LSB / Ajouter bit de parité / justifié à gauche. Les options définies dans SECard ne sont pas prises en compte.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## Options du protocole

- ❖ « 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.
- ❖ Autoriser le mode clair après une authentification sur le canal sécurisé.
  - ❖ Désactivée : après une commande `osdp_keyset` avec une clé différente de la clé par défaut SCBKD, il est obligatoire de communiquer en Secure Channel.
  - ❖ Activée : après une commande `osdp_keyset` avec une clé différente de la clé par défaut SCBKD, il est possible de communiquer en mode clair même après une authentification réussie.

### ❖ Utiliser ACK à la place de Busy

Cocher cette option si le système ne prend pas en compte la réponse `osdp_busy`.

- ❖ Désactivée : la réponse sera `osdp_busy`.
- ❖ Activée : la réponse sera `osdp_ACK`.

Corresponds à la commande Manufacturer:

SOM	ADDR	LEN	CTRL	CMD	DATA	CKSUM / CRC
53h	Physical Reader Address [00h...7Eh]	0Dh 00h: CKSUM 0Ch 00h: CRC	XXh	80h: osdp_MFG	F5h1Bh C0h 05h DATA	XXh / XXh XXh

**DATA:** 00h reply is osdp\_BUSY  
1 byte 01h reply is osdp\_ACK

### ❖ Décalage

Permet de fixer le premier bit d'ID envoyé par le lecteur à la commande OSDP\_RAW (UID et Private ID). Réglable de 0 à 255 bits.

Ex : si le décalage est 6 et la donnée est 0x123456 (hexa), 0b0001 0010 0011 0100 0101 0110 (binaire)

La donnée avec le décalage sera 0b10 0011 0100 0101 0110 (binaire), 0x023456 (hexa)

### ❖ Change l'adresse RS485 / Baudrate:

Permet de définir l'adresse RS485 et la Vitesse de communication du lecteur, par badge de configuration OCB sans avoir à utiliser la commande `osdp_COMSET`.

### ❖ Wrap texte désactivé : lié à la commande OSDP\_TEXT

- Désactivée : si la commande OSDP\_TEXT est utilisée pour afficher plus de 1 ligne de texte ou 1 ligne de texte qui ne tient pas sur 1 seule ligne de texte, le lecteur effacera tout l'écran et affichera le texte correspondant.

- Activée : si la commande OSDP\_TEXT est utilisée pour afficher plus de 1 ligne de texte ou 1 ligne de texte qui ne tient pas sur 1 seule ligne de texte le lecteur coupera le texte au-delà de la première ligne ; le lecteur n'affichera que la première ligne et n'effacera pas tout l'écran.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### Nouveauté 3.6

#### ❖ Ancien IEEE :

Pour les lecteurs en version firmware < Z11 : IEEE= 0xF51BC0

Pour les lecteurs en version firmware ≥ Z11 : IEEE= 0x2C17E0

Ancien IEEE      IEEE= 0xF51BC0

Ancien IEEE      IEEE= 0x2C17E0

Remarque : A la suite d'une mise à jour d'un lecteur en firmware ≥ Z11, celui-ci bascule automatiquement avec le nouveau numéro IEEE (0x2C17E0).

En mode Raw, il est possible de personnaliser la donnée avant transmission avec les informations suivantes :

<Prefix><ID-Tag><ID-Len><ID-Number><Suffix>

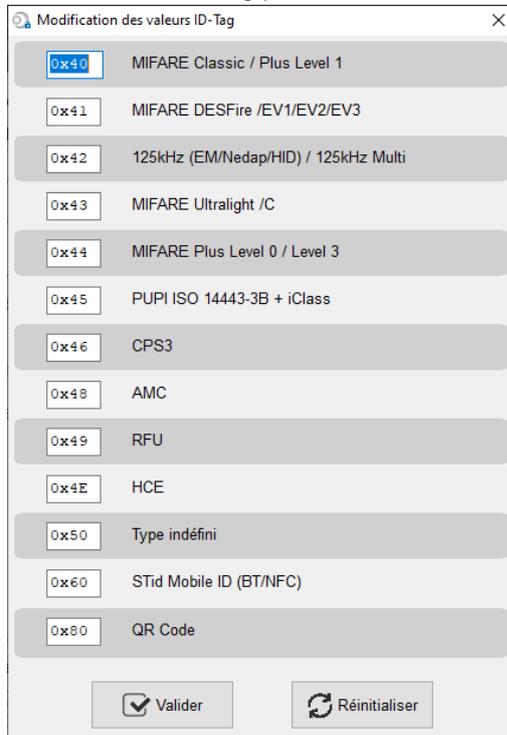
- ❖ *Prefix* : ajoute un préfixe avant d'envoyer la trame. Valeur hexadécimale sur maximum 5 octets.
- ❖ *Suffix* : ajoute un suffixe avant d'envoyer la trame. Valeur hexadécimale sur maximum 5 octets.

#### ❖ ID-Tag :

Un octet qui identifie le type de « tag » lu et sera ajouté à la trame.

L'ID-Tag sera ajouté à un UID ou à un ID privé.

Les valeurs d'ID-Tag peuvent être modifiées dans le tableau ci-dessous :



ID-Tag	Type
0x40	MIFARE Classic / Plus Level 1
0x41	MIFARE DESFire /EV1/EV2/EV3
0x42	125kHz (EM/Nedap/HID) / 125kHz Multi
0x43	MIFARE Ultralight /C
0x44	MIFARE Plus Level 0 / Level 3
0x45	PUPI ISO 14443-3B + iClass
0x46	CPS3
0x48	AMC
0x49	RFU
0x4E	HCE
0x50	Type indéfini
0x60	STid Mobile ID (BT/NFC)
0x80	QR Code

Le bouton Reset restaure les valeurs STid par défaut.

- ❖ *ID-Len* : 2 octets indiquant la longueur de ID-Number
  - Pour une donnée en Hexadécimal : ID-Len = nombre d'octets de l'ID-Number
  - Pour une donnée en décimal : ID-Len = nombre de caractères de l'ID-Number



### Exemple 1 : Paramétrages :

Tag : DESFire  
 ID-Number = 0000ABCDEF  
 ID-Len = 5

OSDP Data:123454100050000ABCDEF5678

Prefix	ID-Tag	ID-Len	ID-Number	Suffix
1234	41	0005	0000ABCDEF	5678

OSDP bit count = 96 (16<sub>prefix</sub> + 8<sub>tag</sub> + 16<sub>len</sub> + 40<sub>id</sub> + 16<sub>suffix</sub>)

### Exemple 2:

Tag : ioPROX  
 ID-binary = 100 1110 0000 0101 0001 0101 1001 1011 1011 1100  
 ID-Len = 39 bits

ID Justifié à gauche : 100 1110 0000 0101 0001 0101 1001 1011 1011 1100 0 = 0x 9C0A2B3778

OSDP Data: 0x 42 9C0A2B3778

OSDP bit count = 47 (8<sub>tag</sub> + 39<sub>len</sub>)

ID Justifié à droite : 0 100 1110 0000 0101 0001 0101 1001 1011 1011 1100 = 0x 4E05159BBC

OSDP Data: 0x42 4E05159BBC

OSDP bit count = 47 (8<sub>tag</sub> + 39<sub>len</sub>)



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## ❖ 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  $\leq$  UID/ID  $\leq$  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.

## OCB – Etape 4

Assistant OCB

**LED et Buzzer**  
Options et paramètres

1 2 3 4 5 6 7 8

**Etat par défaut de la LED**

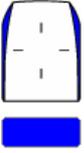
Mode

Off

Fixe

Clignotement

Couleur



Durée clignotement ON x100ms

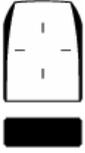
2

Durée clignotement OFF x100ms

2

**Action détection carte**

Couleur



Nb cycle LED

0

Durée LED ON x100ms

4

Durée LED OFF x100ms

0

Nb cycle buzzer

0

Durée buzzer ON x100ms

4

Durée buzzer OFF x100ms

0

LED à la connexion Bluetooth®

**Niveau sonore du Buzzer**

 Fort

← Précédent    → Suivant    X Annuler

### Etat par défaut de la LED

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

- ❖ Off
- ❖ Fixe
- ❖ Clignotement classique

L'image de droite permet de visualiser l'effet sélectionné : clignotement et couleur.  
Cet état peut-être modifier avec la commande `osdp_LED` et les paramètres permanents.

### Action détection carte

- ❖ Permet de définir l'état (couleur & clignotement) de la LED et du buzzer lorsqu'un identifiant valide est détecté.  
Cette information est indépendante de l'acceptation de l'identifiant.
- ❖ 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.

### Niveau sonore du buzzer

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

-  Accueil
-  Paramètres
-  Configuration lecteur
-  SCB / OCB
-  SKB
-  BCC
-  SSCP
-  Création badges
-  Outils

Assistant OCB

**Clavier et biométrie**

Options et paramètres

1
2
3
4
5
6
7
8

**Paramètres du lecteur biométrique**

<p>Niveau de sécurité</p> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">1</div>	<p>Nombre de doigts à enrôler</p> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">1</div>
<p>Seuil</p> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">5</div>	<p>Nombre de doigts à vérifier</p> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">1</div>

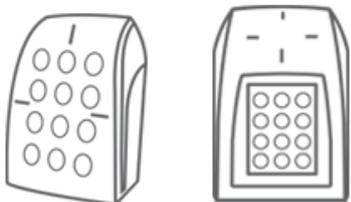


Consolidation de la capture des minuties

Détection faux doigt Désactivée

**Options clavier**

<p><b>Appui touche</b></p> <p><input checked="" type="checkbox"/> Buzzer</p> <p><input type="checkbox"/> Scintillement</p>	<p><b>Affichage</b></p> <p><input checked="" type="radio"/> Clavier</p> <p><input type="radio"/> Image par défaut</p>
<p><input checked="" type="checkbox"/> Rétroéclairage</p> <p style="margin-left: 20px;"><input checked="" type="radio"/> Permanent light</p> <p style="margin-left: 20px;"><input type="radio"/> Custom light duration</p>	<p><input type="checkbox"/> Scramble Pad</p> <p style="text-align: right; margin-right: 20px;"> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">6</div> s                 </p>



← Précédent
→ Suivant
✕ Annuler

### 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 entraîne 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.
- ❖ Détection faux doigts : Active / Désactive la détection de faux de doigt avec un niveau de détection.

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

## Options clavier

- ❖ Appui touche : Permet d'activer / désactiver 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 :
  - 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. Deux options sont disponibles

Eclairage permanent : Rétroéclairage permanent du clavier.

Durée d'éclairage : Rétroéclairage du clavier lors d'un appui touche et pendant un temps configurable

Scintillement : en fonction du mode rétroéclairage choisi, permet de faire flasher ON ou OFF les LEDS du rétroéclairage du clavier lorsqu'un utilisateur appuie sur une touche du clavier.

<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p><b>Appui touche</b></p> <p><input checked="" type="checkbox"/> Buzzer</p> <p><input type="checkbox"/> Scintillement</p> </div> <p><input type="checkbox"/> Rétroéclairage</p> <p>Pas de rétroéclairage Pas de flash du rétroéclairage sur appui touche</p>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p><b>Appui touche</b></p> <p><input checked="" type="checkbox"/> Buzzer</p> <p><input type="checkbox"/> Scintillement</p> </div> <p><input checked="" type="checkbox"/> Rétroéclairage</p> <p><input type="radio"/> Permanent light</p> <p><input type="radio"/> Custom light duration <input type="text" value="6"/> s</p> <p><input type="checkbox"/> Scramble Pad</p> <p>Rétroéclairage activé Pas de flash du rétroéclairage sur appui</p>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p><b>Appui touche</b></p> <p><input checked="" type="checkbox"/> Buzzer</p> <p><input checked="" type="checkbox"/> Scintillement</p> </div> <p><input type="checkbox"/> Rétroéclairage</p> <p>Pas de rétroéclairage Flash court ON du rétroéclairage sur appui</p>
<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p><b>Appui touche</b></p> <p><input checked="" type="checkbox"/> Buzzer</p> <p><input checked="" type="checkbox"/> Scintillement</p> </div> <p><input checked="" type="checkbox"/> Rétroéclairage</p> <p><input checked="" type="radio"/> Permanent light</p> <p>Rétroéclairage activé Flash court OFF du rétroéclairage sur appui</p>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p><b>Appui touche</b></p> <p><input checked="" type="checkbox"/> Buzzer</p> <p><input type="checkbox"/> Scintillement</p> </div> <p><input checked="" type="checkbox"/> Rétroéclairage</p> <p><input type="radio"/> Permanent light</p> <p><input checked="" type="radio"/> Custom light duration <input type="text" value="6"/> s</p> <p><input type="checkbox"/> Scramb</p> <p>Rétroéclairage OFF et passe ON sur appui touche pendant un temps configurable puis revient OFF</p>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p><b>Affichage</b></p> <p><input checked="" type="radio"/> Clavier</p> <p><input type="radio"/> Image p:</p> </div>



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## OCB – Etape 6

Assistant OCB

### Options écran tactile

Affiche les paramètres de configuration

1 2 3 4 5 6 7 8

#### Langue du lecteur

English

**Rotation 180°** Sélectionner l'index de vos textes et images

0

#### Textes

Couleur

Ligne 1 Présentez votre

Ligne 2 identifiant

Ligne 3

#### Images

Charger

Effacer

Ajuster

Port COM1

Baudrate 38400

Charger vos images dans le lecteur  
(Exclusivement par liaison série)



← Précédent

→ Suivant

✕ Annuler

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

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

**Index** : sélectionner le numéro de l'Index [0 ; 9] où seront chargés l'image et le texte sélectionné.

#### Textes

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



La couleur s'applique aux trois lignes de textes.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## Image

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

<p>Charger</p> 	Permet de charger un fichier image pour l'état sélectionné.
<p>Effacer</p> 	Permet de supprimer le fichier image de l'état sélectionné.
<p>Ajuster</p> 	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 :

#### Attention

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

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

Port :   
 Baudrate :



2 - Mettre le lecteur sous tension et cliquer sur le bouton

3 - L'avancement du chargement est indiqué par la barre de progression.

### Remarque :

- \* L'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 :





Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## OCB – Etape 7

Assistant OCB

### Options Blue/NFC Mobile ID

Paramètres et options de lecture

1
2
3
4
5
6
7
8

**Blue mode** STid Mobile ID

**Désignation**

Nom de la configuration (max 14 caractères) \* myConfigName  STid Mobile ID (CSN)

Code site \* 12AB \* Champs obligatoires

**Modes d'identification et distances de communication**

Badge

Contact



Mains-libres

Jusqu'à ≈3m



Slide / Détection externe

Très proche



Détection d'un événement externe via l'entrée du lecteur

Remote

Jusqu'à ≈3m



Bouton télécommande actif

Remote 1  Remote 2

TapTap

Jusqu'à ≈3m



**Options lecteur**

Déverrouillage du smartphone requis par le lecteur

Ajout de nouvelles valeurs NFC SAK/ATQA

000000
000000
000000

← Précédent
→ Suivant
✕ Annuler

### Mode Blue/NFC

Permet de configurer le lecteur Bluetooth® pour fonctionner avec l'application STid Mobile ID® ou Orange™ Pack ID ou Open Mobile Protocol.

Ce choix a un impact sur les écrans de l'assistant de configuration Etape 5 et Blue/NFC Mobile ID Paramètres.

### 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.

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

STid Mobile ID®

Wizard Step 5

Assistant OCB

### Options Blue/NFC Mobile ID

Paramètres et options de lecture 1 2 3 4 5 6 7 8

**Blue mode** STid Mobile ID

**Désignation**

Nom de la configuration (max 14 caractères) \* myConfigName  STid Mobile ID (CSN)

Code site \* 12AB \* Champs obligatoires

**Modes d'identification et distances de communication**

Badge Contact  Mains-libres Jusqu'à ~3m

Slide / Détection externe Très proche  Remote Jusqu'à ~3m

TapTap Jusqu'à ~3m Bouton télécommande actif

Remote 1  Remote 2

**Options lecteur**

Déverrouillage du smartphone requis par le lecteur  Ajout de nouvelles valeurs NFC SAK/ATQA

000000 000000 000000

← Précédent
→ Suivant
✕ Annuler

Wizard Blue/NFC Mobile ID settings

Assistant OCB

### Blue/NFC Mobile ID

**Paramètres lecteur**

**Mode de lecture**

ID Privé

Depuis DESFire

ID privé sinon CSN

**Type de clé**

Une clé (RW)

Deux clés (R et W)

**Données**

Taille 5

Décalage 0

Inversé

**Paramètres du badge d'accès virtuel**

Nom du badge d'accès virtuel (max 14 caractères)\*

myVCardName

Aperçu du badge

ID  Remote 1

Code site  Remote 2

Nom de la configuration  Déverrouillage requis

Interdire la suppression  Déverrouillage Bio

Valider
✕ Annuler

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

Wizard étape 5

### Orange PackID

Assistant OCB

**Options Blue/NFC Mobile ID**  
 Paramètres et options de lecture
 1 2 3 4 5 6 7 8

**Blue mode** Orange Pack ID

**Désignation**

Nom de la configuration (max 14 caractères) \* myConfigName  STid Mobile ID (CSN)

Code site \* 12AB \* Champs obligatoires

**Modes d'identification et distances de communication**

Badge

Contact

Slide / Détection externe

Très proche

TapTap

Jusqu'à ≈3m

Mains-libres

Jusqu'à ≈3m

Remote

Jusqu'à ≈3m

Détection d'un événement externe via l'entrée du lecteur

**Bouton télécommande actif**

Remote 1  Remote 2

**Options lecteur**

Déverrouillage du smartphone requis par le lecteur

Ajout de nouvelles valeurs NFC SAK/ATQA

000000 000000 000000

← Précédent
→ Suivant
✕ Annuler

Le mode de détection pour cette application est fixé au contact

Wizard Blue/NFC Mobile ID paramètres

Assistant OCB

**Blue/NFC Mobile ID**

**Paramètres lecteur**

**Mode de lecture**

ID Privé

Depuis DESFire

ID privé sinon CSN

**Type de clé**

Une clé (RW)

Deux clés (R et W)

**Données**

Taille 5

Décalage 0

Inversé

**Paramètres Orange™ Pack ID**

Company Identifier 0543

Service ID 00000001

Access ID 0F0F0F0F0F0F

TX power (dbm) -8

✓ Valider
✕ Annuler

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

## Open Mobile Protocol

Wizard étape 5

Assistant OCB

### Options Blue/NFC Mobile ID

Paramètres et options de lecture

1 2 3 4 5 6 7 8

**Blue mode** Open Mobile Protocol

**Désignation**

Nom de la configuration (max 14 caractères) \* myConfigName  STid Mobile ID (CSN)

Code site \* 12AB \* Champs obligatoires

**Modes d'identification et distances de communication**

Badge  Mains-libres

Contact Jusqu'à ≈3m

Slide / Détection externe

Remote Jusqu'à ≈3m

Très proche

Détection d'un événement externe via l'entrée du lecteur

TapTap Jusqu'à ≈3m

Bouton télécommande actif

Remote 1  Remote 2

**Options lecteur**

Déverrouillage du smartphone requis par le lecteur

Ajout de nouvelles valeurs NFC SAK/ATQA

000000 000000 000000

← Précédent    Suivant →    X Annuler

Wizard Blue/NFC Mobile ID paramètres

Assistant OCB

**Blue/NFC Mobile ID**

**Paramètres lecteur**

**Mode de lecture**

ID Privé

Depuis DESFire

ID privé sinon CSN

**Type de clé**

Une clé (RW)

Deux clés (R et W)

**Données**

Taille 5

Décalage 0

Inversé

**Open Mobile Protocol**

**Mode de communication**

Communication sécurisée

Complete local name ARCoa

Code site 51BC

Octets génériques 000000

Puissance émise (dbm) 4

Identifiant Entreprise 51BC

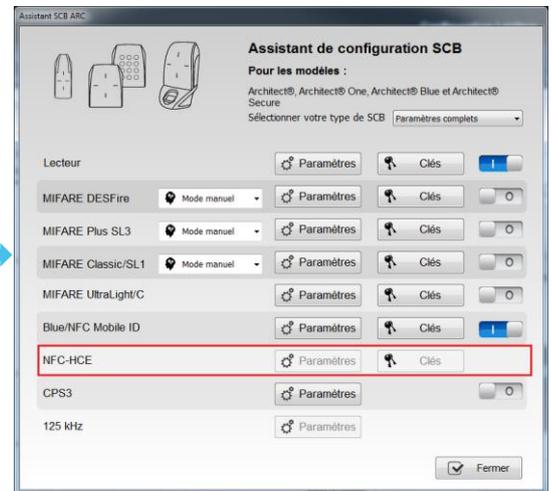
Valider     Annuler

## Compatibilité Blue/NFC Mobile ID et NFC-HCE

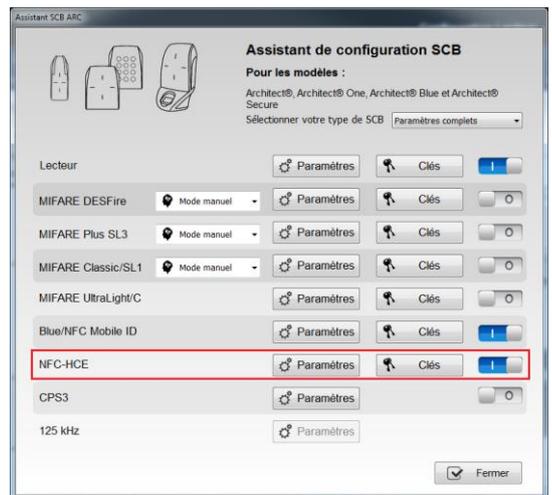
Si « STid Mobile ID® » ou « Open Mobile Protocol » est activé alors il n'est pas possible d'activer le NFC-HCE, les paramètres et clés sont grisés. C'est le NFC Mobile ID qui est automatiquement activé.



OU

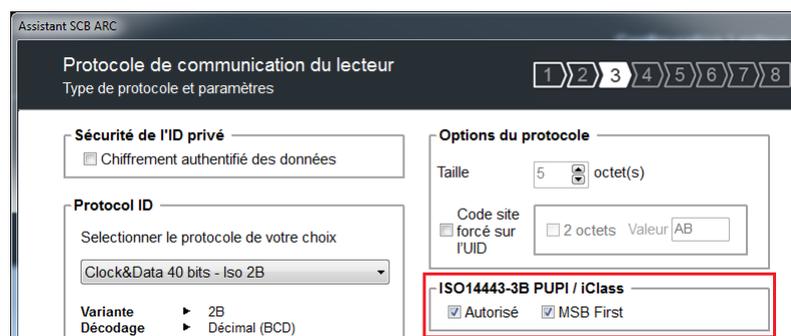


Si « Orange™ Pack ID » est activé alors il est possible d'activer le NFC-HCE, les paramètres et clés sont dégrisés.



## Compatibilité NFC Mobile ID et « ISO14443-3B PUPI / iClass »

Il est possible d'activer à la fois « NFC Mobile ID » et « ISO14443-3B PUPI », le « NFC Mobile ID » s'effectuant en ISO14443-A.





Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges

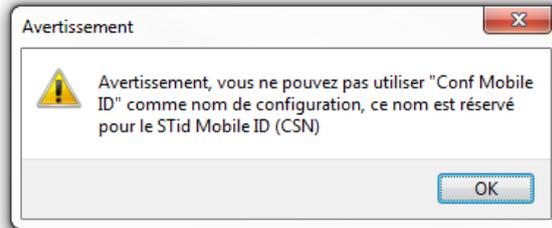


Outils

## 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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## 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/ Détection externe :**
  - Slide : Fonctionne en effleurant le lecteur de la main sans présenter le téléphone au lecteur.
  - Détection externe : Fonctionne en changeant le niveau de l'entrée LED2. (voir plus bas)
    - 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
- ❖ **Bouton télécommande actif**

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

### 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**



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

**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.

**Remarques :**

- L'activation du NFC-HCE pour "NFC Mobile ID" n'est pas une option dans SECard mais une option au niveau de l'application STid Mobile ID® (activé par défaut). Cette option n'est disponible que pour les smartphones Android.
- "NFC Mobile ID" n'est pas compatible avec l'application STid Settings.

❖ **Détection d'un événement externe via l'entrée du lecteur :**

L'information de présence main est donnée par le capteur capacitive ou le niveau d'entrée LED2 sur les ARCS.

Si active : l'information est donnée par le niveau de la LED2.

- LED2 non connectée ou connectée à un niveau haut = Main non présente
- LED2 connectée à la masse (GND) = Main présente.

Par exemple : connecter un système de détection à la LED2. Lorsque des personnes sont détectées, la lecture du smartphone est activée.

❖ **Déverrouillage du smartphone requis par le lecteur : 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.

### ❖ Ajout de Nouvelles valeurs NFC SAK/ATQA

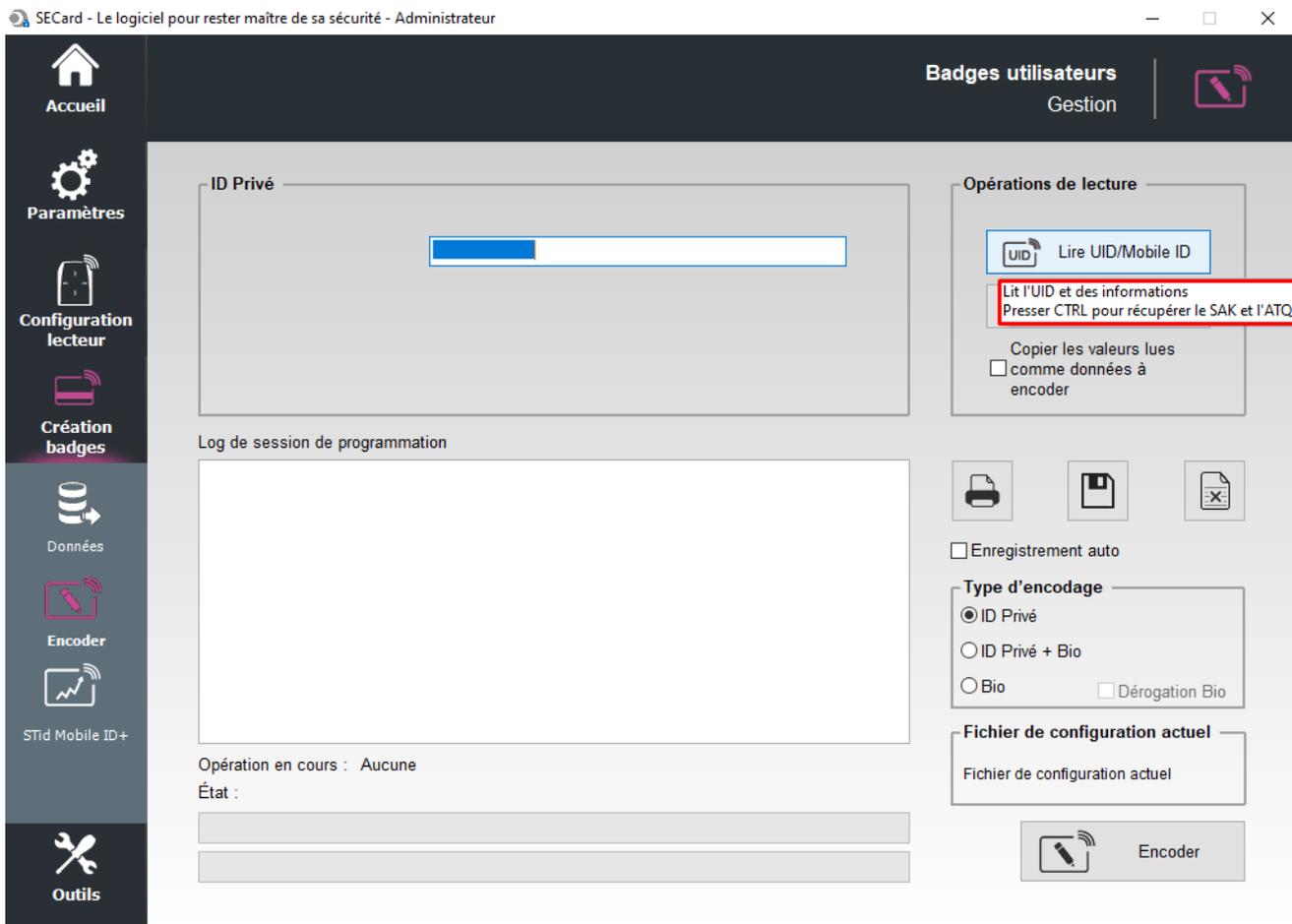
En RFID une puce est identifiée par deux paramètres ATQA et SAK. Ces paramètres doivent être connus des lecteurs pour que les identifiants soient lus.

Les smartphones en NFC répondent à cette même règle. Un certain nombre d'ATKA+SAK sont d'ores et déjà implémenté dans les lecteurs STid.

Pour assurer la compatibilité des lecteurs avec la lecture de nouveaux smartphones en mode NFC, ces champs permettent de renseigner jusqu'à trois valeurs de ATQA et SAK.

### Comment connaître ces valeurs pour votre smartphone :

- ❖ Activer le NFC du smartphone
- ❖ Aller dans Création badges



- ❖ Présenter le smartphone à l'encodeur SECard, en maintenant la touche CTRL + clic sur Lire UID

❖ Résultat **Current operation: SAK=20, ATQA=0004**

- ❖ Entrer cette valeur dans le champ :

**Options lecteur**

Déverrouillage du smartphone requis par le lecteur

Ajout de nouvelles valeurs NFC SAK/ATQA

200400

## OCB – Etape 8 *Ajout fonctionnalité 3.6*

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

Assistant OCB

### Code matriciel / code QR

Paramètres et options lecteur

1 2 3 4 5 6 7 8

#### Sélection des types de code matriciel

**Code 2D**

- Data Matrix
- Code QR
- Aztec code

**Code 1D**

- Code 39
- Code 128

#### Eclairage ambiant

- Mode Eco ?
- Mode normal / Jour et nuit ?
- Mode luminosité intense ?

**Paramètres avancés**

Luminosité du faisceau d'éclairage

Intense

Luminosité du faisceau cible

Haute

Sensibilité de détection

Normale

#### Format du code matriciel

- Hexadécimal
- Décimal
- ASCII
- Brut

← Précédent ✓ Valider ✗ Annuler

### ❖ Sélection du type de code matriciel

Sélectionner les types de code à lire.

Data Matrix	QR Code	Aztec code	Code 128	Code 39
123456	123456	123456		



Home



Settings



Reader configuration



SCB / OCB



SKB



BCC



SSCP



Create user cards



Tools

### ❖ Format du code matriciel

Sélectionner le format du code matriciel à lire.

La taille maximale du code dépend du format choisi :

Format	Taille en caractères	Octets
Hexadécimal	96	48
Décimal	25	10
ASCII	192	48
Brut	192	

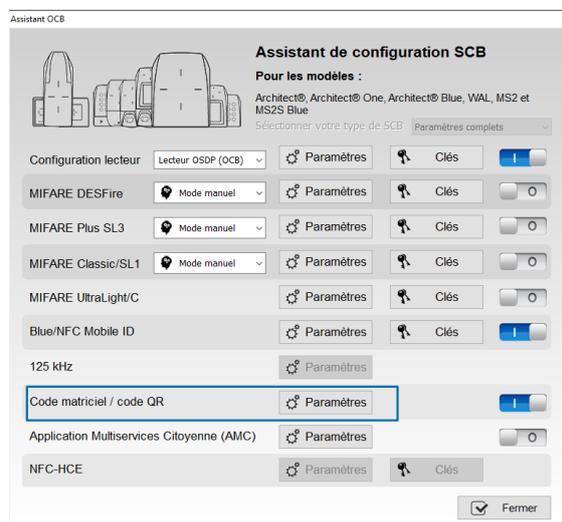
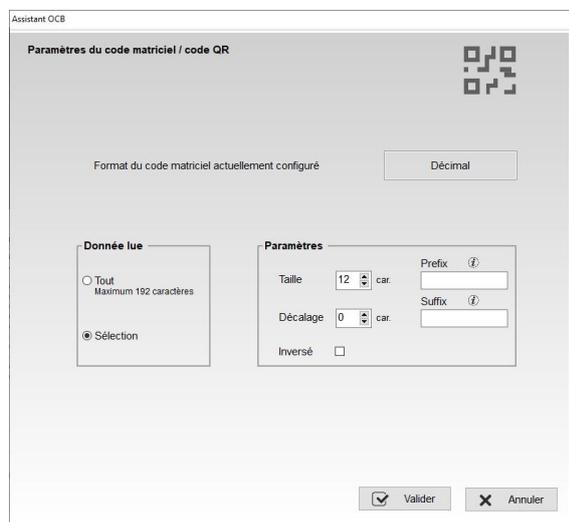
De 0 à 1208925819614629174706175  
0x0 à 0xFFFFFFFFFFFFFFFFFFFFFFFF

Remarque : seuls les caractères listés ci-dessous sont autorisés en ASCII :

Valeur	ASCII caractère	Valeur	ASCII caractère	Valeur	ASCII caractère
30	0	38	8	61	a
31	1	39	9	62	b
32	2	41	A	63	c
33	3	42	B	64	d
34	4	43	C	65	e
35	5	44	D	66	f
36	6	45	E		
37	7	46	F		

Remarque : si le code à lire n'est pas dans le type de code défini dans l'assistant, le code n'est pas lu. Par exemple, si le type décimal est défini et que le code à lire contient une lettre, le code ne sera pas lu.

Pour lire une partie spécifique du code utiliser les paramètres Code matriciel :





Home



Settings



Reader configuration



SCB / OCB



SKB



BCC



SSCF



Create user cards



Tools

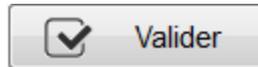
❖ **Eclairage ambiant**

- Mode Eco : environnements à luminosité faible à normale.
- Mode normal / Jour et nuit : toutes conditions de luminosité.
- Mode luminosité intense : Luminosité très forte.

❖ **Paramètres avancés**

Luminosité du faisceau d'éclairage	Contrôle la puissance du spot qui éclaire le code	Normal		Intense
Luminosité du faisceau cible	Contrôle la puissance du laser qui cible le code	Basse	Normale	Haute
Sensibilité de détection	Contrôle la sensibilité du déclencheur pour commencer à scanner le code	Faible	Normal	Max

Cliquer sur le bouton



pour terminer la configuration des paramètres lecteurs.

### III. 4 - Assistant OCB : clés de sécurité du lecteur

Assistant OCB

#### Clé de sécurité lecteur

Garder le contrôle de votre sécurité.  
Définir/modifier vos clés.



#### Clé entreprise OCB

Utiliser une clé de transport

Actuelle

Nouvelle

#### PUPI ISO14443-3B

Signature Clé

#### Chiffrement authentifié

Clé

#### Secure channel based key (SCBK)

Assign

Valider
  Annuler

**Attention : les lecteurs osdp™ en configuration usine sont protégés par une clé de transport, valeur de clé non connue.**

**Attention**

La clé entreprise OCB est importante et doit absolument être connue de l'administrateur. Elle protège les données du « OCB » 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 « OCB » et devra obligatoirement être réinitialisé en usine.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## Configurer un lecteur d'usine

Cocher « Utiliser une clé de transport » et « Nouvelle » et renseigner une valeur dans le champ.

**Clé entreprise OCB**

Utiliser une clé de transport

Actuelle  Nouvelle

Lorsque ce badge de configuration OCB est présenté au lecteur, la clé de sécurité du lecteur prend la valeur du champ nouvelle (ex 0xAA...AA)

**Ce badge de configuration est utilisable sur les lecteurs d'usine et sur les lecteurs ayant déjà été configurés par ce badge :**

OCB « Clé de transport » vers « clé 0xAA...AA »	Lecteur à la Clé de transport	OK
	Lecteur déjà à la clé 0xA...AAA	OK
	Lecteur à une autre valeur de clé	NOK

## Modifier la clé d'un lecteur

Renseigner la valeur de clé du lecteur dans le champ Actuelle et la valeur de la nouvelle clé. Lorsque ce badge de configuration est présenté au lecteur, la clé de sécurité du lecteur prend la valeur du champ nouvelle (ex 0xBB...BB) uniquement si la valeur de clé Actuelle est celle connue par le lecteur.

**Clé entreprise OCB**

Utiliser une clé de transport

Actuelle  New   

OCB « clé 0xAA...AA » vers « clé 0xBB...BB »	Lecteur à la Clé de transport	NOK
	Lecteur à la clé 0xAA...AA	OK
	Lecteur déjà à la clé 0xBB...BB	OK
	Lecteur à une autre valeur de clé	NOK



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## Procédure conseillée en phase de test

### Etape 1 : Créer un badge OCB pour passer le lecteur de la clé de transport à la clé 0xFF...FF :

**Clé entreprise OCB**

Utiliser une clé de transport

Actuelle  New

- ❖ Etiqueter ce badge afin de l'identifier.
- ❖ Présenter le badge OCB au lecteur, attendre les BIPS de prise en compte.
- ❖ Le lecteur est maintenant à la clé 0xFF...FF
- ❖ Vous pouvez ré-encoder ce badge afin d'effectuer des changements de paramètres du lecteur et faire des tests de configuration sans risque de perdre la clé de sécurité du lecteur.
- ❖ Lorsque la configuration est validée passer à l'étape 2 pour sécuriser le lecteur avec une clé différente de FF.

### Etape 2 : Créer un second badge OCB pour passer les lecteurs de la clé 0xFF...FF à une valeur de clé :

**Clé entreprise OCB**

Utiliser une clé de transport

Actuelle  New

- ❖ Etiqueter ce badge afin de l'identifier.
- ❖ Présenter le badge OCB au lecteur, attendre les BIPS de prise en compte.
- ❖ Le lecteur est maintenant à la clé de valeur « nouvelle ».

### PUPI ISO 14443-3B

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

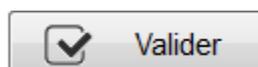
### Chiffrement authentifié (AtE) :

Permet de renseigner la clé pour le chiffrement authentifié.

### Secure channel based key (SCBK)

Charge la clé de Secure channel à l'aide du badge de configuration OCB.

Cliquer sur le bouton



pour terminer la configuration des clés.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



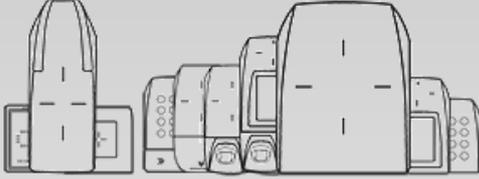
Création badges



Outils

### III. 5 - MIFARE® DESFire® : paramètres

Assistant SCB



## Assistant de configuration SCB

**Pour les modèles :**  
 Architect®, Architect® One, Architect® Blue, WAL, MS2 and MS2S Blue

Sélectionner votre type de SCB Paramètres complets

Configuration lecteur	Type de configuration	Paramètres	Clés	État
MIFARE DESFire	<div style="border: 1px solid #ccc; padding: 2px;"> <span>Mode manuel</span> </div>	<span>Paramètres</span>	<span>Clés</span>	<input checked="" type="checkbox"/>
MIFARE Plus SL3	<div style="border: 1px solid #ccc; padding: 2px;"> <span>Standard</span> </div>	<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
MIFARE Classic/SL1	<div style="border: 1px solid #ccc; padding: 2px;"> <span>Haute sécurité</span> </div>	<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
MIFARE UltraLight/C	<div style="border: 1px solid #ccc; padding: 2px;"> <span>Haute sécurité Bio</span> </div>	<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
Blue/NFC Mobile ID	<div style="border: 1px solid #ccc; padding: 2px;"> <span>Carte CIMS</span> </div>	<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
	<div style="border: 1px solid #ccc; padding: 2px;"> <span>Carte AGENT</span> </div>	<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
	<div style="border: 1px solid #ccc; padding: 2px;"> <span>Carte STITCH</span> </div>	<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
	<div style="border: 1px solid #ccc; padding: 2px;"> <span>HighSec EV2</span> </div>	<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>
125 kHz		<span>Paramètres</span>		<input type="checkbox"/>
Matrix code / QR code		<span>Paramètres</span>		<input type="checkbox"/>
NFC-HCE		<span>Paramètres</span>	<span>Clés</span>	<input type="checkbox"/>

Fermer

Pour faciliter le paramétrage de la puce DESFire, un menu déroulant propose des pré-configurations. En fonction de la configuration choisie 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.

**Mode Haute Sécurité EV2 :** Correspond à une configuration haute sécurité avec Diversification des clés et Proximity Check.

**Mode Haute Sécurité EV2 Bio :** Correspond à une configuration biométrie haute sécurité sur DESFire EV2.

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

**Carte CIMS :**

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

Entrez le numéro de fichier qui vous a été communiqué.  
Couramment le fichier n°1

Entrez la valeur de la clé applicative

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

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

## Carte Agent :

Assistant SCB ARC

**Paramètres MIFARE DESFire**

**Mode de lecture**  
 UID  
 ID Privé  
 ID Privé sinon UID  
 Depuis Blue Mobile ID

**Type clé utilisateur**  
 Une clé (RW)  
 Deux clés (R et W)

**Crypto**  
 3DES  
 AES  
 AES ou 3DES

**Options DESFire**  
 Formater carte  
 Random ID  
 Free App Dir  
 Free Create/Delete  
 Utiliser la clé du FID pour changer sa valeur

**Mode**  
 Ev1 seul  Ev2 ou Ev1  Ev2 seul

**Application Identifier (AID)**  
 MAD3 F51BC0

**Mode de communication**  
 Verrouiller mode EV2  
 EV2 Proximity check  
 Temps de réponse du Proximity Chec 20 x100µs  
 Fully Enciphered

**Fichier1 (FID1)**  
 MSB First  
 Activer Fichier2

**Fichier2 (FID2)**  
 Ecrire  Concaténer  
 Premier

**Options biométrie**  
 N° du FID biométrique 2  
 Active la dérogation biométrique

**N°** 1 **comme FID2**

Taille 3 Décalage 0

Taille 4 Décalage 0

Annuler

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

Entrer le numéro de fichier que vous souhaitez créer.

Couramment le fichier n°1

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.

Assistant SCB ARC

**Clés MIFARE DESFire**

**Clé Maître Carte**  
 Actuelle 00000000000000000000000000000000  
 Nouvelle 00000000000000000000000000000000

**Clé Maître Application**  
 Actuelle 12345678901234567890123456789012  
 Nouvelle 297EC78D2A72C22B34D47767128CBD1B

**Clés Fichier1**  
 N° clé 1  
 Actuelle 12345678901234567890123456789012  
 Nouvelle 3940D83BF9FA7051B3AEE5E3AD3E1FD3

**Clés Fichier2**  
 N° clé 3  
 Actuelle 00000000000000000000000000000000  
 Nouvelle 00000000000000000000000000000000

**Clé d'écriture**  
 N° clé 2  
 Actuelle 12345678901234567890123456789012  
 Nouvelle 7CADAB8B49B8FEC9E2C0707A9CD3973A

**Clés DESFire de sécurité des données biométriques**  
 N° clé 5  
 Actuelle 00000000000000000000000000000000  
 Nouvelle 00000000000000000000000000000000

**Clé d'écriture**  
 N° clé 6  
 Actuelle 00000000000000000000000000000000  
 Nouvelle 00000000000000000000000000000000

**Clé RandomID diversifiée pour GetUID**  
 N° clé 2 Actuelle 12345678901234567890123456789012  
 Nouvelle 00000000000000000000000000000000

Valider Annuler

## Carte STICTCH

Assistant SCB ARC

**Paramètres MIFARE DESFire**

**Mode de lecture**

- UID
- ID Privé
- ID Privé sinon UID
- Depuis Blue Mobile ID

**Type clé utilisateur**

- Une clé (RW)
- Deux clés (R et W)

**Crypto**

- 3DES
- AES
- AES ou 3DES

**Options DESFire**

- Formater carte
- Random ID
- Free App Dir
- Free Create/Delete
- Utiliser la clé du FID pour changer sa valeur

**Mode**

- Ev1 seul
- Ev2 ou Ev1
- Ev2 seul

**Application Identifier (AID)**

MAD3 F51BC0

**Options biométriques**

- Verrouiller mode EV2
- EV2 Proximity check

**Mode de communication**

Fully Enciphered

Temps de réponse du Proximity Check: 20 x100µs

**Fichier1 (FID1)**

N°: 2  comme FID2

Taille: 3

Décalage: 0

**Fichier2 (FID2)**

Ecrire  Concaténer

**Options biométriques**

N° du FID biométrique

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

Entrer le numéro de fichier qui vous a été communiquée.

Indiquer le décalage éventuel permettant de lire l'identifiant attendu.

Assistant SCB ARC

**Clés MIFARE DESFire**

**Clé Maître Carte**

Actuelle: 00000000000000000000000000000000

Nouvelle: 00000000000000000000000000000000

**Clé Maître Application**

Actuelle: 00000000000000000000000000000000

Nouvelle: 297EC78D2A72C22B34D47767128CBD1B

**Diversification**

Activer  CMK  NXP  AID inversé

Données de diversification NXP:  Bourrage

8000

Clé de diversification 3DES:  IDPrime

FF

**Clés Fichier1**

N° clé: 1

Actuelle: 00000000000000000000000000000000

Nouvelle: 3940D83BF9FA7051B3AEE5E3AD3E1FD3

**Clés Fichier2**

N° clé: 3

Actuelle: 00000000000000000000000000000000

Nouvelle: 00000000000000000000000000000000

**Clé d'écriture**

N° clé: 2

Actuelle: 12345678901234567890123456789012

Nouvelle: 7CADAB8B49B8FEC9E2C0707A9CD3973A

**Clé d'écriture**

N° clé: 4

Actuelle: 00000000000000000000000000000000

Nouvelle: 00000000000000000000000000000000

**Clés DESFire de sécurité des données biométriques**

N° clé: 5

Actuelle: 00000000000000000000000000000000

Nouvelle: 00000000000000000000000000000000

**Clé d'écriture**

N° clé: 6

Actuelle: 00000000000000000000000000000000

Nouvelle: 00000000000000000000000000000000

**Clé RandomID diversifiée pour GetUID**

N° clé: 2

Actuelle: 12345678901234567890123456789012

Nouvelle: 00000000000000000000000000000000

Valider  Annuler

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



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## Mode Manuel

Assistant OCB

### Paramètres MIFARE DESFire

**Mode de lecture**

UID

ID Privé

ID Privé sinon UID

Depuis Blue Mobile ID

**Type clé utilisateur**

Une clé (RW)

Deux clés (R et W)

**Crypto**

3DES

AES

AES ou 3DES

**Options DESFire**

Format Card

Random ID

Free App Dir

Free Create/Delete

Utiliser la clé du FID pour changer sa valeur

**Mode**

EV1 seul  EV2 ou EV1  EV2 seul

Mode Lock EV2

Proximity check EV2

Temps de réponse Proximity Check x100µs

Application Identifier (AID)

MAD3

Mode de communication

Fully Enciphered v

MSB First  UID MSB First  Activer Fichier2

**Fichier1 (FID1)**

N°   comme FID2

Taille

Décalage

**Fichier2 (FID2)**

Ecrire  Concaténer  Premier

N°

Taille

Décalage

**Options biométriques**

N° du FID biométrique

Active la dérogation biométrique

Voir les clés

Valider

Annuler

### 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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

## Crypto

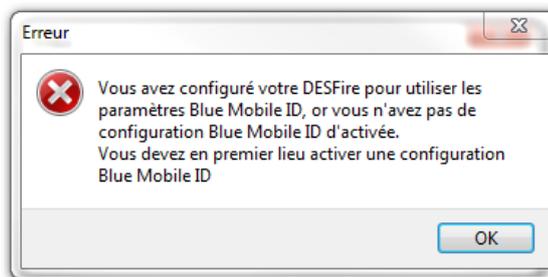
Permet de choisir la méthode d'authentification à utiliser.

- ❖ 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 apparaît :



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

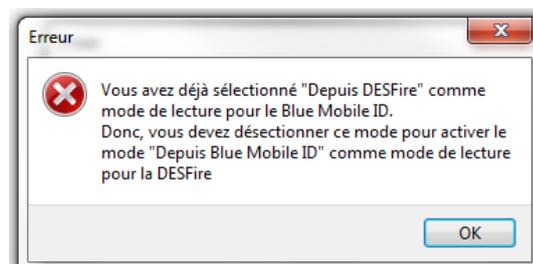
Les paramètres fixés et non modifiables :

- ✓ 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 apparaît :





Accueil



Paramètres

Configuration  
lecteur

SCB / OCB



SKB



BCC



SSCP

Création  
badges

Outils

## Options DESFire®

### ❖ Formater carte :

Si cette option est activée, les puces DESFire® EVx 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® EVx 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® EVx.

### ❖ 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® EVx 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



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

#### ❖ 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 essaye 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).



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## 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.

## UID MSB First

Si le mode de lecture est défini sur ID Privé sinon UID, permet de définir le sens de lecture de l'ID privé indépendamment de celui de l'UID.

UID MSB First

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

Si la case est décochée, le lecteur lira l'UID Least Significant Byte 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 ».



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## 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) corresponde 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 apparaîtront 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**.

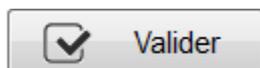
Pour cela, l'ajout de 0 non significatifs peut s'avérer nécessaire.  
Exemple : pour un ID 0x11 0x22, si la taille définie est sur 3 octets, il faudra alors renseigner 0x00 0x11 0x22.

## 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**

**Goto Keys :** raccourci vers la page de paramétrages des clés DESFire.

Cliquer sur le bouton



pour terminer la configuration des paramètres DESFire®.

### III. 6 - MIFARE® DESFire® : clés

-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

Assistant OCB

#### Clés MIFARE DESFire

Paramètres principaux Paramètres fichiers

**Card Master key**

Actuelle

Nouvelle

**Diversification**

Activer

**Clé maître application**

Actuelle

Nouvelle

**Clé RandomID diversifiée pour GetUID**

Keyld

Actuelle

New

Assistant OCB

#### Clés MIFARE DESFire

Paramètres principaux Paramètres fichiers

**Clés Fichier1**

Keyld

Actuelle

Nouvelle

**Clé d'écriture**

Keyld

Courante

Nouvelle

**Clés Fichier2**

Keyld

Actuelle

Nouvelle

**Clé d'écriture**

Keyld

Actuelle

Nouvelle

**Clés DESFire de sécurité des données biométriques**

Keyld

Actuelle

Nouvelle

**Clé d'écriture**

Keyld

Actuelle

Nouvelle



Permet de définir toutes les clés relatives à la puce MIFARE® DESFire®.

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®](#).

-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

Assistant OCB

### Clés MIFARE DESFire

Paramètres principaux | Paramètres fichiers

#### Card Master key

Actuelle

Nouvelle

#### Diversification

Activer

CMK     NXP     AID inversé

IDPrime     NXP divAV1

Données de diversification NXP  Bourrage

Clé de diversification 3DES

#### Clé maître application

Actuelle

Nouvelle

#### Clé RandomID diversifiée pour GetUID

Keyld

Actuelle

New

## Clé Maître Carte

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

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® EVx.

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.

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

## 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 saisisse 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.

### 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.

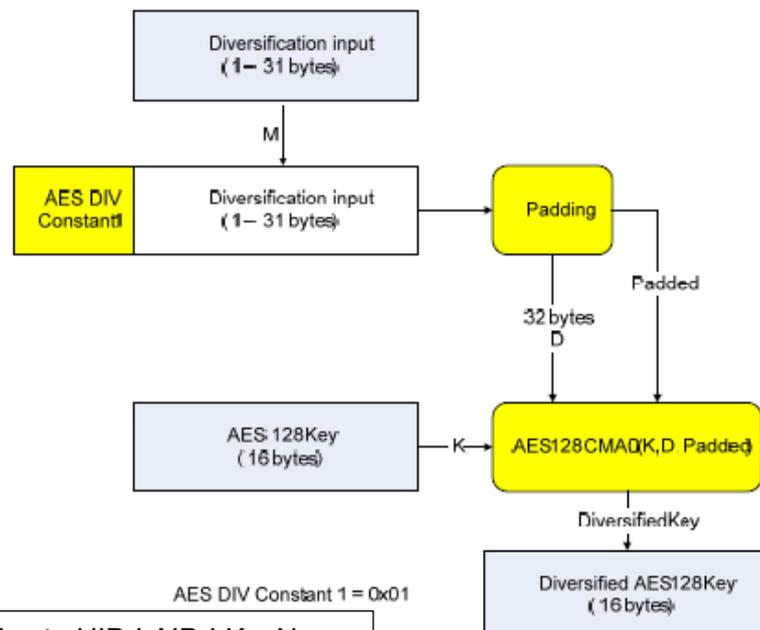
Afin de désactiver la diversification des clés appliquée sur la Card Master Key, il est nécessaire de décocher l'option "CMK" et de formater la puce via la case "Formate la carte". De plus un changement de clés est nécessaire.

❖  NXP

clé diversifiée selon la méthode NXP-AN-165310.

❖  NXP

clé diversifiée selon la méthode NXP-AN10922.



"Diversification input" est : UID | AID | KeyNum.

-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

- ❖ 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.

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

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

Données de diversification NXP     Bourrage

00

- ❖ 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\*.

Données de diversification NXP     Bourrage

00

- ❖ 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.

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.

- ❖  IDPrime cocher cette case **pour lire** des badges encodés avec la diversification spécifique Gemalto MD3811 (1 | UID | Padding & Card UID Len=4). **Uniquement pour lire des badges déjà encodés pas pour faire de l'encodage.**

- ❖  NXP divAV1 clé diversifiée selon la méthode NXP AN-0148 (3DES divAv1).

-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

Assistant OCB

### Clés MIFARE DESFire

Paramètres principaux | Paramètres fichiers

**Clés Fichier1**

Keyld <input type="text" value="1"/>	<b>Clé d'écriture</b>
Actuelle <input type="text" value="00000000000000000000000000000000"/>	Keyld <input type="text" value="2"/>
<input type="checkbox"/> Nouvelle <input type="text" value="00000000000000000000000000000000"/>	Courante <input type="text" value="00000000000000000000000000000000"/>
	<input type="checkbox"/> Nouvelle <input type="text" value="00000000000000000000000000000000"/>

**Clés Fichier2**

Keyld <input type="text" value="3"/>	<b>Clé d'écriture</b>
Actuelle <input type="text" value="00000000000000000000000000000000"/>	Keyld <input type="text" value="4"/>
<input type="checkbox"/> Nouvelle <input type="text" value="00000000000000000000000000000000"/>	Actuelle <input type="text" value="00000000000000000000000000000000"/>
	<input type="checkbox"/> Nouvelle <input type="text" value="00000000000000000000000000000000"/>

**Clés DESFire de sécurité des données biométriques**

Keyld <input type="text" value="5"/>	<b>Clé d'écriture</b>
Actuelle <input type="text" value="00000000000000000000000000000000"/>	Keyld <input type="text" value="6"/>
<input type="checkbox"/> Nouvelle <input type="text" value="00000000000000000000000000000000"/>	Actuelle <input type="text" value="00000000000000000000000000000000"/>
	<input type="checkbox"/> Nouvelle <input type="text" value="00000000000000000000000000000000"/>

### 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.

#### 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.**



-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

• **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

**Clé maitre application**

Actuelle

Nouvelle

**Clés Fichier1**

Keyld

Actuelle

Nouvelle

Second encodage avec la même valeur de clé

**Clé maitre application**

Actuelle

Nouvelle

**Clés Fichier1**

Keyld

Actuelle

Nouvelle

Second encodage avec changement de la valeur de la clé

**Clé maitre application**

Actuelle

Nouvelle

**Clés Fichier1**

Keyld

Actuelle

Nouvelle

-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

Cas de deux clés :

Premier encodage sur badge vierge

**Clé maitre application**

Actuelle

Nouvelle

**Clés Fichier1**

<p>Keyld <input type="text" value="0"/></p> <p>Actuelle <input type="text" value="00000000000000000000000000000000"/></p> <p><input checked="" type="checkbox"/> Nouvelle <input type="text" value="F7FF47BE78E36BC1B501D9905CFA2963"/></p>	<p><b>Clé d'écriture</b></p> <p>Keyld <input type="text" value="0"/></p> <p>Courante <input type="text" value="F7FF47BE78E36BC1B501D9905CFA2963"/></p> <p><input type="checkbox"/> Nouvelle <input type="text" value="00000000000000000000000000000000"/></p>
---	---

Ré encodage sans changement de valeur de la clé

**Clé maitre application**

Actuelle

Nouvelle

**Clés Fichier1**

<p>Keyld <input type="text" value="0"/></p> <p>Actuelle <input type="text" value="F7FF47BE78E36BC1B501D9905CFA2963"/></p> <p><input checked="" type="checkbox"/> Nouvelle <input type="text" value="00000000000000000000000000000000"/></p>	<p><b>Clé d'écriture</b></p> <p>Keyld <input type="text" value="0"/></p> <p>Courante <input type="text" value="F7FF47BE78E36BC1B501D9905CFA2963"/></p> <p><input type="checkbox"/> Nouvelle <input type="text" value="00000000000000000000000000000000"/></p>
---	---

Ré encodage avec changement de valeur de la clé

**Clé maitre application**

Actuelle

Nouvelle

**Clés Fichier1**

<p>Keyld <input type="text" value="0"/></p> <p>Actuelle <input type="text" value="F7FF47BE78E36BC1B501D9905CFA2963"/></p> <p><input checked="" type="checkbox"/> Nouvelle <input type="text" value="73272D8B3A4F10489FF66C24602F7F9A"/></p>	<p><b>Clé d'écriture</b></p> <p>Keyld <input type="text" value="0"/></p> <p>Courante <input type="text" value="73272D8B3A4F10489FF66C24602F7F9A"/></p> <p><input type="checkbox"/> Nouvelle <input type="text" value="00000000000000000000000000000000"/></p>
---	---



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## Clés DESFire de sécurité des données biométriques

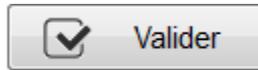
Permet de paramétrer le numéro de clé et la valeur de la clé du fichier biométrique.

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.

Cliquer sur le bouton



pour terminer la configuration des clés DESFire® EVx.

### III. 7 - MIFARE Plus® SL3 : paramètres

Assistant SCB ARC

**Paramètres MIFARE Plus Level 3**

<p><b>Mode de lecture</b></p> <p><input type="radio"/> UID</p> <p><input checked="" type="radio"/> ID Privé</p> <p><input type="radio"/> ID Privé sinon UID</p>	<p><b>Type clé utilisateur</b></p> <p><input checked="" type="radio"/> Une clé (RW)</p> <p><input type="radio"/> Deux clés (R et W)</p>	<p><b>Données</b></p> <p>Taille <input type="text" value="5"/></p> <p>Décalage <input type="text" value="0"/></p> <p>MSB First <input checked="" type="checkbox"/></p>
<p><b>Emplacement du secteur</b></p> <p><input checked="" type="radio"/> Automatique</p> <p><input type="radio"/> Forcé avec la MAD</p> <p><input type="radio"/> Forcé sans la MAD</p>		
	<p>Numéro secteur</p> <p><input type="text" value="1"/></p>	<p>AID</p> <p><input type="text" value="51BC"/> </p>
<p><b>Options biométriques</b></p> <p><input checked="" type="radio"/> Automatique</p> <p><input type="radio"/> Forcé avec la MAD</p> <p><input type="radio"/> Forcé sans la MAD</p>		
	<p>Numéro secteur</p> <p><input type="text" value="32"/></p>	<p>AID</p> <p><input type="text" value="5100"/></p> <p><input type="checkbox"/> Active la dérogation biométrique</p>

Valider     Annuler

#### 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.



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## 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 *cluster 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 » 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 » 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.



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## Options biométriques

Les empreintes à encoder seront inscrites dans les secteurs 32 à 39 de la puce 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. 8 - MIFARE Plus® SL3 : clés

-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

Assistant SCB ARC

**Clés MIFARE Plus Level 3**

**Diversification des clés**

 Diversification     Div NXP

**Clés utilisateurs**

<p>Clé de lecture actuelle</p> <input style="width: 95%;" type="text" value="FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"/> <p><input type="checkbox"/> Nouvelle</p> <input style="width: 95%;" type="text" value="00000000000000000000000000000000"/> <input type="checkbox"/>	<p>Clé d'écriture actuelle</p> <input style="width: 95%;" type="text" value="FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"/> <p><input type="checkbox"/> Nouvelle</p> <input style="width: 95%;" type="text" value="00000000000000000000000000000000"/> <input type="checkbox"/>
--	--

**Paramètres MAD**

<p>Clé A de lecture MAD</p> <input style="width: 95%;" type="text" value="A0A1A2A3A4A5A6A7A0A1A2A3A4A5A6A7"/>	<p>Clé B d'écriture MAD</p> <input style="width: 95%;" type="text" value="FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"/> <p><input checked="" type="checkbox"/> Nouvelle</p> <input type="checkbox"/> <input style="width: 95%;" type="text" value="B0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF"/> <input type="checkbox"/>
---	---

**Clés MIFARE Plus Level 3 pour les données biométriques**

<p>Clé de lecture actuelle</p> <input style="width: 95%;" type="text" value="00000000000000000000000000000000"/> <p><input checked="" type="checkbox"/> Nouvelle</p> <input style="width: 95%;" type="text" value="00000000000000000000000000000000"/> <input type="checkbox"/>	<p>Clé d'écriture actuelle</p> <input style="width: 95%;" type="text" value="00000000000000000000000000000000"/> <p><input type="checkbox"/> Nouvelle</p> <input style="width: 95%;" type="text" value="00000000000000000000000000000000"/> <input type="checkbox"/>
---	--

Valider     Annuler

#### 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**



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## 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, il est possible de la changer en remplissant le champ Nouvelle clé B MAD.

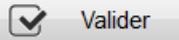
Lors d'une gestion de MAD, les clés des secteurs « 0 » et « 16 » changent. Les conditions d'accès sont :

- 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 »

## 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 de les modifier.

Cliquer sur le bouton



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

### III. 9 - MIFARE® Classic/SL1 : paramètres

Assistant SCB ARC

#### Paramètres MIFARE Classic/SL1

**Mode de lecture**

UID

ID Privé

ID Privé sinon UID

**Type clé utilisateur**

Une clé (RW)

Deux clés (R et W)

**Données**

Taille

Décalage

MSB First

**Emplacement du secteur**

Automatique

Forcé avec la MAD

Forcé sans la MAD

Numéro secteur	AID	
<input type="text" value="1"/>	<input type="text" value="51BC"/>	<input checked="" type="checkbox"/>

**Options biométriques**

Automatic template location

Forcé avec la MAD

Forcé sans la MAD

N° du secteur	AID	
<input type="text" value="32"/>	<input type="text" value="5100"/>	<input type="checkbox"/> Active la dérogation biométrique

Valider

Annuler

#### 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.



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## 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 *cluster 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.



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



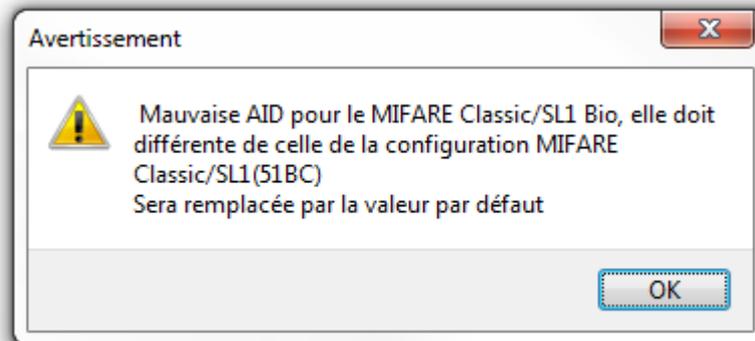
Outils

## Options biométriques

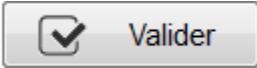
Uniquement disponible pour des puces MIFARE® Classic 4ko.

Définir le secteur ( $\geq 32$ ) 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  **Valider** pour terminer la configuration des paramètres MIFARE® Classic/SL1.

### III. 10 - MIFARE® Classic /SL1 : clés

-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

Assistant SCB ARC

#### Clés MIFARE Classic/SL1

**Clé de lecture utilisateur**

Actuelle  Nouvelle

**Clé d'écriture utilisateur**

Actuelle  Nouvelle

**Diversification**

Diversifier les clés

Clé de diversification 3DES actuelle  Nouvelle

Authentification SL1

Clé AES de sécurité de niveau 1

**Clés MAD**

Clé A de lecture MAD   Nouvelle clé B MAD

Clé B d'écriture MAD

**Clés utilisateur de la partie biométrique Classic/SL1**

Clé de lecture actuelle  Nouvelle

Clé d'écriture actuelle  Nouvelle

#### 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.



Accueil



Paramètres

Configuration  
lecteur

SCB / OCB



SKB



BCC



SSCP

Création  
badges

Outils

## 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 1 ayant 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 »

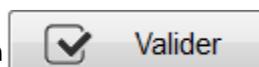
### ATTENTION,

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.

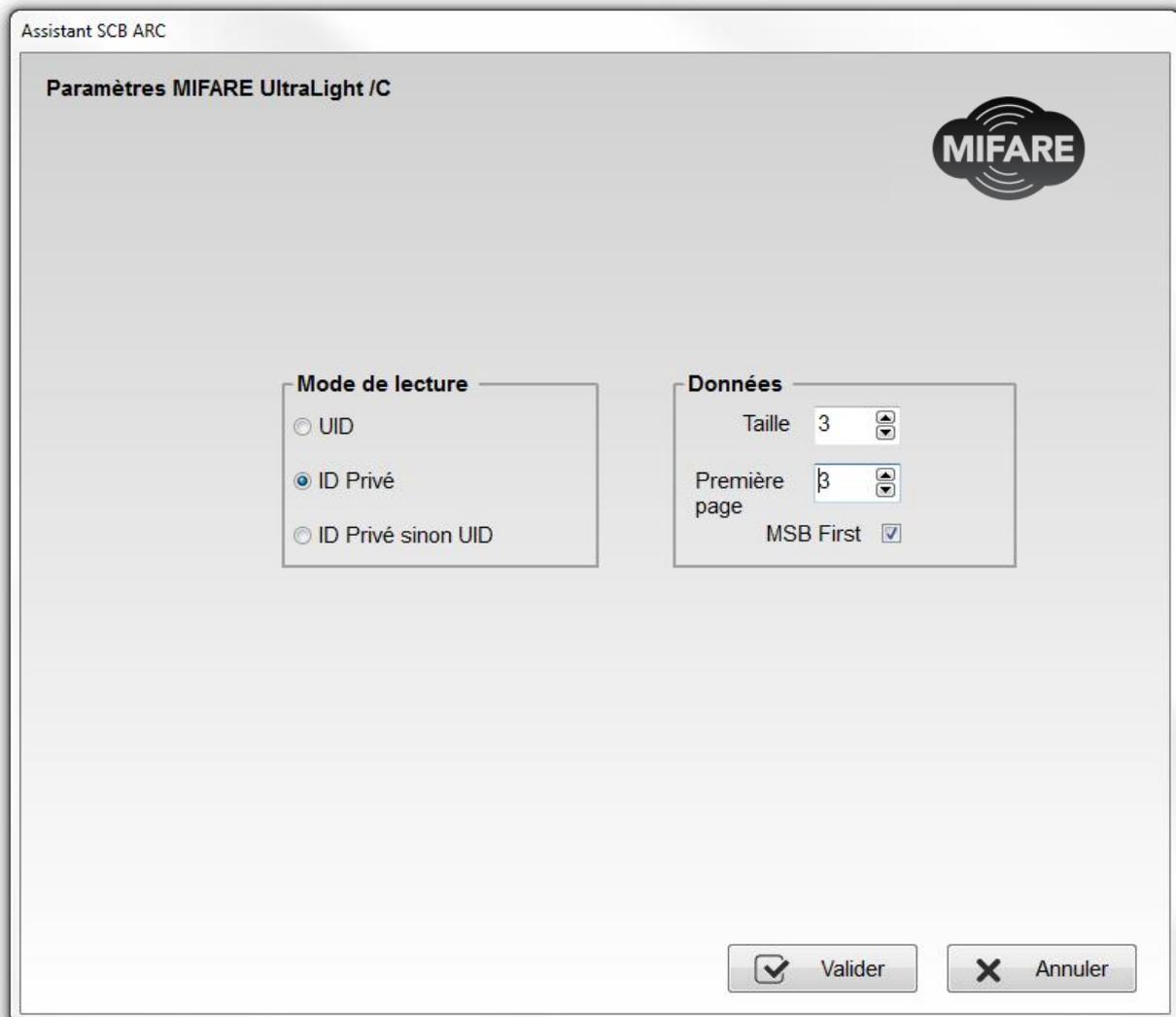
Cliquer sur le bouton



pour terminer la configuration des clés MIFARE®

Classic/SL1.

### III. 11 - MIFARE Ultralight® C : paramètres



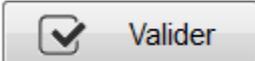
#### Mode de lecture

- ❖ 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. 12 - MIFARE Ultralight® C : Clés

Assistant SCB ARC

**Clés MIFARE Ultra Light /C** 

Garder la maîtrise de votre sécurité. Définir/modifier vos clés.

Activer authentification 3DES (uniquement ULC)

**Clés 3DES**

Clé utilisateur  

Nouvelle

Verrouiller le mode d'authentification 3DES

Lecture libre

Diversifier clés

Clé de diversification

Verrouiller opérations d'écriture (irréversible)

Valider     Annuler

#### 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.



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

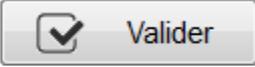
## Diversifier clés

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

### III. 13 - Blue/NFC Mobile ID : paramètres

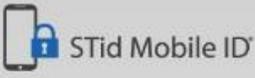
#### III.13.1 - STid Mobile ID®

##### ❖ Mode de lecture : ID privé

Assistant SCB



**Blue/NFC Mobile ID**






**Paramètres lecteur**

**Mode de lecture**

ID Privé

Depuis DESFire

ID privé sinon CSN

**Type de clé**

Une clé (RW)

Deux clés (R et W)

**Données**

Taille

Décalage

Inversé

**Paramètres du badge d'accès virtuel**

Nom du badge d'accès virtuel (max 14 caractères)\*

Aperçu du badge



ID

Code site

Nom de la configuration

Interdire la suppression

Remote 1

Remote 2

Déverrouillage requis

Déverrouillage Bio

Valider
  Annuler

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.

#### Données

- ❖ Taille : Détermine la longueur de l'identifiant.  
**En SCB, Taille doit être égal à la taille du protocole de l'étape SCB – Etape3**
- ❖ Décalage : Définit 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).

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

## Paramètres du badge d'accès virtuel

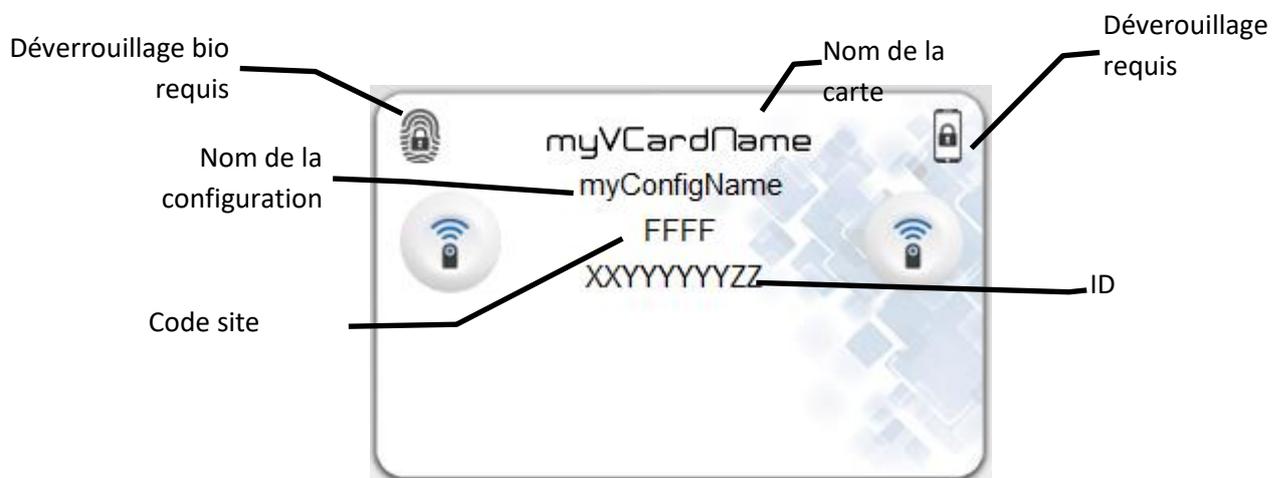
Personnalisation de l'affichage du badge virtuel.

Nom de la carte d'accès : Nom qui apparaîtra 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



**Interdire la suppression** : interdit la suppression du badge d'accès virtuel par l'utilisateur. Seul l'administrateur, via SECard (Paramètres / Crédits / Supprimer votre badge virtuel d'accès) peut le supprimer.

## ❖ Mode de lecture : Depuis DESFire

Assistant SCB

Blue/NFC Mobile ID

STid Mobile ID

GET IT ON Google Play  
Download on the App Store

**Paramètres lecteur**

**Mode de lecture**

ID Privé

Depuis DESFire

ID privé sinon CSN

**Type de clé**

Une clé (RW)

Deux clés (R et W)

**Données**

Taille: 5

Décalage: 0

Inversé

**Paramètres du badge d'accès virtuel**

Nom du badge d'accès virtuel (max 14 caractères)\*

STid Secure ID

Aperçu du badge

ID

Code site

Nom de la configuration

Interdire la suppression

Remote 1

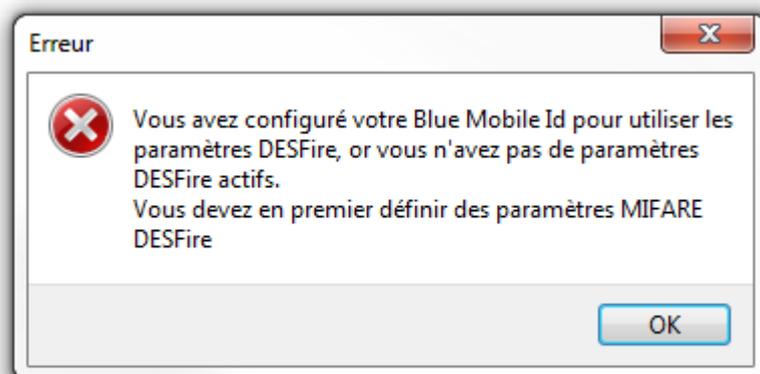
Remote 2

Déverrouillage requis

Déverrouillage Bio

✓ Valider    ✗ Annuler

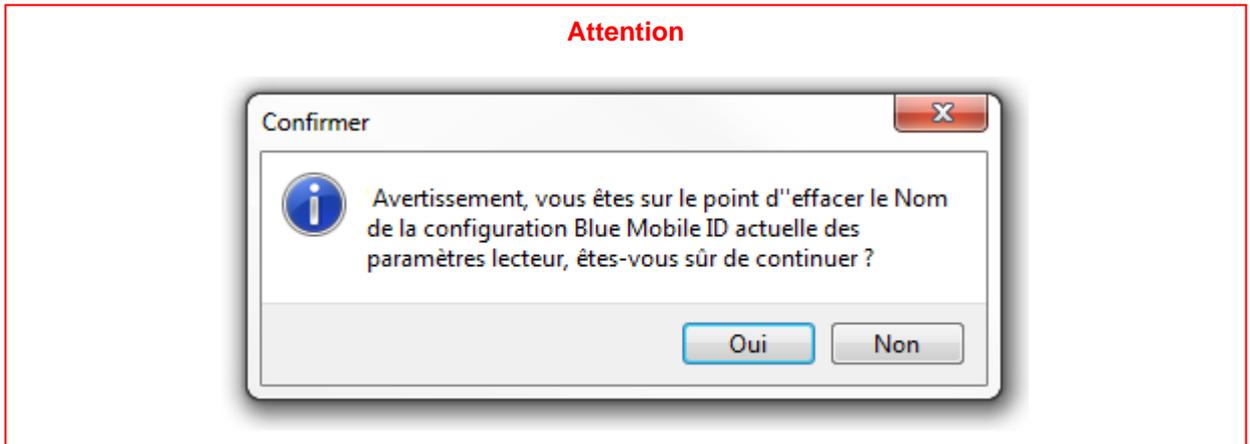
Si ce mode est activé, une configuration DESFire doit être active sinon le message d'erreur suivant apparaîtra :



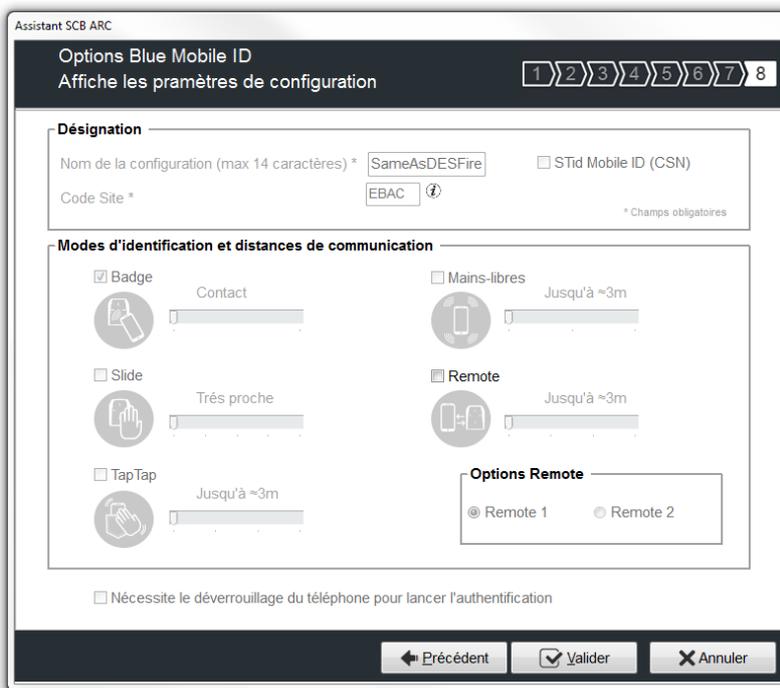
-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

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.



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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### III.13.2 - Orange™ Pack ID

SCB wizard



**Blue/NFC Mobile ID**



---

**Paramètres lecteur**

**Mode de lecture**

ID Privé

Depuis DESFire

ID privé sinon CSN

**Type de clé**

Une clé (RW)

Deux clés (R et W)

**Données**

Taille

Décalage

Inversé

**Paramètres Orange™ Pack ID**

Company Identifier

Service ID

Access ID

TX power (dbm)

Valider
  Annuler

- ❖ 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. (défaut 4 dbm).  
Valeurs possibles : -16, -12, -8, -4, 0 and 4 dbm.



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

### III.13.3 - Open Mobile Protocol

SCB wizard

**Blue/NFC Mobile ID**

**Paramètres lecteur**

**Mode de lecture**  
 ID Privé  
 Depuis DESFire  
 ID privé sinon CSN

**Type de clé**  
 Une clé (RW)  
 Deux clés (R et W)

**Données**  
Taille   
Décalage   
 Inversé

**Open Mobile Protocol**

**Mode de communication**  
 Communication sécurisée

Complete local name

Code site

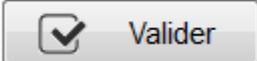
Octets génériques

Puissance émise (dbm)

Identifiant Entreprise

Valider  Annuler

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

Cliquer sur le bouton  pour terminer la configuration

### III. 14 - Blue/NFC Mobile ID : clés

-   
Accueil
-   
Paramètres
-   
Configuration lecteur
-   
SCB / OCB
-   
SKB
-   
BCC
-   
SSCP
-   
Création badges
-   
Outils

SCB wizard

**Clés Blue/NFC Mobile ID**







Pack ID

Garder la maîtrise de votre sécurité. Définir/modifier vos clés.

**Clé de lecture/écriture Blue/NFC**

Actuelle	00000000000000000000000000000000
<input type="checkbox"/> Nouvelle	00000000000000000000000000000000 <input type="checkbox"/>

**Clé d'écriture Blue/NFC**

Actuelle	00000000000000000000000000000000
<input type="checkbox"/> Nouvelle	00000000000000000000000000000000 <input type="checkbox"/>

Valider
  Annuler

Permet de définir les clés de sécurité utilisées pour les données Blue/NFC.

Les clés par défaut sont 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges

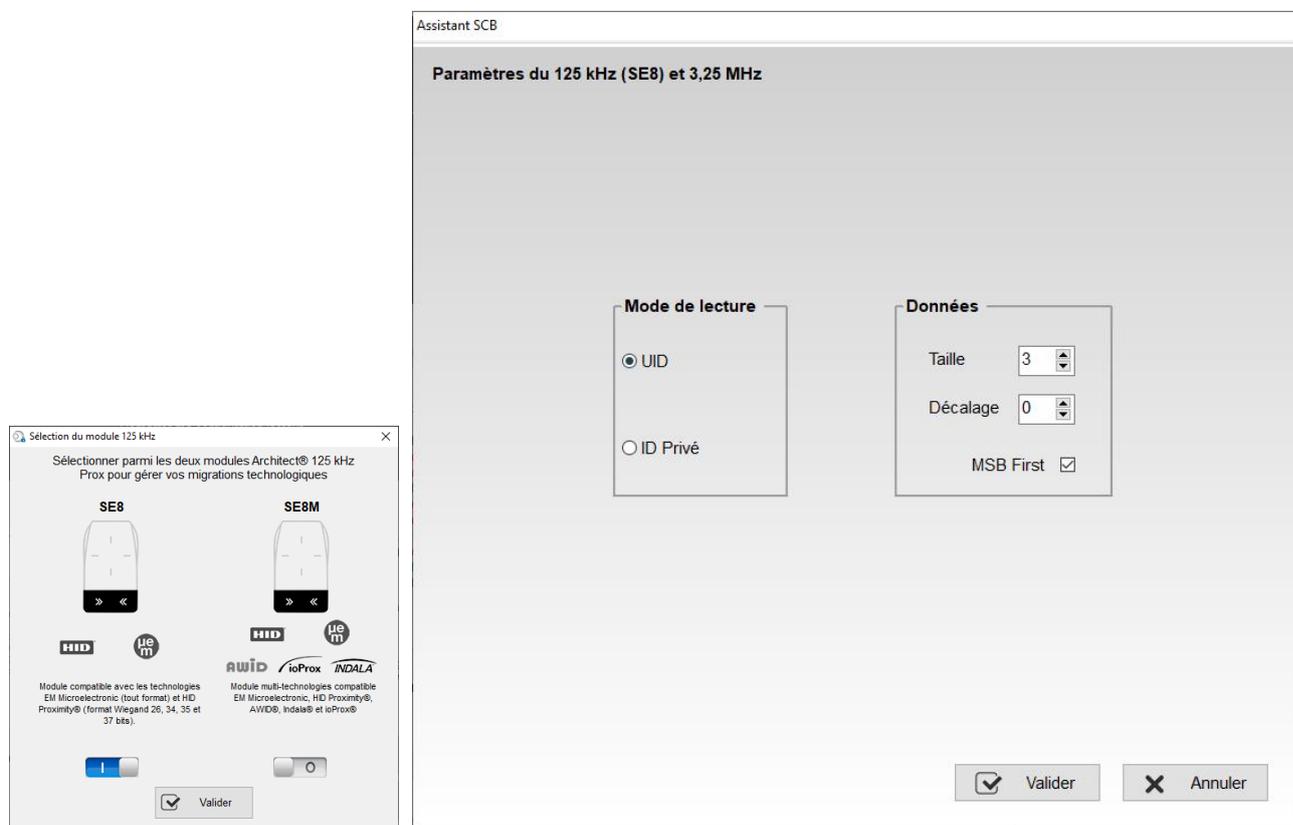


Outils

### III. 15 - 125 kHz : paramètres

L'écran de paramètres dépend du module SE8 choisi à l'étape 2.

#### III.15.1 – SE8



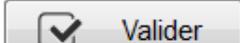
Permet de configurer les paramètres de lecture liés aux puces EM4102, EM4x50, HID, Nedap 125 kHz.

#### 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 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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



Création badges



Outils

### III.15.2 – SE8M

Sélection du module 125 kHz

Sélectionner parmi les deux modules Architect® 125 kHz Prox pour gérer vos migrations technologiques

**SE8**

**HID**

Module compatible avec les technologies EM Microelectronic (tout format) et HID Proximity® (format Wiegand 26, 34, 35 et 37 bits).

**SE8M**

**HID**

**AWID** **ioProx** **INDALA**

Module multi-technologies compatible EM Microelectronic, HID Proximity®, AWID®, Indala® et ioProx®

Valider

Assistant SCB

#### Paramètres SE8M Prox 125 kHz multi-technologies

HID Proximity®

AWID®

EM Microelectronic  MSB First

ioProx®  XSF(39 bits)  26 bits  Lecteur (codesite+codecarte:24 bits)

Indala®  27 bits  Lecteur (27 bits de données)

Valider  Annuler



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### ❖ HID Proximity®

Le protocole de sortie dépend du format d'encodage du badge.

Le protocole de sortie sélectionné à l'étape 3 de l'assistant de configuration n'est pas pris en compte.

### ❖ AWID®

Le protocole de sortie dépend du format d'encodage du badge.

Le protocole de sortie sélectionné à l'étape 3 de l'assistant de configuration n'est pas pris en compte.

### ❖ EM Microelectronic

Le protocole de sortie est celui sélectionné à l'étape 3 de l'assistant de configuration.

#### MSB First

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

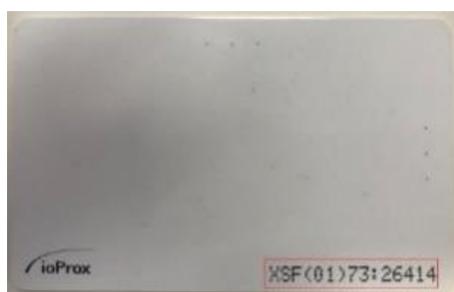
Si la case est décochée, le lecteur lira l'identifiant Least Significant Byte First.

### ❖ ioProx®

 XSF(39 bits)

#### Structure du message

Bit 1 ...Bit 5 (6 bits)	Bit 6 ... Bit 38 (data)			Bit 39 (1 bit)
	Bit 6...bit 13 (8 bits)	Bit 14...Bit 21 (8 bits)	Bit 22...Bit 38 (16 bits)	
Taille de la donnée	Code famille	Code site	Code carte	Parité paire sur les 38 bits



Exemple :

39 taille	0x01 code famille	0x73 (code site)	26414 = 0x672E	Parité
10 0111	0000 0001	0111 0011	0110 0111 0010 1110	0

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

● 26 bits

Structure du message

Bit 1	Bit 2 ... Bit 25 (data)		Bit 26
	Bit 2...Bit 9	Bit 10...bit 25	
<i>Parité paire du bit 2 au bit 13</i>	<i>Code site</i>	<i>Code carte</i>	<i>Parité impaire du bit 4 au bit 25</i>



Exemple :

Parité	0x73 (code site)	26414 = 0x672E	Parité
1	0111 0011	0110 0111 0010 1110	0

● Lecteur (codesite+codecarte:24 bits)

« Code site + code carte » sont envoyés dans une trame selon le protocole de sortie du lecteur choisi à l'étape 3 de l'assistant de configuration.

❖ Indala

● 27 bits

Structure du message

Bit 1 ...Bit 27 (27 bits)
Code carte



Exemple :

19030 = 0x0004A56
000 0000 0000 0100 1010 0101 0110

● Lecteur (27 bits de données)

Les 27 bits du code carte sont envoyés dans une trame selon le protocole de sortie du lecteur choisi à l'étape 3 de l'assistant de configuration

### III. 16 - Code matriciel / code QR : paramètres *Ajout fonctionnalité 3.6*

Assistant SCB

**Paramètres du code matriciel / code QR**



Format du code matriciel actuellement configuré

Décimal

**Donnée lue**

Tout  
Maximum 192 caractères

Sélection

**Paramètres**

Taille  car.

Décalage  car.

Inversé

Prefix  ⓘ

Suffix  ⓘ

Valider

Annuler

❖ **Tout** : lit la chaîne de caractères complète.

❖ **Sélection** : lit la chaîne de caractères selon les paramètres Taille et Décalage.

- Si la taille est fixée à 0, il n'y a pas de filtrage sur la chaîne de caractères, la chaîne de caractère est complètement lue. Il est possible d'avoir une taille 0 et de fixer un offset.
- Inversé : permet d'inverser le code lu suivant le format défini du QR Code

Exemple :

- Décimal : lecture du code décimal, conversion en hexadécimal puis inversion octet par octet
  - 1234 => 0x04D2 => 0xD204
- Hexadécimal : lecture du code hexadécimal, puis inversion octet par octet
  - 1234 => 0x1234 => 0x3412
- ASCII : lecture du code ascii, conversion en hexadécimal puis inversion octet par octet
  - 31323334 => 0x1234 => 0x3412

Remarque : si le type de code à lire n'est pas du type de code défini dans l'assistant, le code n'est pas lu. Par exemple, si le type décimal est défini et que le code à lire contient une lettre, le code ne sera pas lu.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### ❖ Prefix / Suffix :

Le préfixe et / ou le suffixe peuvent être utilisés pour lire uniquement les données qui contiennent des caractères de texte spécifiques de début et / ou de fin ou pour trouver le numéro d'identification dans une chaîne de texte plus longue.

Les caractères de préfixe / suffixe seront supprimés de la donnée lue.

Le préfixe / suffixe ne doivent pas nécessairement être en début ou en fin de la donnée lue.

Si le préfixe et / ou le suffixe n'est pas identifié dans la donnée, l'ID est considéré comme non valide.

La gestion du préfixe et / ou du suffixe est complémentaire aux autres paramètres de traitement de l'identifiant comme la taille et l'offset.

La taille maximum du préfixe et du suffixe est de 20 octets chacun.

<identifiant=12345><lieu=greasque>	
<div style="border: 1px solid gray; padding: 5px;"> <p style="text-align: right;">Format du code matriciel actuellement configuré <span style="float: right;">Décimal</span></p> <p><b>Paramètres</b></p> <p>Taille <input type="text" value="3"/> car. Prefix <input type="text" value="&lt;identifiant="/> <span style="float: right;">?</span></p> <p>Décalage <input type="text" value="2"/> car. Suffix <input type="text" value="&gt;"/> <span style="float: right;">?</span></p> <p>Inversé <input type="checkbox"/></p> </div> <p>Donnée lue entre Prefix et Suffix : 12345            Application de l'Offset à 2, donnée : 345            Application de Len à 3, donnée : 345            ID valide            Remontée = 345 en ISO // 0x159 en Wiegand</p>	<div style="border: 1px solid gray; padding: 5px;"> <p style="text-align: right;">Format du code matriciel actuellement configuré <span style="float: right;">Décimal</span></p> <p><b>Paramètres</b></p> <p>Taille <input type="text" value="0"/> car. Prefix <input type="text" value="&lt;identifiant="/> <span style="float: right;">?</span></p> <p>Décalage <input type="text" value="0"/> car. Suffix <input type="text" value="&gt;"/> <span style="float: right;">?</span></p> <p>Inversé <input type="checkbox"/></p> </div> <p>Donnée lue entre Prefix et Suffix : 12345            ID valide = 12345 en ISO</p>
<div style="border: 1px solid gray; padding: 5px;"> <p style="text-align: right;">Format du code matriciel actuellement configuré <span style="float: right;">Décimal</span></p> <p><b>Paramètres</b></p> <p>Taille <input type="text" value="3"/> car. Prefix <input type="text" value="&lt;identifiant="/> <span style="float: right;">?</span></p> <p>Décalage <input type="text" value="2"/> car. Suffix <input type="text" value=""/> <span style="float: right;">?</span></p> <p>Inversé <input type="checkbox"/></p> </div> <p>Donnée lue après Prefix : 12345&gt;&lt;lieu=greasque&gt;            Application de l'Offset à 2, donnée : 345&gt;&lt;lieu=greasque&gt;            Application de Len à 3, donnée : 345            ID valide = 345</p>	<div style="border: 1px solid gray; padding: 5px;"> <p style="text-align: right;">Format du code matriciel actuellement configuré <span style="float: right;">Décimal</span></p> <p><b>Paramètres</b></p> <p>Taille <input type="text" value="0"/> car. Prefix <input type="text" value="&lt;identifiant="/> <span style="float: right;">?</span></p> <p>Décalage <input type="text" value="2"/> car. Suffix <input type="text" value=""/> <span style="float: right;">?</span></p> <p>Inversé <input type="checkbox"/></p> </div> <p>Donnée lue après Prefix : 12345&gt;&lt;lieu=greasque&gt;            Application de l'Offset à 2, donnée : 345&gt;&lt;lieu=greasque&gt;            Application de Len à 0, donnée : 345&gt;&lt;lieu=greasque&gt;            ID non valide : rejeté</p>
<div style="border: 1px solid gray; padding: 5px;"> <p style="text-align: right;">Format du code matriciel actuellement configuré <span style="float: right;">Décimal</span></p> <p><b>Paramètres</b></p> <p>Taille <input type="text" value="2"/> car. Prefix <input type="text" value="&lt;identifiant="/> <span style="float: right;">?</span></p> <p>Décalage <input type="text" value="1"/> car. Suffix <input type="text" value="&gt;"/> <span style="float: right;">?</span></p> <p>Inversé <input type="checkbox"/></p> </div> <p>Donnée lue entre Prefix et suffix : 12345            Application de l'Offset à 1, donnée : 2345            Application de Len à 2, donnée : 23            ID valide = 23</p>	<div style="border: 1px solid gray; padding: 5px;"> <p style="text-align: right;">Format du code matriciel actuellement configuré <span style="float: right;">Hexadécimal</span></p> <p><b>Paramètres</b></p> <p>Taille <input type="text" value="0"/> car. Prefix <input type="text" value="&lt;identifiant="/> <span style="float: right;">?</span></p> <p>Décalage <input type="text" value="1"/> car. Suffix <input type="text" value="&gt;"/> <span style="float: right;">?</span></p> <p>Inversé <input type="checkbox"/></p> </div> <p>Donnée lue entre Prefix et suffix : 12345            Application de l'Offset à 1, donnée : 2345            Application de Len à 0, donnée : 2345            ID valide            Remontée = 0x2345 en Wiegand // 9029 en ISO</p>

- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- SSCP
- Création badges
- Outils

2C569E26 toto@stid.com	
<div style="border: 1px solid #ccc; padding: 5px;"> <p style="text-align: right; margin: 0;">Format du code matriciel actuellement configuré <span style="float: right;">Hexadécimal</span></p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p><b>Paramètres</b></p> <p>Taille <input type="text" value="8"/> car. <input type="text" value="Prefix"/></p> <p>Décalage <input type="text" value="0"/> car. <input type="text" value="Suffix"/></p> <p>Inversé <input type="checkbox"/></p> </div> <p>Donnée lue jusqu'à Suffix : 2C569E26            Application de l'Offset à 0, donnée : 2C569E26            Application de Len à 8, donnée : 2C569E26            ID valide            Remontée = 0x2C569E26 en Wiegand            743874086 en ISO</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <p style="text-align: right; margin: 0;">Format du code matriciel actuellement configuré <span style="float: right;">Décimal</span></p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p><b>Paramètres</b></p> <p>Taille <input type="text" value="8"/> car. <input type="text" value="Prefix"/></p> <p>Décalage <input type="text" value="0"/> car. <input type="text" value="Suffix"/></p> <p>Inversé <input type="checkbox"/></p> </div> <p>Donnée lue jusqu'à Suffix : 2C569E26            Application de l'Offset à 0, donnée : 2C569E26            Application de Len à 8, donnée : 2C569E26            ID rejeté car format décimal sélectionné</p> </div>
<p>Nombre: GABRIEL GRANADOS CHAVEZ            Num. Colab: 2002</p>	
<div style="border: 1px solid #ccc; padding: 5px;"> <p style="text-align: right; margin: 0;">Format du code matriciel actuellement configuré <span style="float: right;">Décimal</span></p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p><b>Paramètres</b></p> <p>Taille <input type="text" value="4"/> car. <input type="text" value="Num.Colab:  "/></p> <p>Décalage <input type="text" value="0"/> car. <input type="text" value="Suffix"/></p> <p>Inversé <input type="checkbox"/></p> </div> <p>Donnée après Prefix avec un espace : 2002            Application de l'Offset à 0, donnée : 2002            Application de Len à 4, donnée : 2002            ID valide            Remontée = 0x07D2 en Wiegand            2002 en ISO</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <p style="text-align: right; margin: 0;">Format du code matriciel actuellement configuré <span style="float: right;">Décimal</span></p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p><b>Paramètres</b></p> <p>Taille <input type="text" value="12"/> car. <input type="text" value="Prefix"/></p> <p>Décalage <input type="text" value="0"/> car. <input type="text" value="-visitapp"/></p> <p>Inversé <input type="checkbox"/></p> </div> <p>Donnée lue jusqu'à Suffix : 548704361841            Application de l'Offset à 0, donnée : 548704361841            Application de Len à 12, donnée : 548704361841            ID valide            Remontée = 0x7FC1541D71 en Wiegand            548704361841 en ISO</p> </div>

### III. 17 - Application Multiservices Citoyenne (AMC) : paramètres *Nouveau 3.6*

Assistant SCB

**Paramètres AMC (Application Multi-services Citoyenne)**



Sélection du type AMC Spécifique Grand Lyon

**Paramètres**

Taille	<input type="text" value="5"/>	<input checked="" type="checkbox"/> Filtre PIDScopeID <small>(i)</small>	AID
			<input type="text" value="080093F0D057"/>
Décalage	<input type="text" value="0"/>	<input checked="" type="checkbox"/> Filtre PIDIssuerRefer <small>(i)</small>	
Reverse	<input type="checkbox"/>	<input type="text" value="0000"/>	
Secteur d'activité	<input type="text" value="53"/>		
Business sector	<input type="text" value="1 - Fiscalité"/>		

**Sécurité**

Vérification de la clé

La norme Application Multi-services Citoyenne (AMC) décrit un cadre technique pour la gestion de services dans les territoires (collectivités territoriales, universités...) en utilisant un support unique (carte, mobile).

**Vous trouverez toutes les informations utiles sur le site : <https://www.adcet.com/fr/>**

Remarque : Lorsque le type AMC est activé, le lecteur ne remonte plus le numéro PUPI des badges ISOB, même si le type ISOB est activé dans SECARD.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP

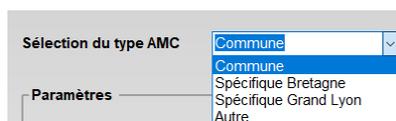


Création badges



Outils

## ❖ Sélection du type AMC



Le système permet une auto configuration sur un ServiceScopeID existant ou une saisie manuelle des informations nécessaires à la lecture de l'identifiant.

L'application AMC désigne l'ensemble des données contenues dans le support pour gérer un groupe de services, ainsi que les ressources fournies par ce support pour la gestion de ces données (fichiers, mécanismes de sécurité, etc.).

Les structures de fichiers AMC peuvent être « communes » ou spécifiques.

## ❖ AID (Application Identifier) AMC

Tableau des AID enregistrés :

AMC	AID
Commune	08009301
Bretagne	30059381
Grand Lyon	080093F0D057
Autre	aaaa bbbb [cccc]

Le champ cccc est optionnel

Pour les AID spécifiques non enregistrés, il est recommandé d'être conforme à la norme ISO/IEC 7816-5 afin d'éviter les conflits d'AID.

## ❖ Filtre PIDScopeID

Trois octets définissant la valeur du Périmètre de service (ServiceScopeID). Les valeurs sont indiquées sur le site ADCET. Pour la France, ajouter 0x250 devant.

AMC	PIDScopeID
Commune	0x 250E00
Bretagne	0x 250908
Grand Lyon	0x 250057
Autre	0xdddddd

Territoire ou Société / Region or company	Date enregistrement / Date of recording	Ref du Périmètre de service / service area	Périmètre de service / Service area
Atoumod-Normandie	14.02.2017	912	Normandie
Bretagne	24.03.2015	908	Bretagne
ADCET	05.01.2017	800	AMC commune
Grand Lyon	17.03.2018	057	Grand Lyon
Syral	22.04.2021	057	Rhône



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### ❖ Filtre PIDIssuerRefer

Les données présentes dans une AMC sont inscrites par un « émetteur de données ».

Cet émetteur est identifié par une référence unique, la référence d'émetteur de données ou IssuerReference (2 octets).

<u>Territoire ou Société</u>	<u>PIDIssuerRefer</u>
Grand Lyon	1057
Gemalto	E002
Otipass	E101
ADCET	FEF0
Idemia	E001
Grand Poitiers	1076
Bordeaux Métropole	0033
Paragon-Id	E003
Atoumod-Normandie	1912
Bretagne	00EB
Métropole européenne de Lille	1053
Amiens Métropole	1006
Evreux Portes de Normandie	1047
Grand Avignon	1013
Wizway	E102
Conduent	E103
Calmell	E004
SELP	E005
Mairie de Lille	0053
SMIRT	1377
COMMUNAUTÉ D'AGGLOMÉRATION DE NEVERS	1068
SMTC	1039

### ❖ Secteur d'activités

La structure Predefined IDs d'une AMC commune doit contenir exactement 35 identifiants (PIDCount = 35, total de la structure = 357 octets) de références 1 à 35, et qui correspondent aux secteurs d'activité CNIL et ADCET, puis à des identifiants RFU.

L'authentification de la structure de données Predefined IDs est réalisée par un processus de vérification de signature qui nécessite la lecture de la totalité de la structure. Secteurs des services et position des identifiants pour les AMC, Commune, Bretagne et Grand Lyon :

Secteur	Numéro
Fiscalité	1
Travail et social	2
Santé	3
Transports	4
Etat civil et citoyenneté	5
Relations avec les élus	6
Prestations scolaires et périscolaires, activités sportives et socioculturelles	7
Economie et urbanisme	8
Polices spéciales et voirie	9
Relations avec les usagers	10
Service agents (non défini par la CNIL)	11



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



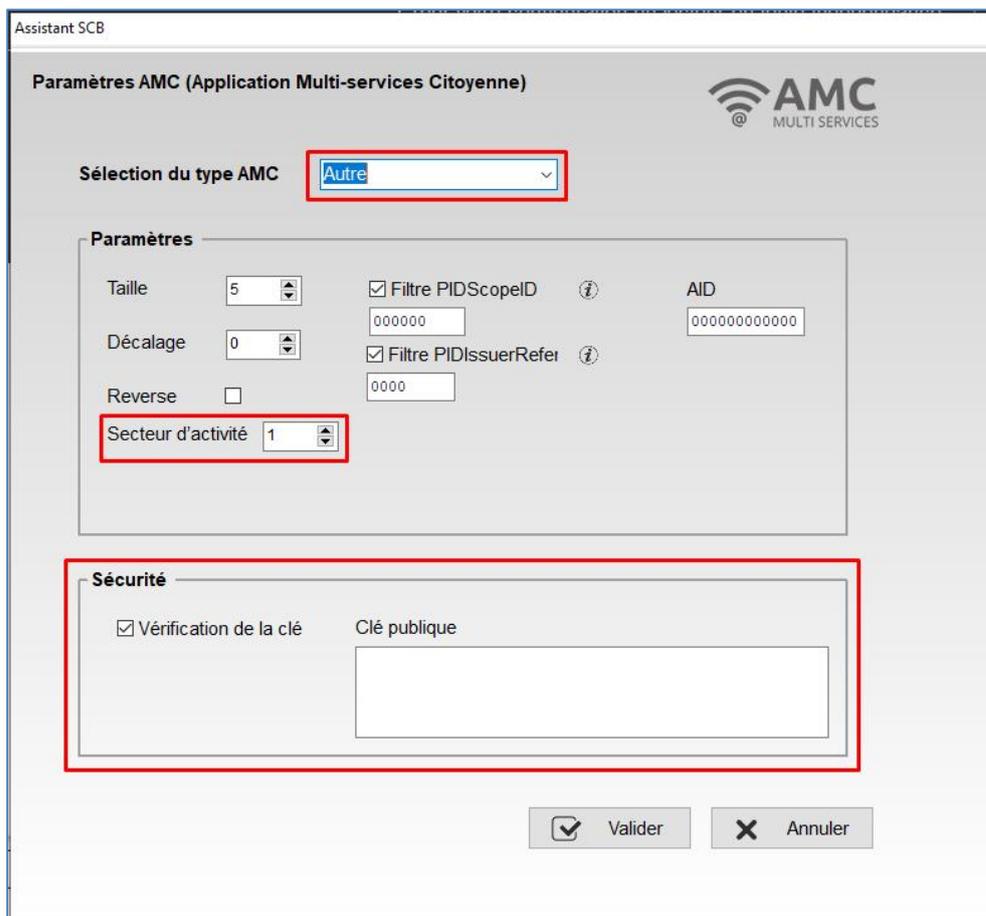
Outils

## ❖ Sécurité

Validation de la signature.

Pour les AMC, Commune, Bretagne et Gran Lyon, la clé publique est connue, par contre pour AMC autre la clé publique doit-être renseigner le champ.

Pour AMC autre, sélectionner un numéro de Secteur d'activité et renseigner la clé publique.



- ❖ Taille : Détermine la longueur de l'identifiant.
- ❖ Décalage : Définit 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).



Accueil



Paramètres



Configuration  
lecteur



SCB / OCB



SKB



BCC



SSCP



Création  
badges



Outils

## Exemple avec badge Korrigo

Assistant SCB

Paramètres AMC (Application Multi-services Citoyenne) 

Sélection du type AMC

**Paramètres**

Taille	<input type="text" value="6"/>	<input checked="" type="checkbox"/> Filtre PIDScopeID 	AID
Décalage	<input type="text" value="0"/>	<input type="text" value="250908"/>	<input type="text" value="30059381"/>
Reverse	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filtre PIDIssuerRefer 	
Secteur d'activité	<input type="text" value="7"/>	<input type="text" value="00EB"/>	
Business sector	<input type="text" value="7 - Prestations scolaires et périscolaires, activités sportives et socioculturelles"/>		

**Sécurité**

Vérification de la clé

ID distribué par le lecteur : **00EBE4F8C7D8**



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### III. 18 - NFC-HCE : paramètres

Voir la [compatibilité Blue/NFC Mobile ID et NFC-HCE](#).

SCB wizard

**Paramètres NFC-HCE**



**Données**

Type d'algorithme ▼  
Select File, FID et Read Binary

AID F053546964 ☾

FID ID 51BC      Taille 5 ▼

Déclage 0 ▼       Inversé

Access ID 000000000000

Valider
 Annuler

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.**

ISO14443-3B PUPI

Autorisé



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



Création badges



Outils

❖ **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 : xxxxxxxxxxx9000                    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



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

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

La commande à implémenter dans l'application est :

- SELECT FILE 0xAID (DESFIRE ISO FILE):

command APDU : 00A40400Size<sub>AID</sub>AID

**Size<sub>AID</sub>**: 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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### III. 19 - NFC-HCE : Clés

Voir la [compatibilité Blue/NFC Mobile ID et NFC-HCE](#)

SCB wizard

NFC-HCE keys



Garder la maîtrise de votre sécurité.  
Définir/modifier votre clé.

**Confidentialité**

Signature      Clé     

Clé de lecture HCE

Valider       Annuler

➤ **Signature**

Signature

l'ID HCE est envoyé en mode clair (défaut)

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'algorithme Orange™ Pack ID  
Clé secrète de la zone Access ID définie dans paramètres.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### III. 20 - CPS3 : paramètres

SCB wizard

  
*carte de professionnel de santé*

**Mode de lecture**

UID

ID Privé

**Données**

Numéro de série  
Fichier Elémentaire

Taille

Décalage

MSB First

Valider     Annuler

#### 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.

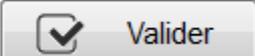
L'Id privé correspond à l'Identifiant Technique (N° de série IAS), c'est un numéro sur 19 digits constitué comme suit :

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

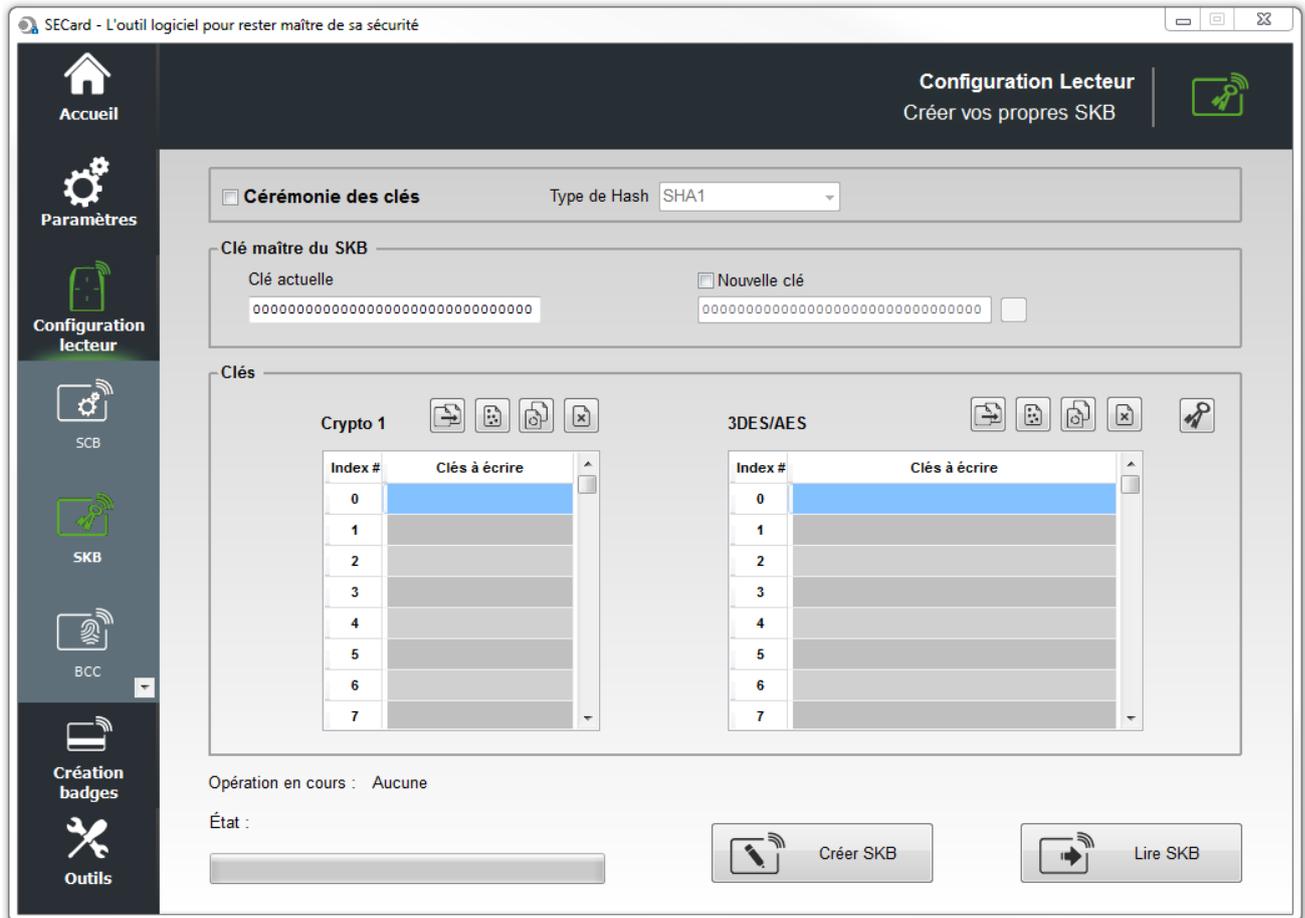
Sa valeur est présente dans le Fichier Elémentaire D003.

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.

## 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–<br>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             |

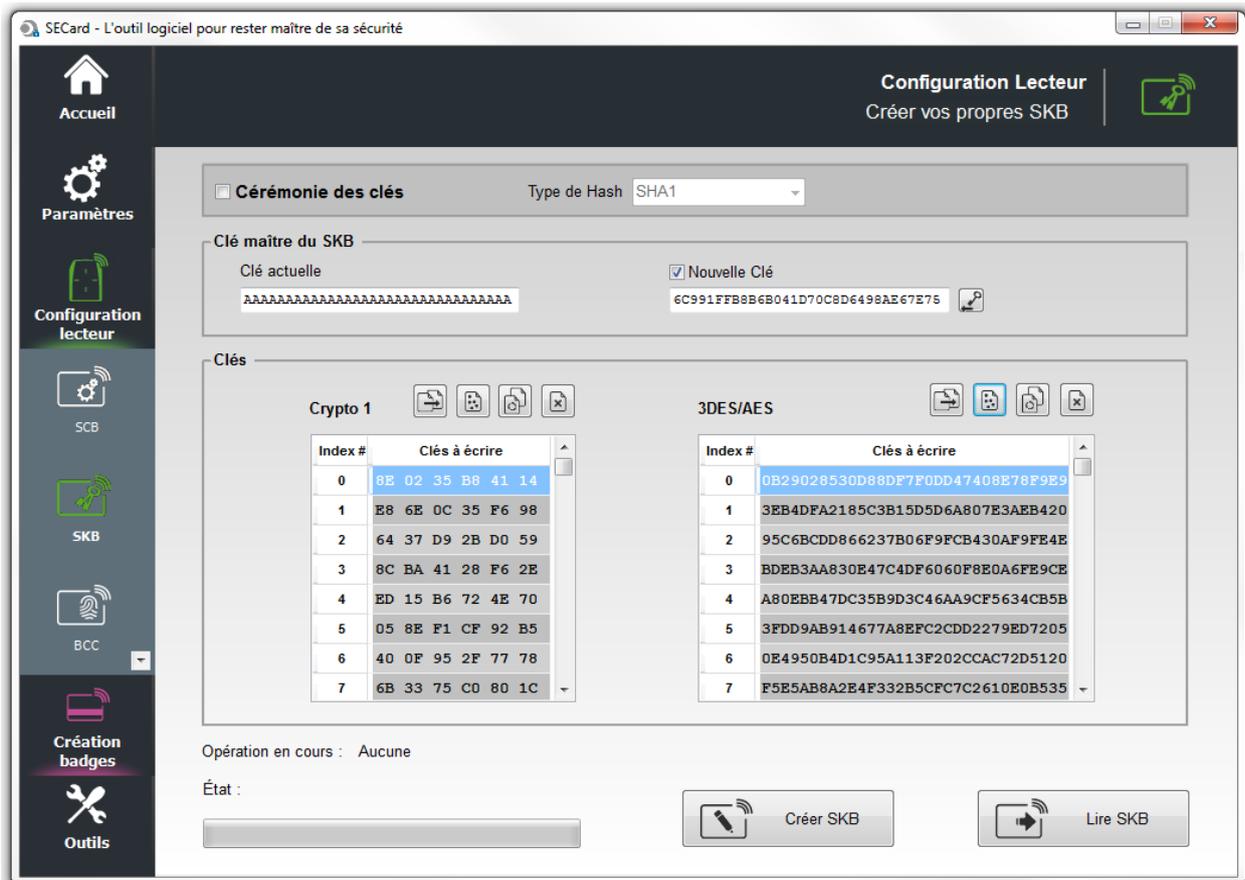
Leur fonction est de fournir un portefeuille de clés indexées (de 0 à 31 *Crypto1* et *3DES/AES*). Une fois sauvegardées en EEPROM par le lecteur, il sera possible de les utiliser en les appelants dans les commandes *SSCP*® par leur numéro d'index. Le but étant de ne plus faire transiter les valeurs 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® EVx ou un badge « SKB » existant.

## IV.1 - Création en mode classique



### Clé maître du SKB

Sur un badge MIFARE® DESFire® EVx 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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

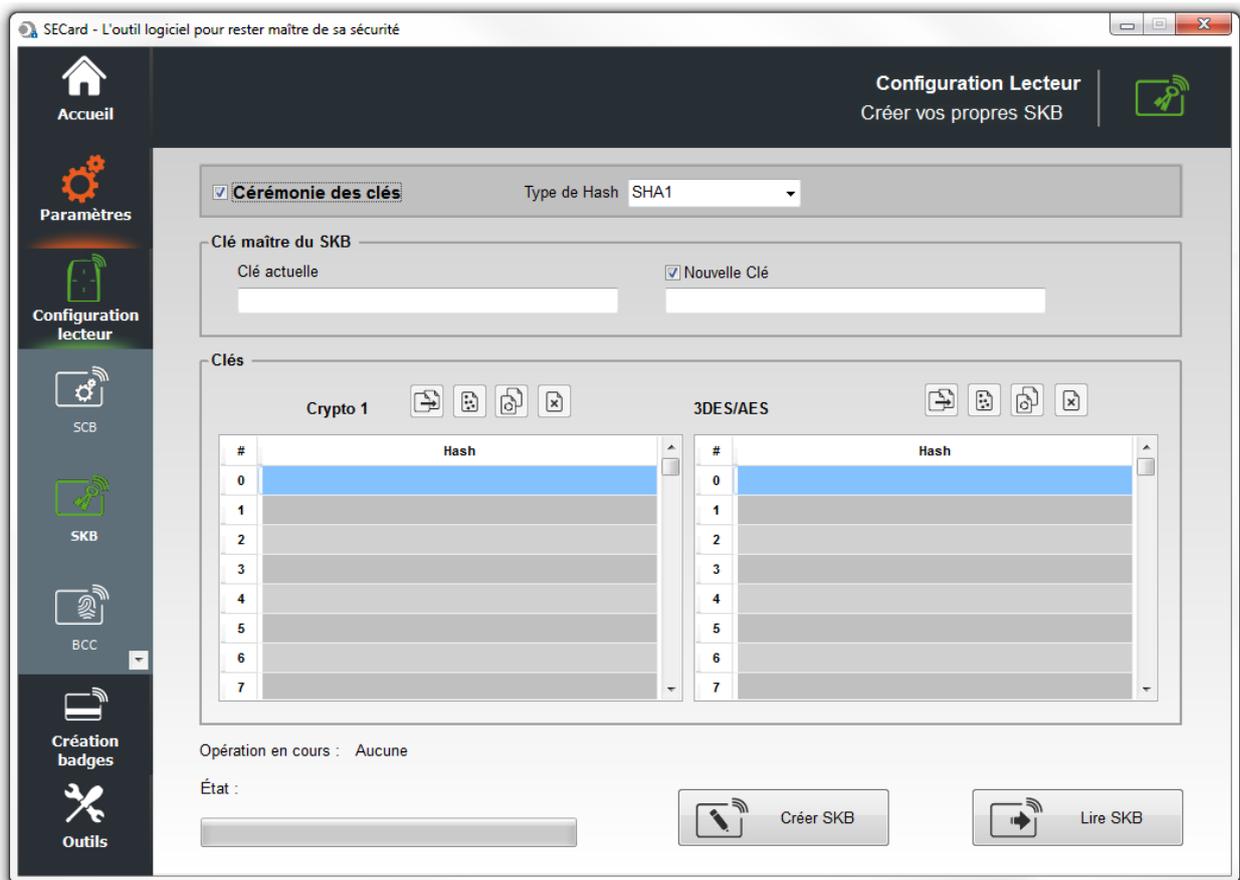
## IV.2 - Création en mode « Cérémonie des clés »

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.

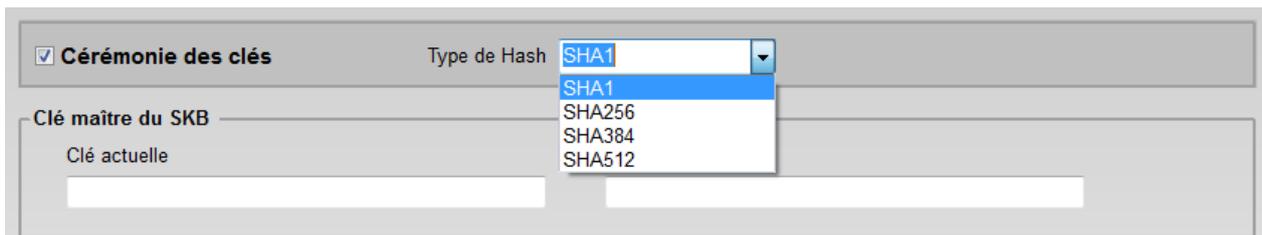
Chaque clé sera le résultat d'un XOR sur les trois clés saisies par les détenteurs. Les valeurs apparaissant dans les champs sont le Hash de ce résultat.

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





Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP

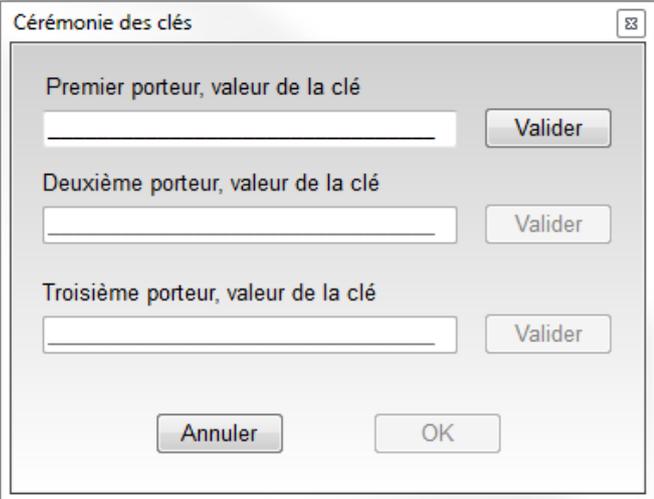


Création badges



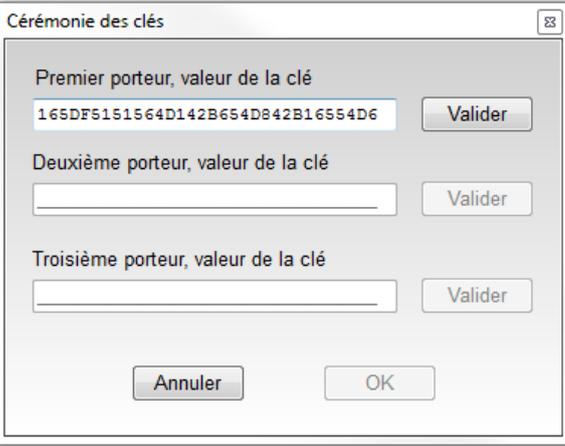
Outils

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

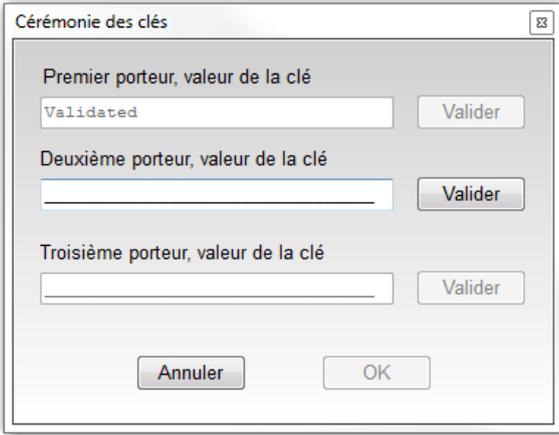


3- Premier porteur

Entrer la valeur de la première clé



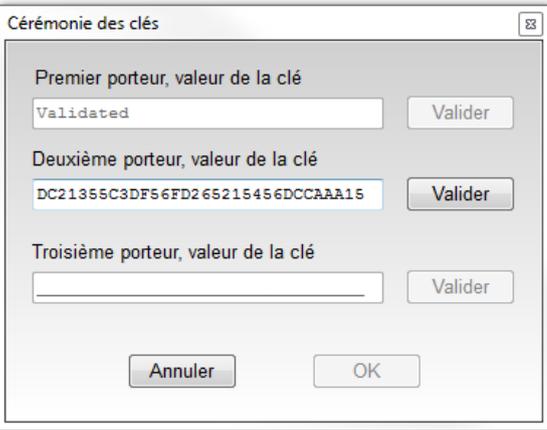
Cliquer sur Valider



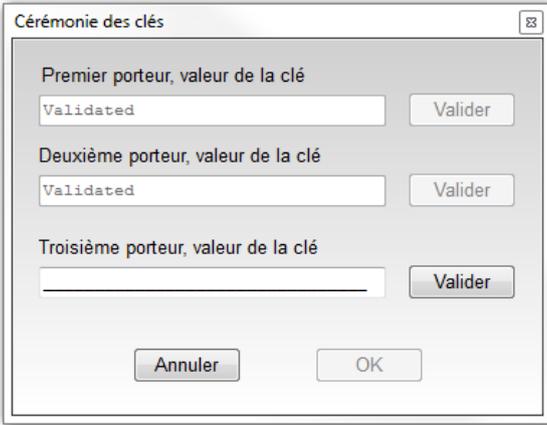
La valeur de la première clé est maintenant masquée.

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**

**Cérémonie des clés**

Premier porteur, valeur de la clé  
Validated Valider

Deuxième porteur, valeur de la clé  
Validated Valider

Troisième porteur, valeur de la clé  
AAFDf554DFAED415C16DF54D16DF5462 Valider

Annuler OK

**Cliquer sur Valider**

**Cérémonie des clés**

Premier porteur, valeur de la clé  
Validated Valider

Deuxième porteur, valeur de la clé  
Validated Valider

Troisième porteur, valeur de la clé  
Validated Valider

Annuler OK

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

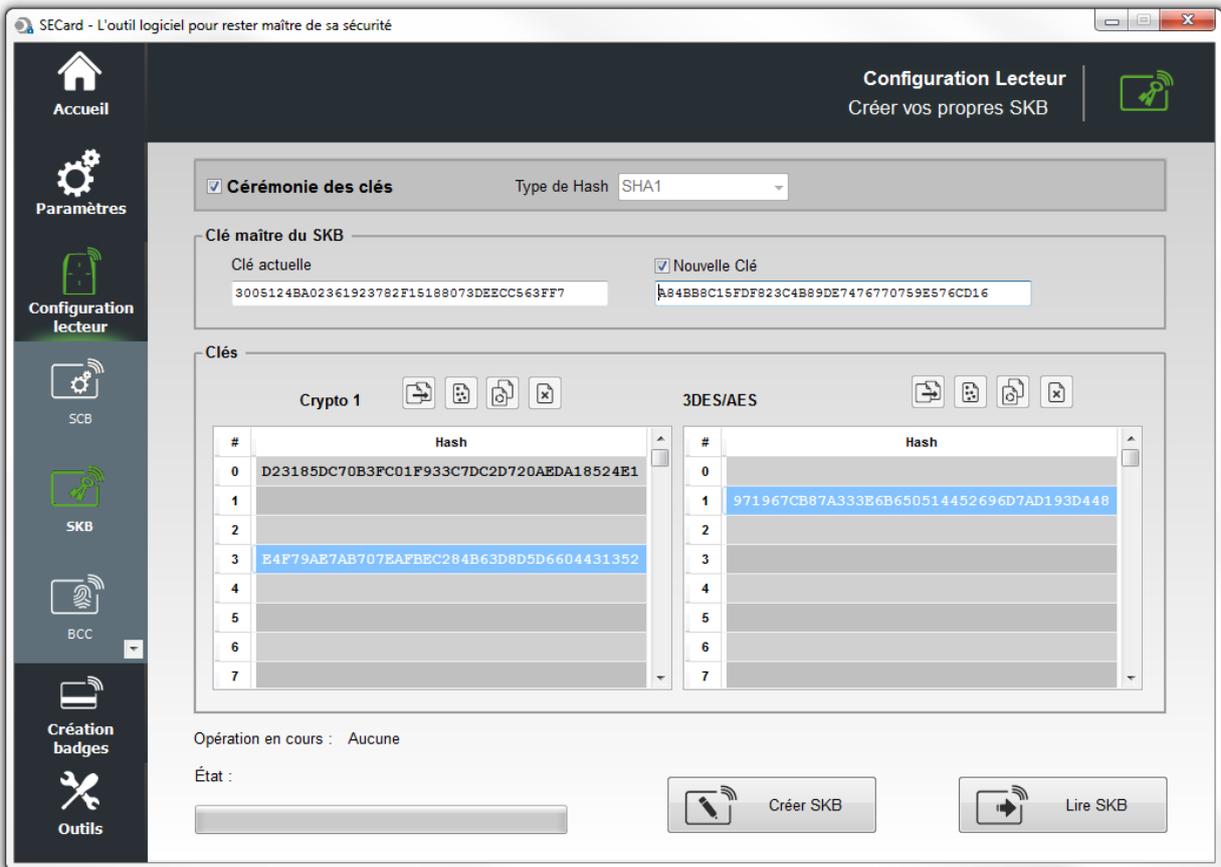
6- Cliquer sur « OK » pour terminer la cérémonie de clés pour la clé maître du badge SKB.

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

The screenshot shows the SECard software interface. The main window is titled "SECard - L'outil logiciel pour rester maître de sa sécurité". On the left, there is a navigation menu with icons for Accueil, Paramètres, Configuration lecteur, SCB, SKB, BCC, and Outils. The main area shows the "Cérémonie des clés" window with "Type de Hash" set to "SHA1". The "Clé maître du SKB" section shows the "Clé actuelle" as "8005124BA02361923782F15188073DEECC563FF7" and the "Nouvelle Clé" field is empty. Below this, there are two tables for "Clés": "Crypto 1" and "3DES/AES". Both tables have columns for "#", "Hash", and a set of icons (copy, paste, print, delete). The "Crypto 1" table has 8 rows (0-7), with row 0 highlighted. The "3DES/AES" table also has 8 rows (0-7), with row 0 highlighted. At the bottom, it says "Opération en cours : Aucune" and "État :". There are two buttons: "Créer SKB" and "Lire 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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



SSCP



Création badges



Outils

### 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.

**Assigner les clés indexées** ✖

Nom des clés	Index clé SKB
Clé maître actuelle du SCB	
Nouvelle clé maître du SCB	
Clé actuelle de la signature série	
Nouvelle clé de la signature série	
Clé actuelle du chiffrement série	
Nouvelle clé du chiffrement série	
Clé actuelle du EasySecure/Wiegand	
Nouvelle clé du EasySecure/Wiegand	
Clé de signature du DUPUSO14443 2B	

Désactiver les fenêtres des clés  
 Cacher les valeurs des clés

**Assigner**

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 :

**Clé entreprise SCB**

Actuelle  Nouvelle

FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
00000000000000000000000000000000

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

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

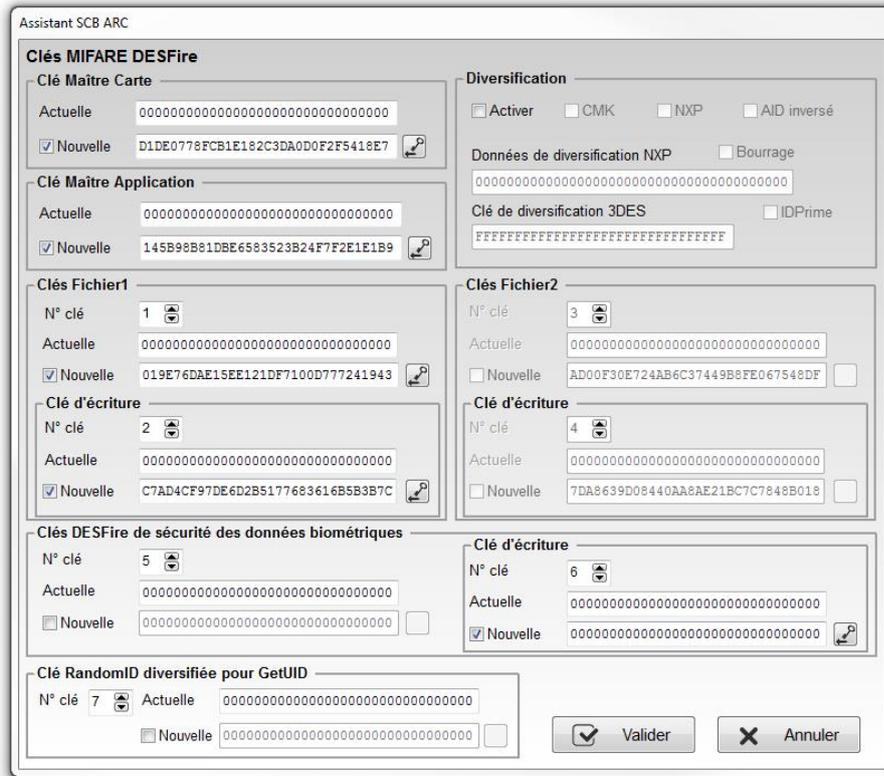
Valider

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

Nom des clés	Index clé SKB
Clé AMK actuelle de la DESFire	
Nouvelle clé AMK de la DESFire	3
Clé de diversification 3DES de la DESFire	
Clé RW actuelle du FID1 de la DESFire	
Nouvelle clé RW du FID1 de la DESFire	4
Clé W actuelle du FID1 de la DESFire	
Nouvelle clé W du FID1 de la DESFire	5
Clé RW actuelle du FID2 de la DESFire	
Nouvelle clé RW du FID2 de la DESFire	

- 3- Cliquer sur le bouton Assigner

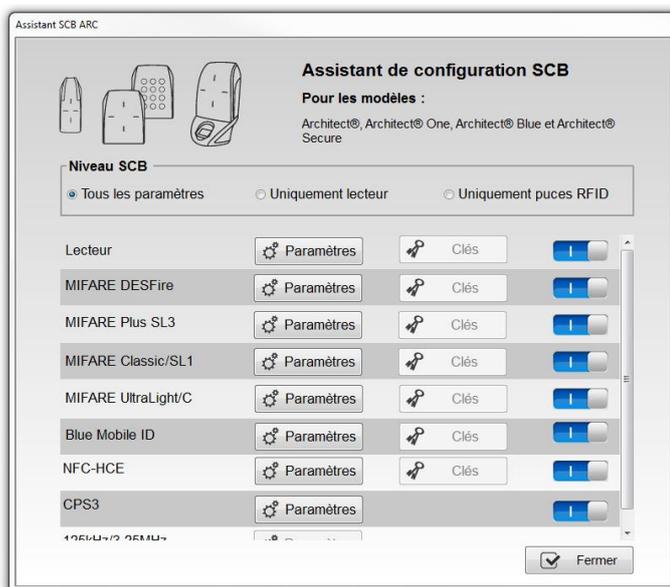
- 4- Si les cases « Désactiver les fenêtres des clés » et « Cacher les valeurs des clés » n'étaient pas cochées lors de l'assignation, la fenêtre de clés DESFire sera :



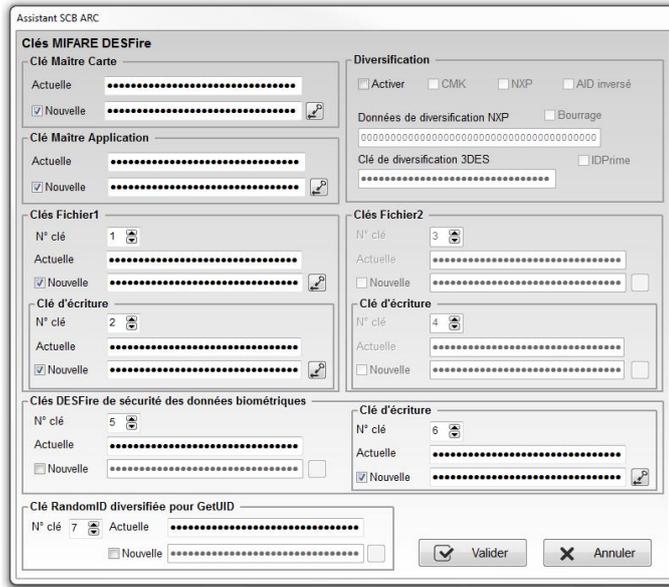
La valeur des clés apparaît dans les champs conformément aux valeurs des clés indexées.

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 :



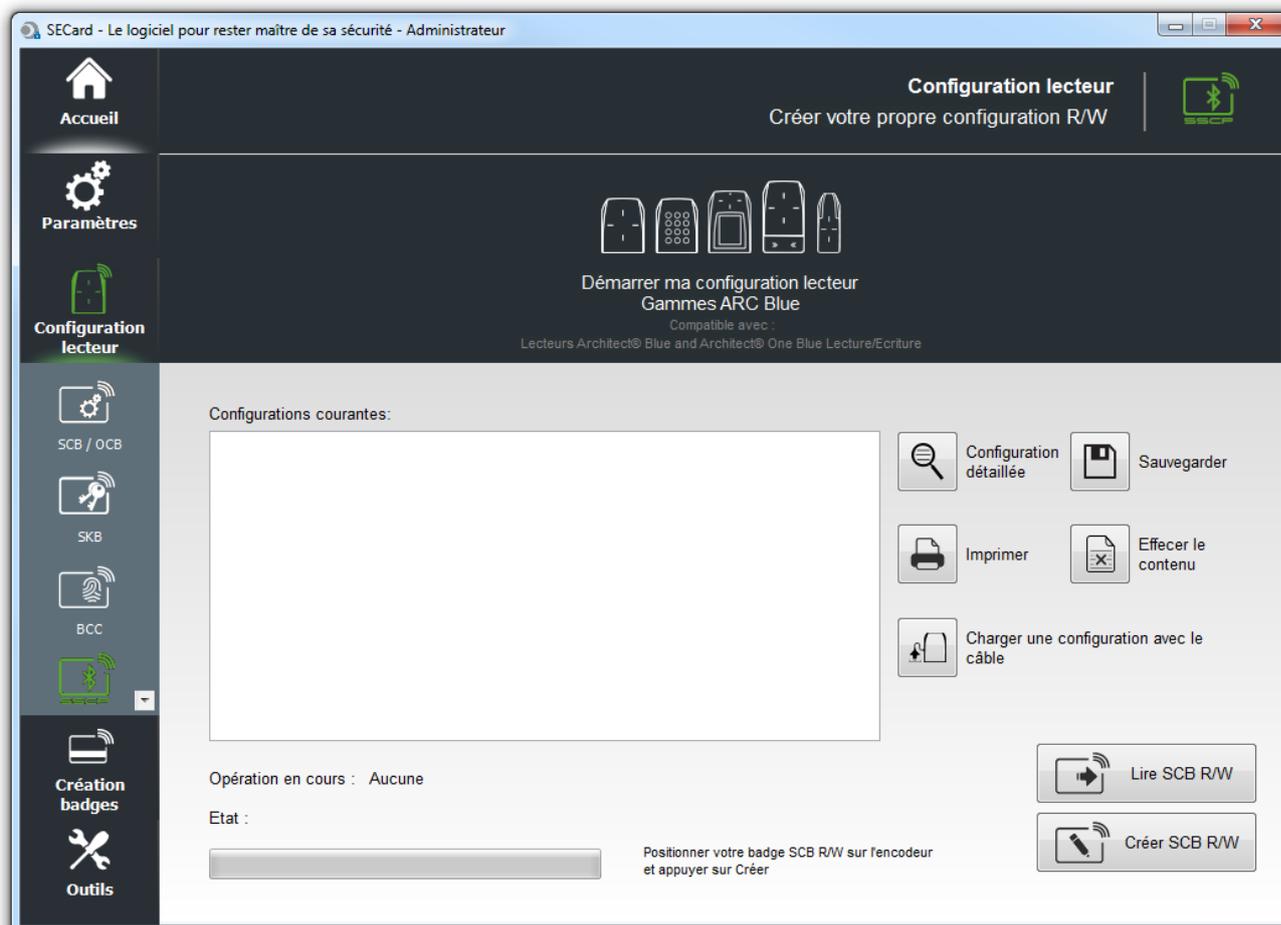
Remarque : Il est possible de modifier un index, ou les options « Désactiver les fenêtres des clés », « Cacher les valeurs des clés » en effectuant la modification et en cliquant à nouveau sur Assigner.

### 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 - SCB R/W

Le SCB R/W est un badge de configuration pour les lecteurs ARC R/W Bluetooth®, il permet de configurer le Blue/NFC de ces lecteurs.



<p>Démarrer ma configuration lecteur Gammes ARC Blue Compatible avec : Lecteurs Architect® Blue and Architect® One Blue Lecture/Ecriture</p>	<p>Permet d'ouvrir l'assistant de configuration pour les lecteurs</p>
	<p>Permet d'imprimer les informations de configuration contenues dans la fenêtre.</p>
	<p>Permet de sauvegarder les informations de configuration contenues dans la fenêtre dans un fichier .rtf.</p>
	<p>Permet d'effacer les informations de configuration contenues dans la fenêtre.</p>
	<p>Permet d'afficher les informations détaillées des configurations courantes.</p>
	<p>Permet de charger la configuration dans le lecteur par la communication série.</p>
	<p>Permet de lire un badge de configuration SCB R/W. Utilise la clé entreprise SCB R/W définie dans l'assistant de configuration.</p>
	<p>Permet de créer un badge de configuration SCB R/W selon les paramètres définis dans l'assistant de configuration.</p>



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



Création badges

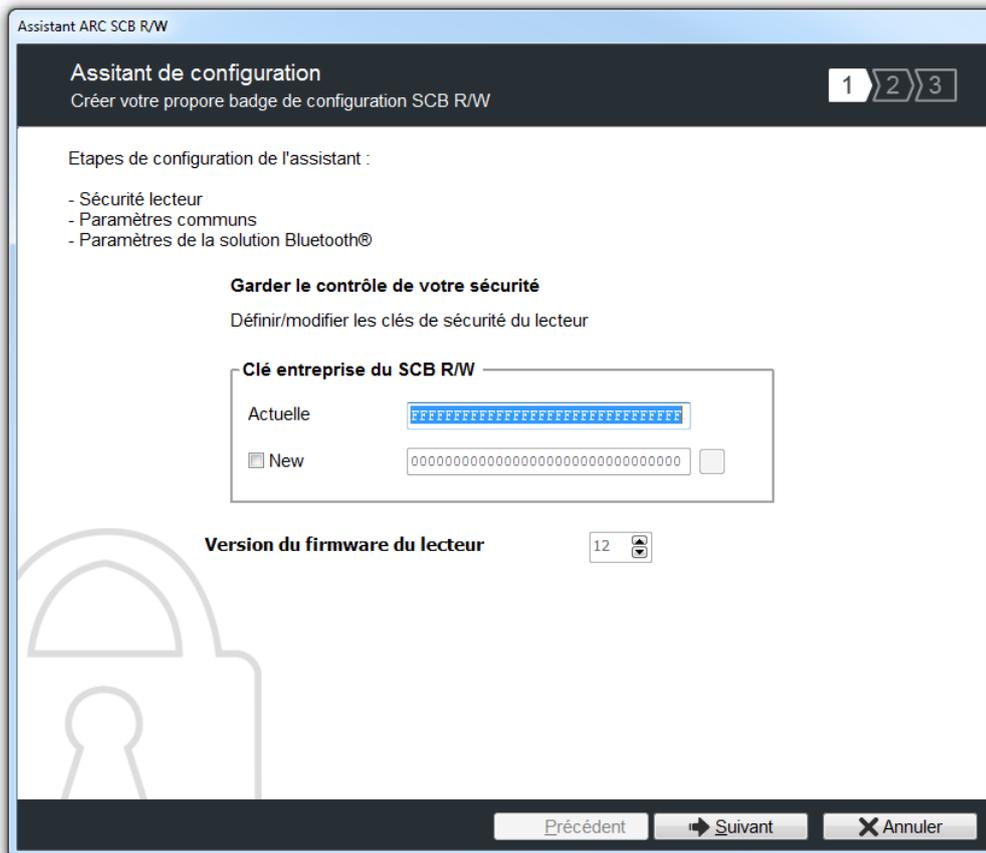


Outils

## VI.1 – Assistant de configuration

La configuration du lecteur se fait en trois étapes, pour passer d'une étape à l'autre il faut cliquer sur « Suivant ».

<a href="#">Click here</a>	Sécurité du lecteur
<a href="#">Click here</a>	Paramètres communs
<a href="#">Click here</a>	Paramètres STid Mobile ID®
<a href="#">Click here</a>	Paramètres Orange™ Pack ID
<a href="#">Click here</a>	Paramètres Open Mobile Protocol



### Clé entreprise SCB R/W

Les lecteurs configurables par les badges SCB R/W sont livrés initialement avec une configuration par défaut (clé usine 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF).

Ceux-ci pourront donc être configurés par un SCB R/W de clé courante 0xFF...FF vers une nouvelle clé entreprise.

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

#### Attention

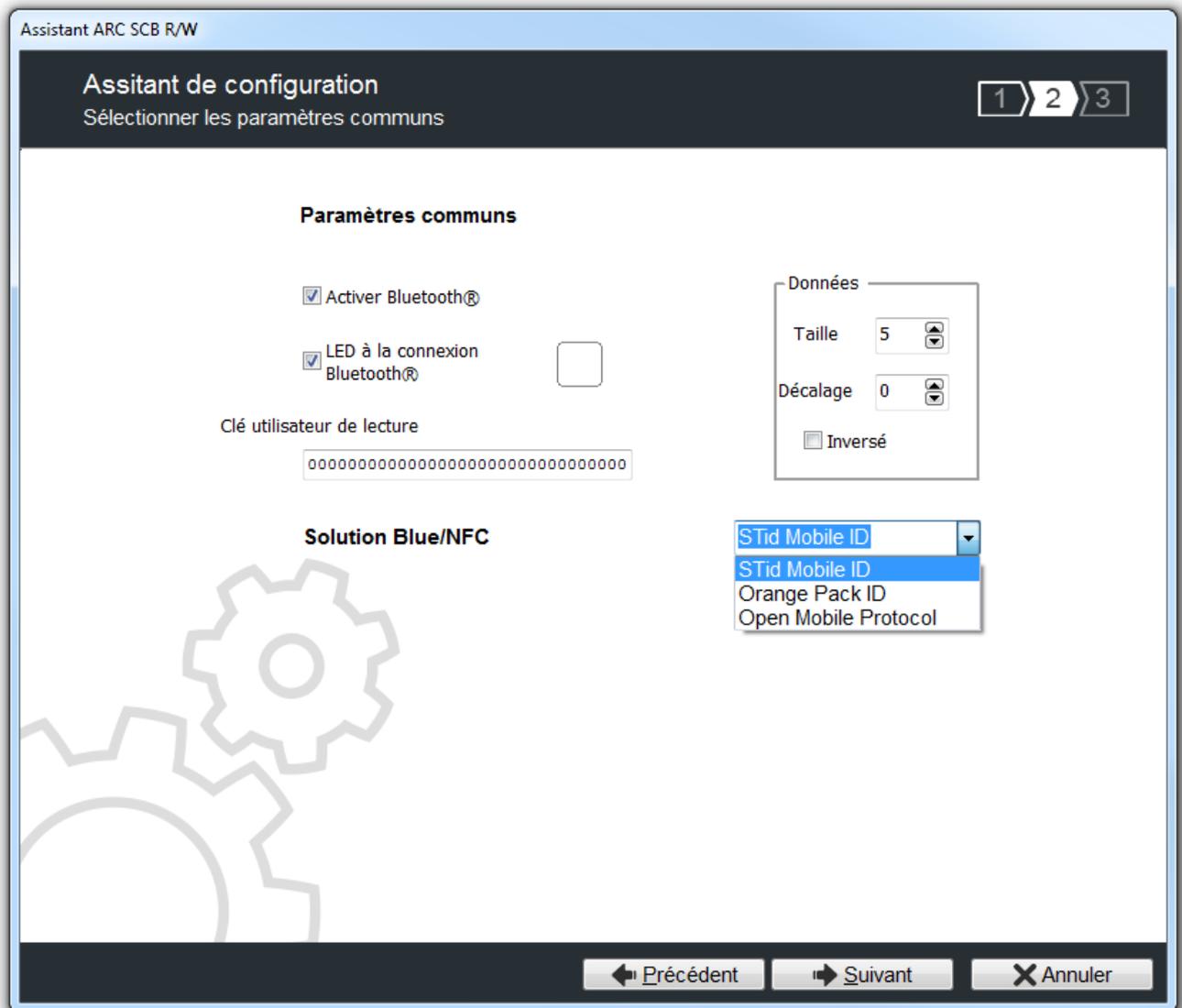
Cette clé est importante et doit absolument être connue de l'administrateur. Elle protège les données du « SCB R/W » et permet des modifications sur la configuration des lecteurs.

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

### Version du firmware du lecteur

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

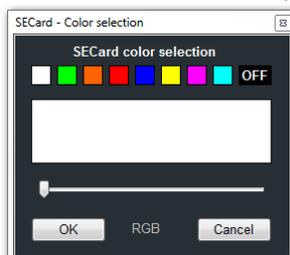
- Accueil
- Paramètres
- Configuration lecteur
- SCB / OCB
- SKB
- BCC
- Création badges
- Outils



**Activer Bluetooth®** : Active/ désactive la solution STid Mobile ID® ou Orange™ Pack ID ou Open Mobile Procol (Blue et le NFC) Quand cette option est désactivée il n’y a pas d’émission d’ondes Bluetooth®.

**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.

**Clé utilisateur de lecture** : Permet de définir la clé de lecture utilisées pour les données Blue/NFC.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



Création badges



Outils

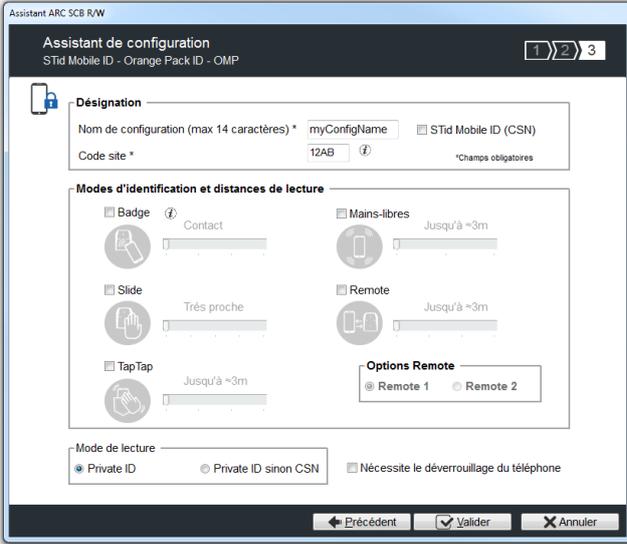
## Données :

- ❖ Taille : Détermine la longueur de l'identifiant.
- ❖ Décalage : Définit 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).

## Solution Blue/NFC :

Configure le lecteur pour lire la solution STidMobile ID® ou Orange™ Pack ID ou Open Mobile Protocol.

Ce choix impacte l'écran de l'assistant de configuration à l'étape 3 :



Assistant ARC SCB R/W  
Assistant de configuration  
STid Mobile ID - Orange Pack ID - OMP

1 2 3

Désignation  
Nom de configuration (max 14 caractères) \* myConfigName  STid Mobile ID (CSN)  
Code site \* 12AB ⓘ \*Champs obligatoires

Modes d'identification et distances de lecture

Badge ⓘ Contact

Mains-libres Jusqu'à ~3m

Slide Très proche

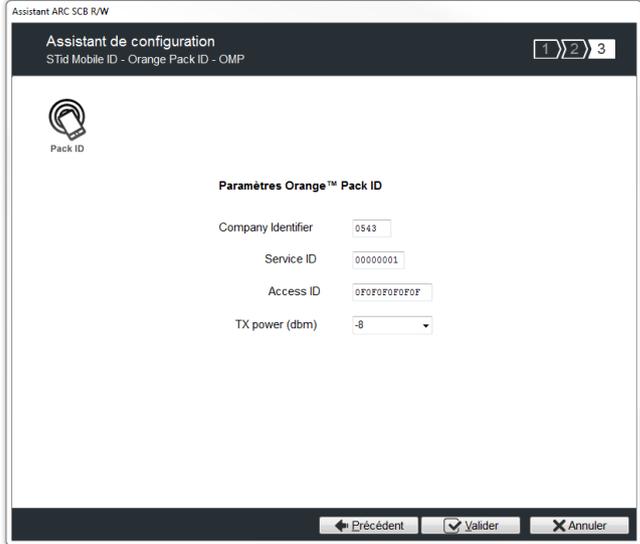
Remote Jusqu'à ~3m

TapTap Jusqu'à ~3m

Options Remote  
 Remote 1  Remote 2

Mode de lecture  
 Private ID  Private ID sinon CSN  Nécessite le déverrouillage du téléphone

← Précédent ✓ Valider ✕ Annuler



Assistant ARC SCB R/W  
Assistant de configuration  
STid Mobile ID - Orange Pack ID - OMP

1 2 3

Pack ID

Paramètres Orange™ Pack ID

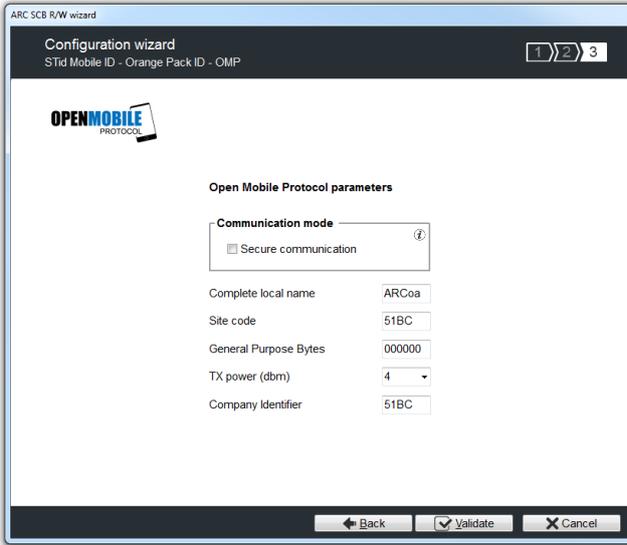
Company Identifier 0543

Service ID 00000001

Access ID 0F0F0F0F0F0F

TX power (dbm) -8

← Précédent ✓ Valider ✕ Annuler



ARC SCB R/W wizard  
Configuration wizard  
STid Mobile ID - Orange Pack ID - OMP

1 2 3

OPENMOBILE PROTOCOL

Open Mobile Protocol parameters

Communication mode ⓘ  
 Secure communication

Complete local name ARCoa

Site code 51BC

General Purpose Bytes 000000

TX power (dbm) 4

Company Identifier 51BC

← Back ✓ Validate ✕ Cancel

### Etape 3 - Mode STid Mobile ID®

Assistant ARC SCB R/W

**Assistant de configuration** STid Mobile ID - Orange Pack ID - OMP

1 2 3

**Désignation**

Nom de configuration (max 14 caractères) \*   STid Mobile ID (CSN)

Code site \*  ⓘ \*Champs obligatoires

**Modes d'identification et distances de lecture**

Badge ⓘ **Contact**  Mains-libres Jusqu'à ≈3m

Slide Très proche  Remote Jusqu'à ≈3m

TapTap Jusqu'à ≈3m

**Options Remote**

Remote 1  Remote 2

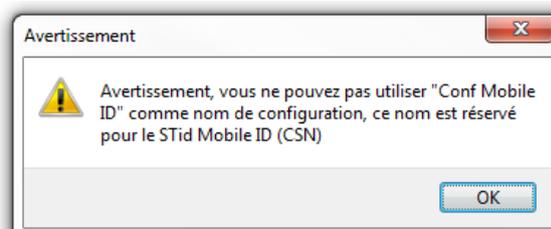
**Mode de lecture**

Private ID  Private ID sinon CSN  Nécessite le déverrouillage du téléphone

← Précédent  Valider X Annuler

### 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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



Création badges



Outils

## 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.

### 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.



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



Création badges



Outils

## Mode de lecture

- ❖ **Mode de lecture : ID privé**  
Lecteur configuré uniquement en lecture de code privé.
- ❖ **Mode de lecture : Id privé sinon CSN**  
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 le CSN.

## 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.

## Etape 3 - Mode Orange™ Pack ID

Assistant ARC SCB R/W

Assistant de configuration  
STid Mobile ID - Orange Pack ID - OMP
1 > 2 > 3



Pack ID

**Paramètres Orange™ Pack ID**

Company Identifier	<input type="text" value="0543"/>
Service ID	<input type="text" value="00000001"/>
Access ID	<input type="text" value="0F0F0F0F0F0F"/>
TX power (dbm)	<input type="text" value="-8"/>

- ❖ **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. (défaut 4 dbm).
  - Valeurs possibles : -16, -12, -8, -4, 0 and 4 dbm.

### Etape 3 - Mode Open Mobile Protocol

Assistant ARC SCB R/W

Assistant de configuration  
STid Mobile ID - Orange Pack ID - OMP

1 2 3

**OPENMOBILE**  
PROTOCOL

**Paramètres Open Mobile Protocol**

**Mode de communication**

Communication sécurisée

Complete local name: ARCoa

Code site: 51BC

Octets génériques: 000000

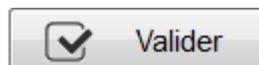
Puissance émise (dbm): 4

Identifiant entreprise: 51BC

← Précédent    ✓ Valider    ✕ Annuler

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

Cliquer sur le bouton  
lecteurs.



pour terminer la configuration des paramètres



Accueil



Paramètres



Configuration lecteur



SCB / OCB



SKB



BCC



Création badges



Outils

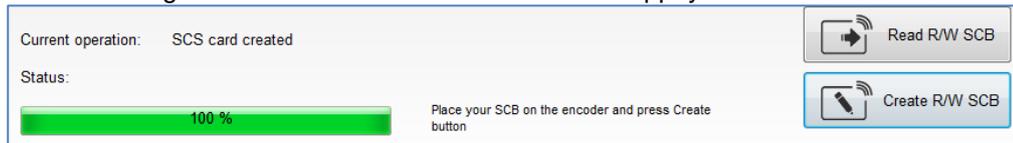
## VI.2 – Création du SCB R/W

Deux possibilités pour charger la configuration dans le lecteur.

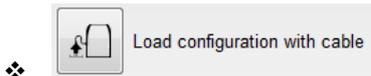


Le badge de configuration SCB R/W peut-être créé sur une puce MIFARE® DESFire® Ev1/ EV2 non verrouillée 4ko et MIFARE® DESFire® Ev1/ EV2 non verrouillée 8ko.

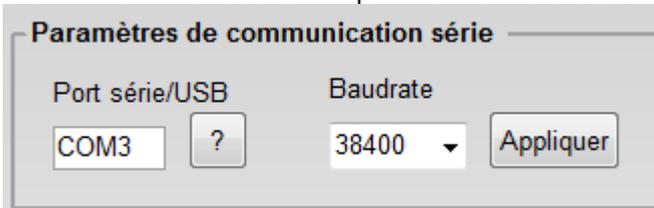
- 1- Poser un badge DESFire® sur l'encodeur SECard et appuyer sur Créer SCB R/W



- 2- Pour charger la configuration dans le lecteur utiliser les commandes SSCP® LoadConf\_X (cf Spec\_Protocole\_5AA-7AA\_MIFARE\_GLOBAL\_V1.17\_FR.pdf)



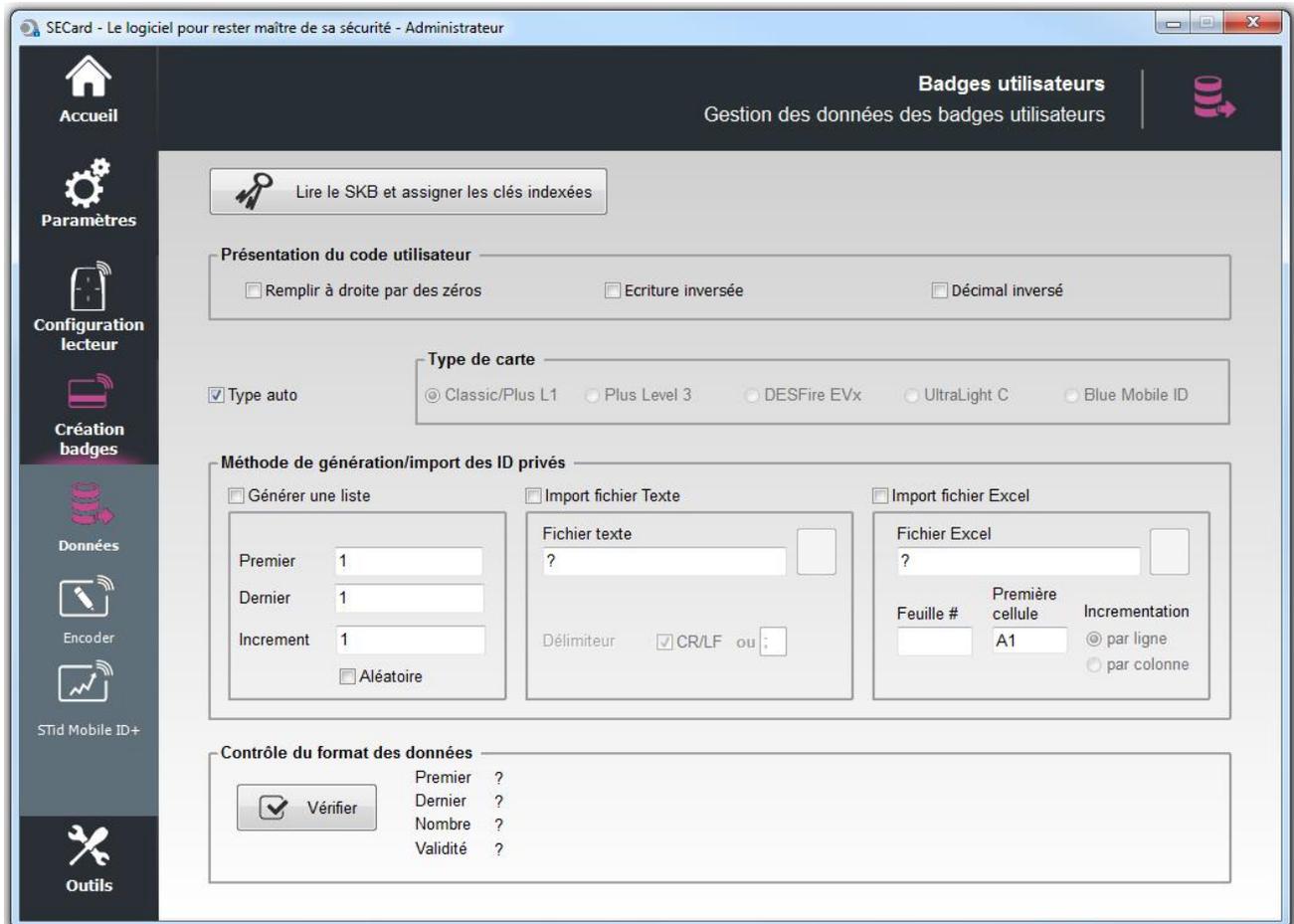
- 1- Connecter le lecteur à configurer au port com du PC.
- 2- Dans les paramètres de communication série ” choisir le numéro de port et la vitesse du lecteur. Le lecteur étant un R/W vous pouvez utiliser CTRL+?



- 3- Appuyer sur le bouton Charger la configuration par câble.

## VI. Création badges

### VII. 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 : 10EFCDA B
- ❖ 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.



Accueil



Paramètres



Configuration lecteur



Création badges



Données



Encoder



STid Mobile ID+



Outils

## 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'incrément 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 :

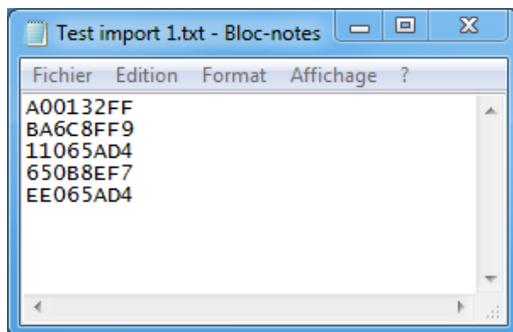
- ✓ La liste aléatoire n'est pas compatible avec le format du Wiegand 26 bits (code site + code carte).
- ✓ Le nombre maximum de valeur aléatoire est 0x7F FF FF FF (soit 2147483647 valeurs).

Avec cette option la valeur encodée n'apparaîtra 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.

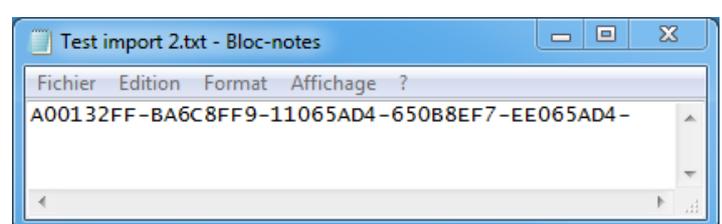
## Import fichier Texte

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)



Accueil



Paramètres



Configuration  
lecteur



Création  
badges



Données



Encoder



STid Mobile ID+



Outils

## 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.

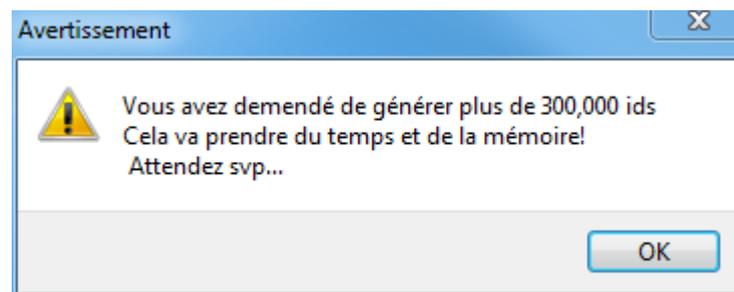
Il est nécessaire que le logiciel Excel® soit installé.

## 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 contenu dans le fichier de configuration .pse.



Accueil



Paramètres



Configuration  
lecteur



Création  
badges



Données



Encoder



STid Mobile ID+



Outils

## Statut

Information ✕

 Badge SKB lu  
Clés SKB assignées

OK

Badge SKB lu

Erreur ✕

 Erreur d'authentification

OK

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.

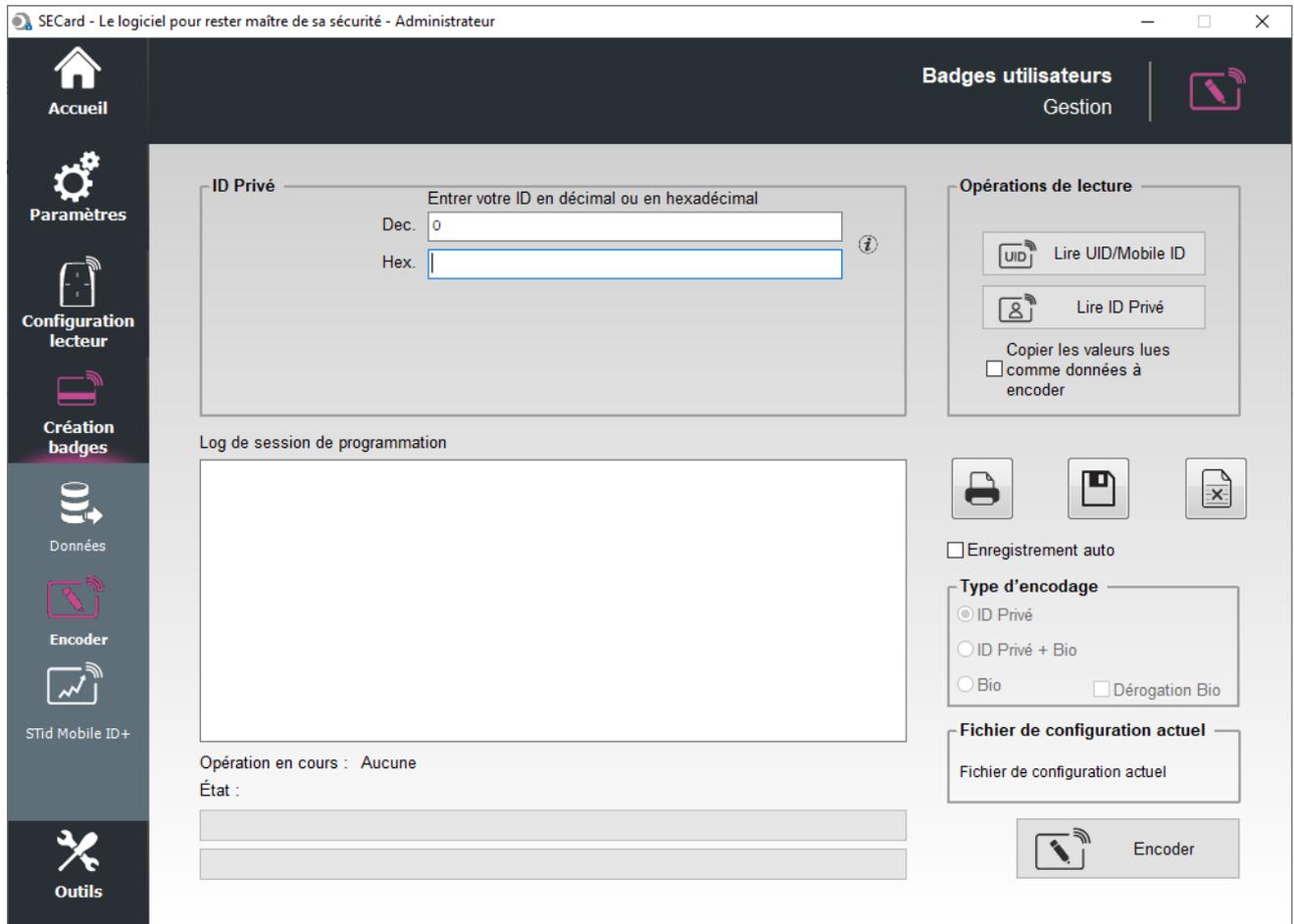
Erreur ✕

 Application pas trouvée

OK

Le badge présenté n'est pas un badge SKB

## VII. 2 – Encoder

SECard - Le logiciel pour rester maître de sa sécurité - Administrateur

Badges utilisateurs Gestion

Accueil

Paramètres

Configuration lecteur

Création badges

Données

Encoder

STid Mobile ID+

Outils

Opérations de lecture

Lire UID/Mobile ID

Lire ID Privé

Copier les valeurs lues comme données à encoder

Log de session de programmation

Opération en cours : Aucune

État :

Type d'encodage

ID Privé

ID Privé + Bio

Bio  Dérogation Bio

Fichier de configuration actuel

Fichier de configuration actuel

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 STid Mobile ID® depuis l'AppStore ou le PlayStore.**





Accueil



Paramètres



Configuration lecteur



Création badges



Données



Encoder

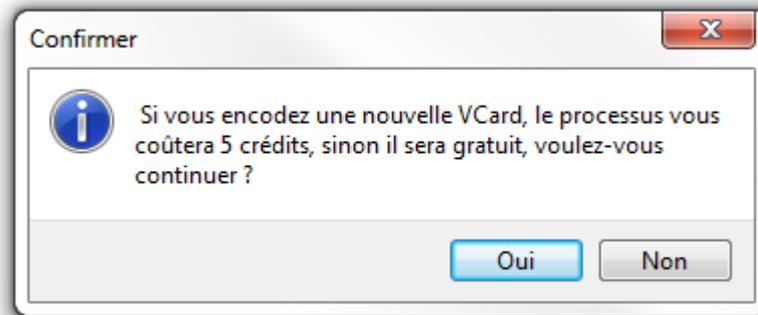


STid Mobile ID+



Outils

## 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

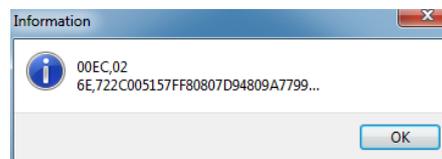
Permet de saisir manuellement la (les) valeur(s) de(s) l'id Privé(s) à encoder.

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

## Opérations de lecture

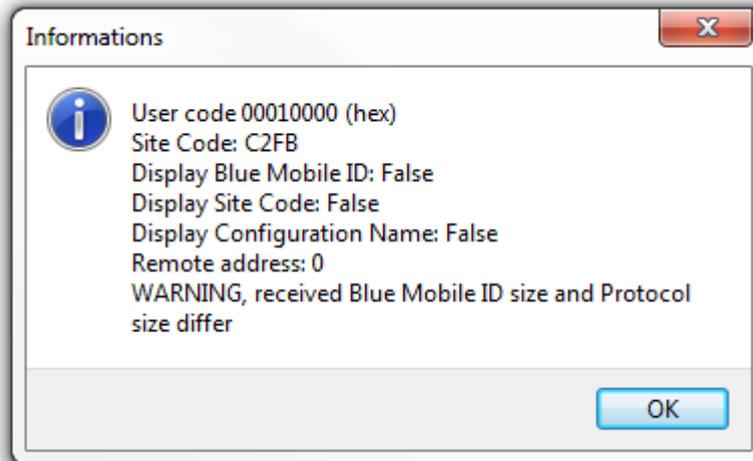
- ❖ Lire UID/ Mobile ID : permet de lire l'UID ainsi que le type de puce de l'identifiant présenté au lecteur.
- ❖ Lire ID Privé : permet de lire le code privé ou les templates de l'identifiant présenté au lecteur selon la configuration en cours et si la case « Copier les valeurs lues comme données à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

Exemple de relecture template :



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

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.



Accueil



Paramètres



Configuration lecteur



Création badges



Données



Encoder



STid Mobile ID+



Outils

## 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...

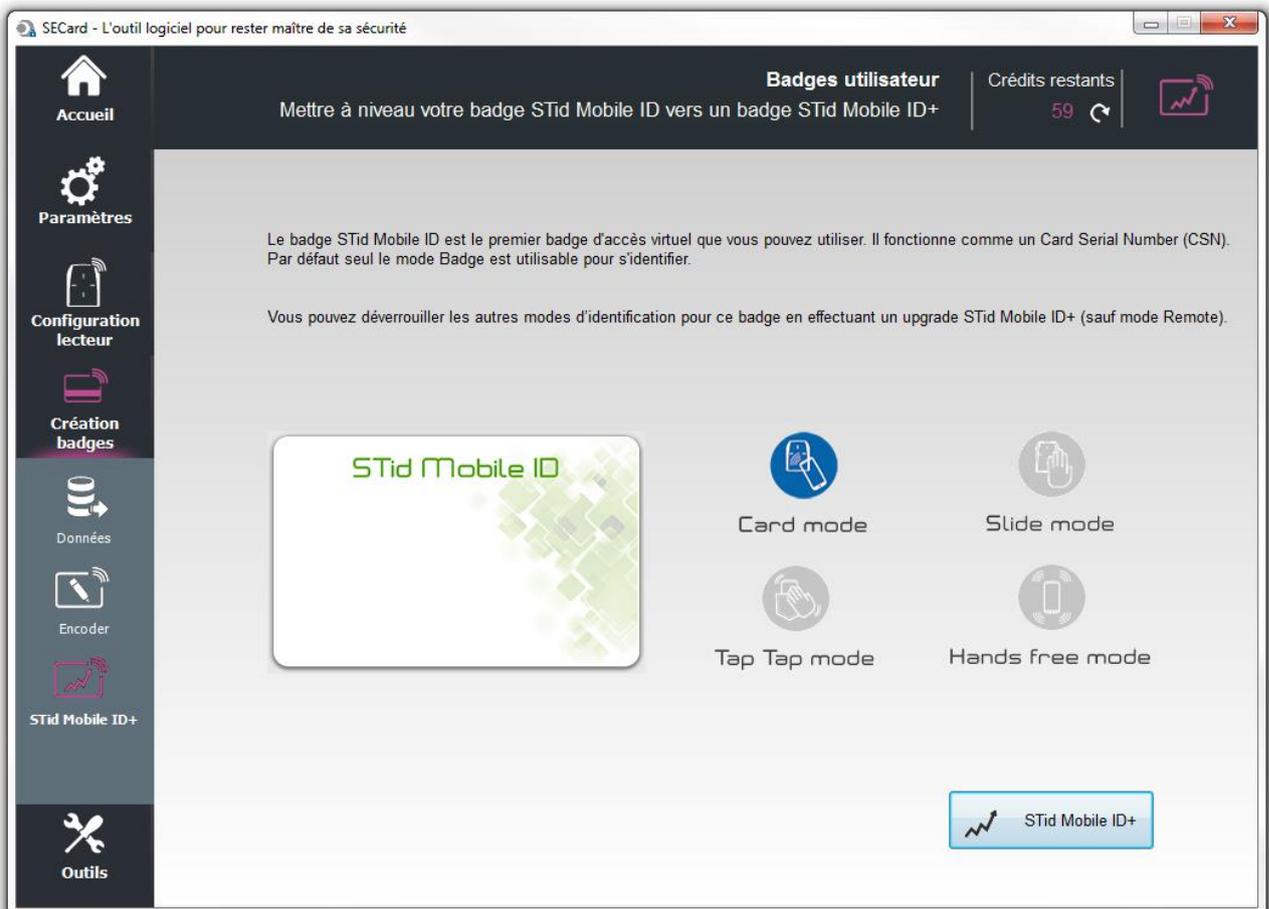
### VII. 3 – STid Mobile ID+

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

**Badges utilisateur** | Crédits restants: 59

Mettre à niveau votre badge STid Mobile ID vers un badge STid Mobile ID+

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 +**

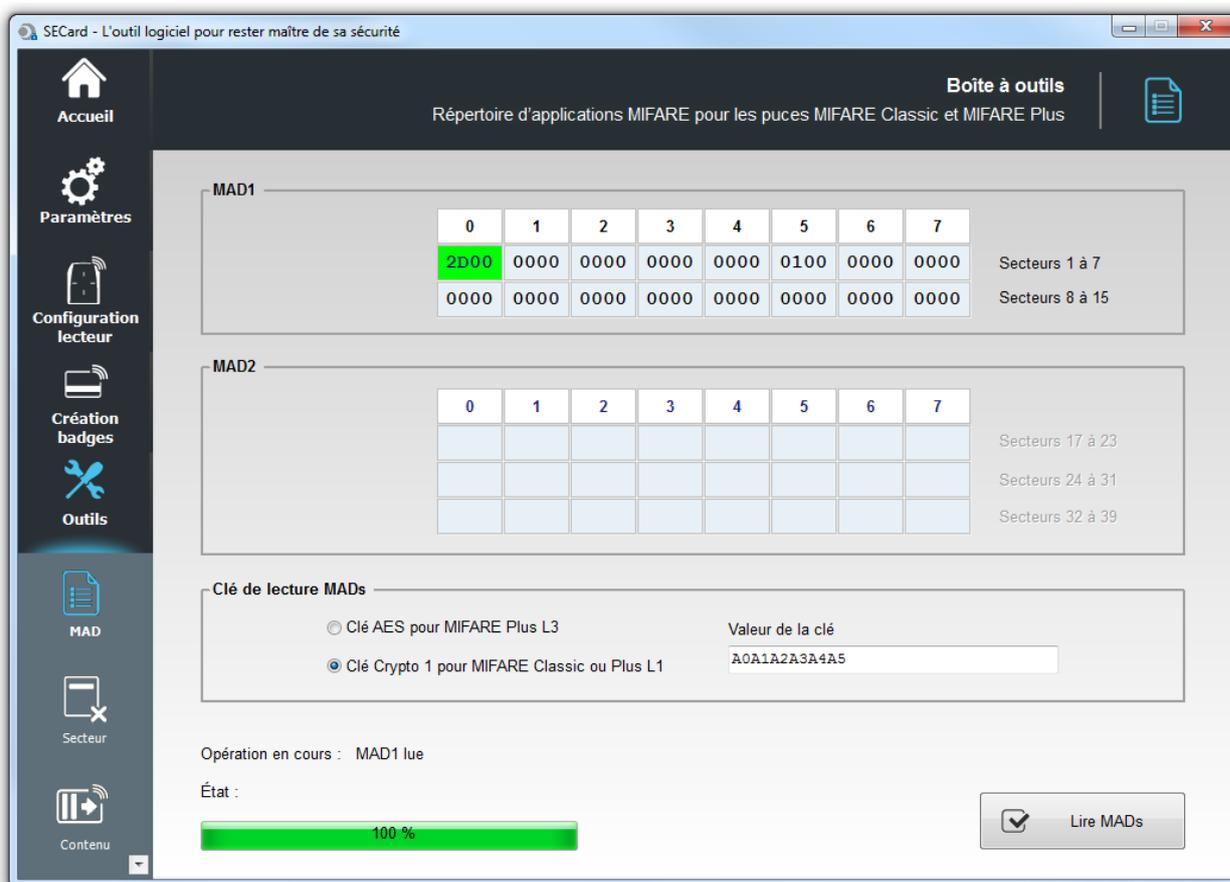
- Card mode
- Slide mode
- Tap Tap mode
- Hands free mode

STid Mobile ID successfully upgraded to STid Mobile ID+

STid Mobile ID+

## VII. Outils

### VIII. 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

SECard - L'outil logiciel pour rester maître de sa sécurité

Boîte à outils  
Répertoire d'applications MIFARE pour les puces MIFARE Classic et MIFARE Plus

MAD1

0	1	2	3	4	5	6	7	
6F00	0000	0000	0000	0000	0000	0000	0000	Secteurs 1 à 7
0000	0000	0000	BC61	0000	BC63	BC62	BC65	Secteurs 8 à 15

MAD2

0	1	2	3	4	5	6	7	
FA00	0000	0000	0000	0000	0000	0000	0000	Secteurs 17 à 23
0000	0000	0000	2700	0000	0000	0000	0000	Secteurs 24 à 31
BC82	0000	0000	0000	0000	0000	0000	0000	Secteurs 32 à 39

Clé de lecture MADs

Clé AES pour MIFARE Plus L3  
 Clé Crypto 1 pour MIFARE Classic ou Plus L1

Valeur de la clé  
A0A1A2A3A4A5A6A7A0A1A2A3A4A5A6A7

Opération en cours : MAD2 lue

État : 100 %

Lire MADs

## Scan de MAD réussi mais paramètres incorrects

SECard - L'outil logiciel pour rester maître de sa sécurité

Boîte à outils  
Répertoire d'applications MIFARE pour les puces MIFARE Classic et MIFARE Plus

MAD1

0	1	2	3	4	5	6	7	
6800	4C58	BC51	0000	0000	0000	0000	0000	Secteurs 1 à 7
0000	0000	0000	0000	0000	0000	0000	0000	Secteurs 8 à 15

MAD2

0	1	2	3	4	5	6	7	
0000	0000	0000	0000	0000	0000	0000	0000	Secteurs 17 à 23
0000	0000	0000	0000	0000	0000	0000	0000	Secteurs 24 à 31
0000	0000	0000	0000	0000	0000	0000	0000	Secteurs 32 à 39

Mauvaise MAD2  
MAD CRC = 00  
au lieu de 16

Clé de lecture MADs

Clé AES pour MIFARE Plus L3  
 Clé Crypto 1 pour MIFARE Classic ou Plus L1

Valeur de la clé  
A0A1A2A3A4A5

Opération en cours : MAD2 lue

État : 100 %

Lire MADs

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

SECard - L'outil logiciel pour rester maître de sa sécurité

Boîte à outils

Répertoire d'applications MIFARE pour les puces MIFARE Classic et MIFARE Plus

Accueil Paramètres Configuration lecteur Création badges Outils MAD Secteur Contenu

Accueil Paramètres Configuration lecteur Création badges Outils

MAD1

0	1	2	3	4	5	6	7

Secteurs 1 à 7  
Secteurs 8 à 15

MAD2

0	1	2	3	4	5	6	7

Secteurs 17 à 23  
Secteurs 24 à 31  
Secteurs 32 à 39

Clé de lecture MADs

Clé AES pour MIFARE Plus L3  
 Clé Crypto 1 pour MIFARE Classic ou Plus L1

Valeur de la clé

A0A1A2A3A4A5

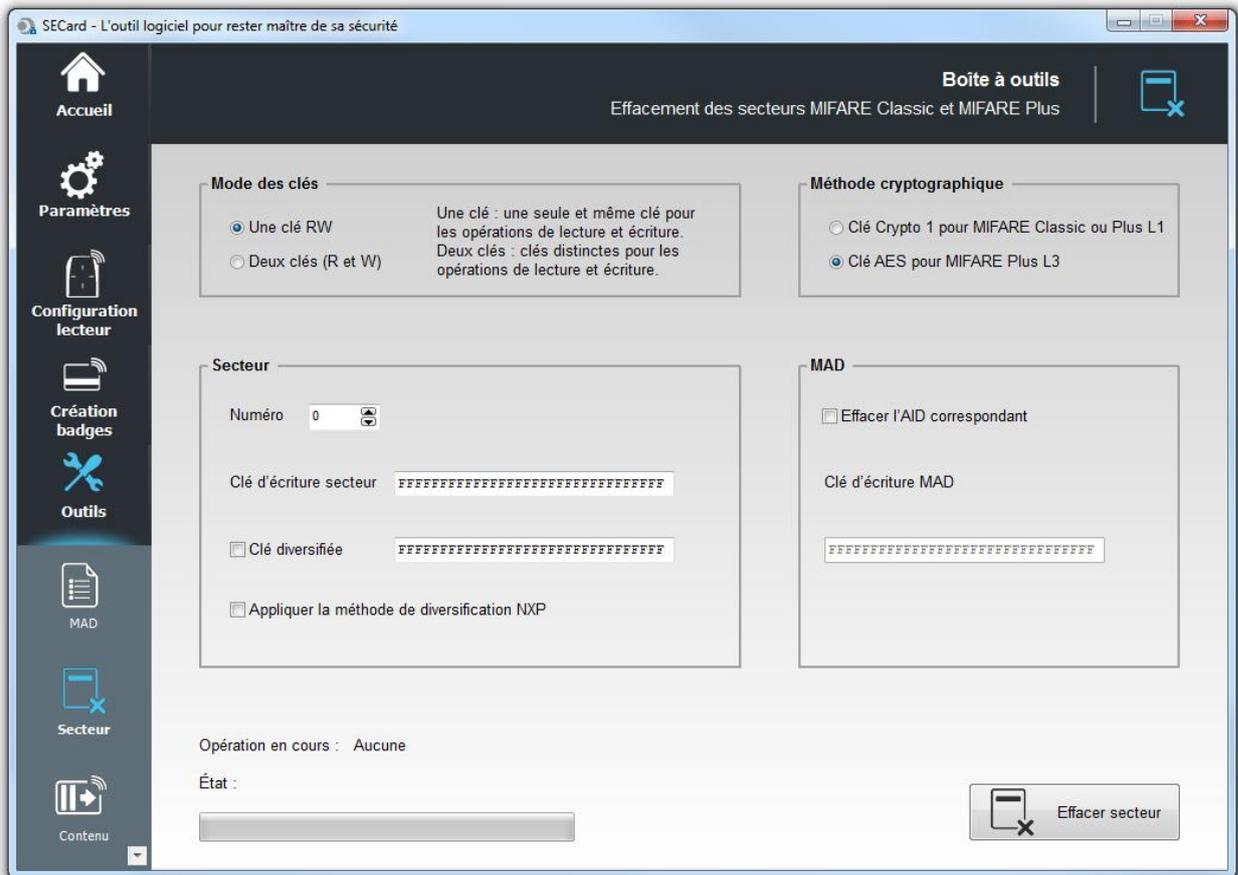
Opération en cours : Lecture de la MAD1...

État : **PN532 Erreur d'authentification Mifare**

20 %

Lire MADs

## VIII. 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.

## VIII. 3 - Contenu

SECard - L'outil logiciel pour rester maître de sa sécurité

Boîte à outils  
Lecture du contenu MIFARE Classic/Plus

Cartographie des données MIFARE

b0	b1	b2	b3	b4	b5	b6	b7	b8	b9	b10	b11	b12	b13	b14	b15	S#	B#
00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF	FF	FF	1	7
A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	2	8
A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	2	9
A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	2	10
A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	2	11
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	3	12
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	3	13
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	3	14
00	00	00	00	00	00	FF	07	80	69	FF	FF	FF	FF	FF	FF	3	15
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	4	16
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	4	17
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	4	18

Type de carte détecté : MIFARE Classic / Plus niveau 1

Temps de lecture : 3869(ms)

Opération en cours : Contenu lu

État : 100 %

Taille carte  
 1 ko  
 2 ko  
 4 ko

A = Erreur d'authentification  
 ? = Erreur inconnue

Lire 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 :

Clés Mifare Classic/Plus

Clés MIFARE Classic | Clés MIFARE Plus

Sector #	Blocks	Keys A	Keys B	Used
0	0..3	FFFFFFFFFFFF	FFFFFFFFFFFF	A
1	4..7	FFFFFFFFFFFF	FFFFFFFFFFFF	A
2	8..11	FFFFFFFFFFFF	FFFFFFFFFFFF	A
3	12..15	FFFFFFFFFFFF	FFFFFFFFFFFF	A
4	16..19	FFFFFFFFFFFF	FFFFFFFFFFFF	A
5	20..23	FFFFFFFFFFFF	FFFFFFFFFFFF	A
6	24..27	FFFFFFFFFFFF	FFFFFFFFFFFF	A
7	28..31	FFFFFFFFFFFF	FFFFFFFFFFFF	A
8	32..35	FFFFFFFFFFFF	FFFFFFFFFFFF	A
9	36..39	FFFFFFFFFFFF	FFFFFFFFFFFF	A
10	40..43	FFFFFFFFFFFF	FFFFFFFFFFFF	A
11	44..47	FFFFFFFFFFFF	FFFFFFFFFFFF	A

Clés diversifiées   
  div NXP   
 Clé de diversification 3DES:

Clés Mifare Classic/Plus

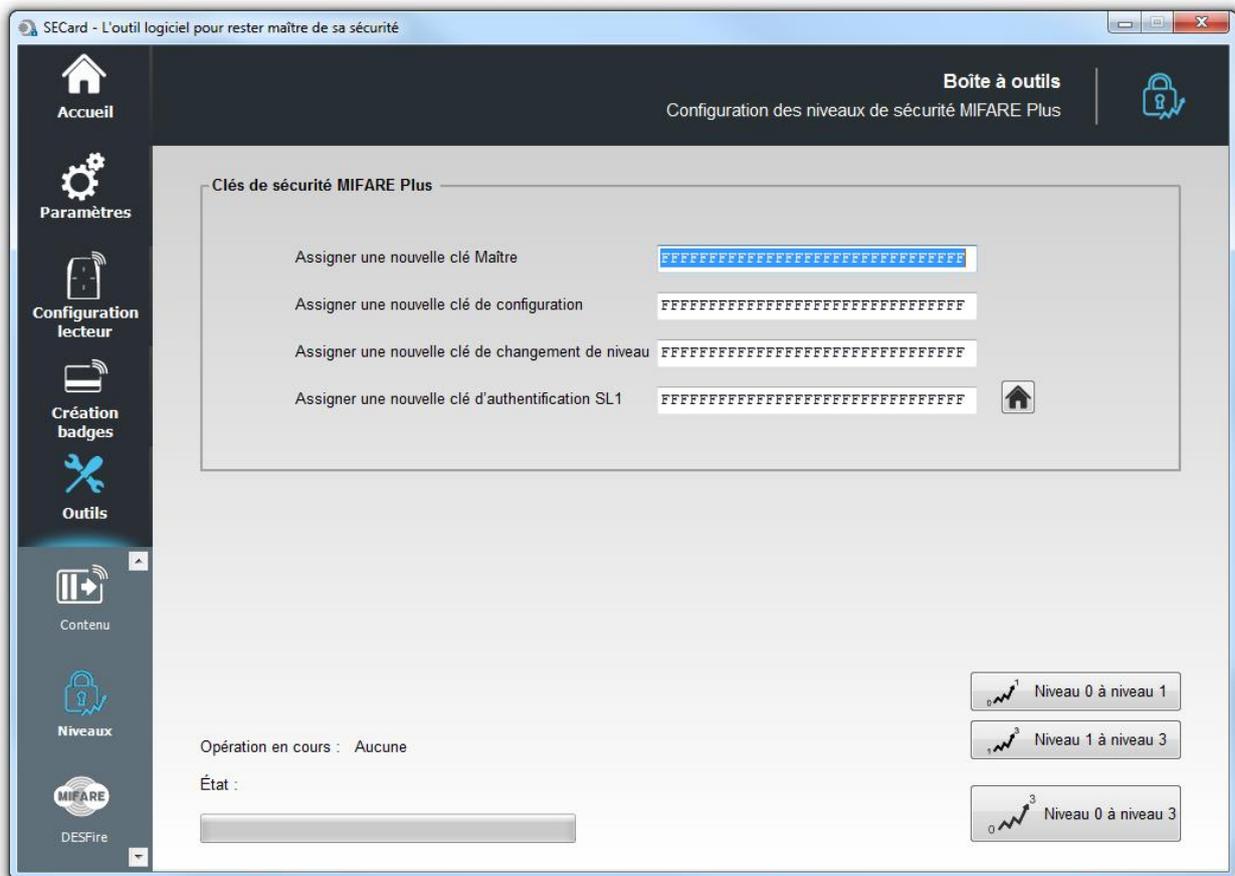
Clés MIFARE Classic | Clés MIFARE Plus

Sector #	Blocks	Keys A	Keys B	Use
0	0..3	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
1	4..7	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
2	8..11	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
3	12..15	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
4	16..19	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
5	20..23	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
6	24..27	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
7	28..31	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
8	32..35	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
9	36..39	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
10	40..43	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A
11	44..47	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	A

Clés diversifiées   
  div NXP   
 Clé de diversification 3DES:

- Accueil
- Paramètres
- Configuration lecteur
- Création badges
- Outils
- MAD
- Secteur
- Contenu

## VIII. 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 quatre champs de clés.

Par défaut, les clés d'une puce MIFARE Plus® sont : « FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF », 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.

## VIII. 5 - DESFire



Accueil



Paramètres



Configuration lecteur



Création badges



Outils



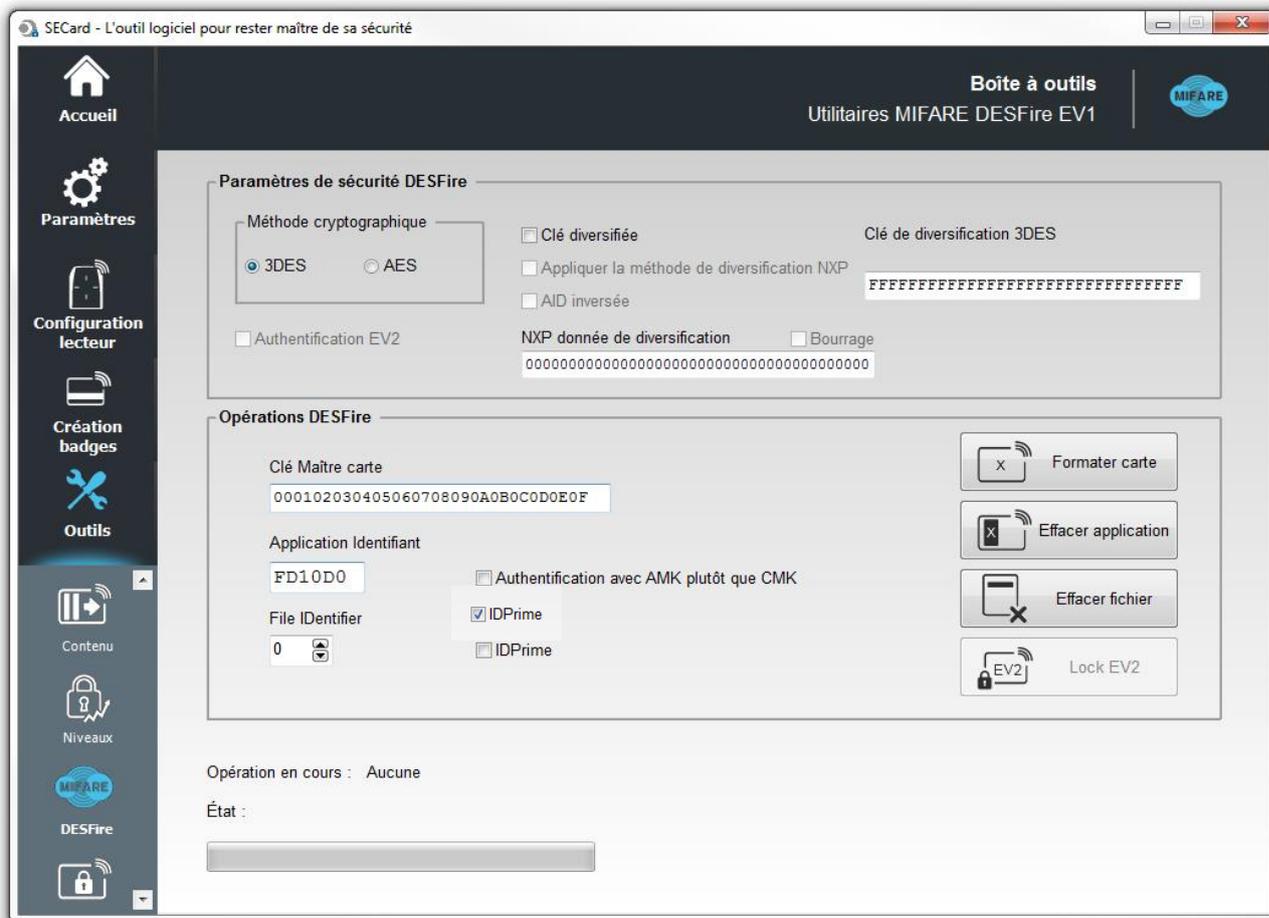
DESFire



Verrouillage



BCA



Permet de formater la puce, d'effacer une application créée sur la puce MIFARE® DESFire® EVx 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

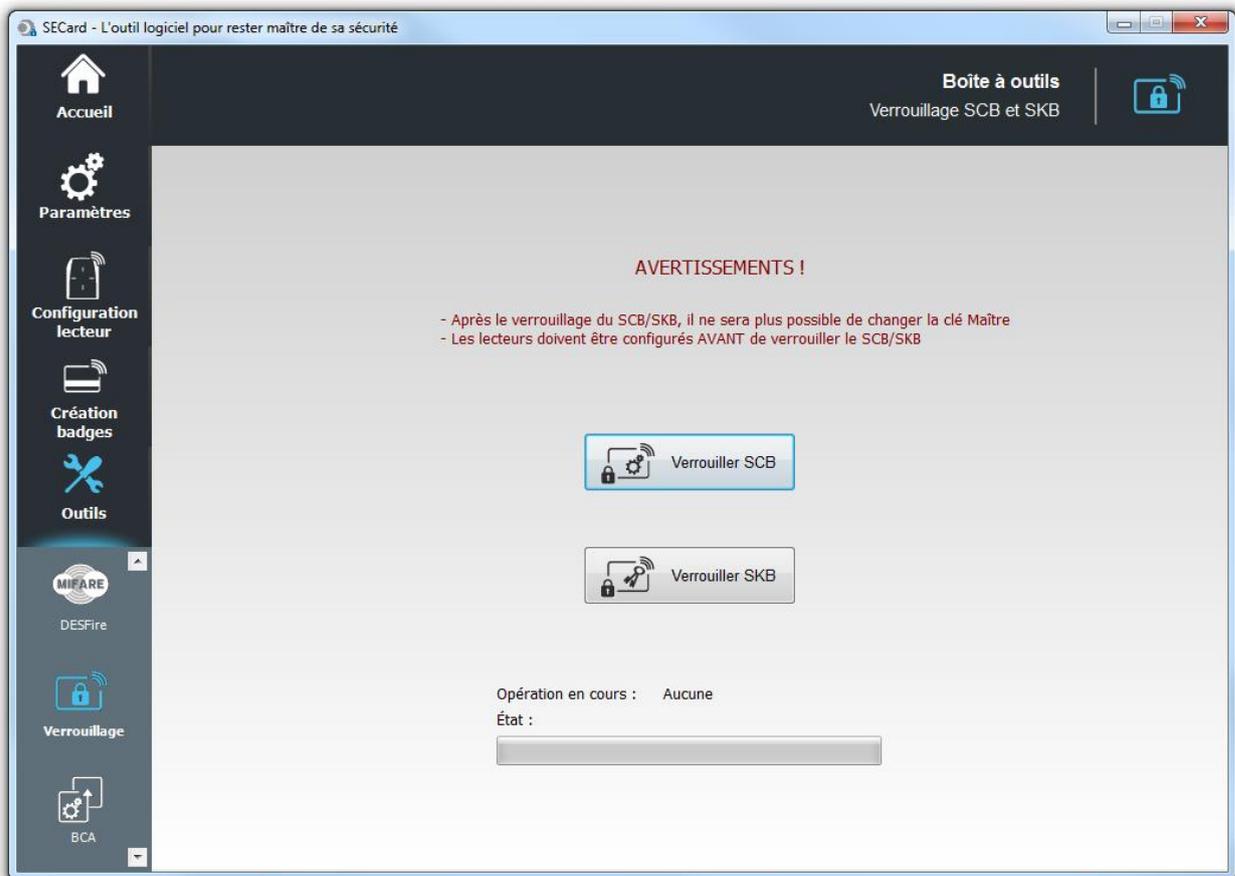
	<ul style="list-style-type: none"> <li>- Renseigner les paramètres de sécurité de la DESFire (méthode cryptographique, clé diversifiée si Ev2 en Lock Ev2 Authentification).</li> <li>- Renseigner la valeur de la Clé Maître carte.</li> </ul> <p><b>Attention</b> Lors du formatage toutes les données seront perdues. Le formatage ne modifie pas la clé maître de la puce.</p>
	<ul style="list-style-type: none"> <li>- Renseigner les paramètres de sécurité de l'application (méthode cryptographique, clé diversifiée si Ev2 en Lock Ev2 Authentification).</li> <li>- Renseigner la valeur de la Clé Maître carte ou Clé Maître Application en fonction des settings de votre puce.</li> <li>- Renseigner l'identifiant de l'application AID</li> </ul> <p><b>Attention</b> Lors de l'effacement d'une application tous les fichiers inclus seront effacés.</p>

-  Accueil
-  Paramètres
-  Configuration lecteur
-  Création badges
-  Outils
-  MIFARE
-  DESFire
-  Verrouillage
-  BCA

 Effacer fichier	<ul style="list-style-type: none"> <li>- Renseigner les paramètres de sécurité de l'application contenant le fichier (méthode cryptographique et si la clé est diversifiée).</li> <li>- Renseigner la valeur de la Clé Maître Application</li> <li>- Renseigner l'identifiant de l'application AID</li> <li>- Renseigner le numéro de fichier à supprimer</li> </ul>
 Lock EV2	<p>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.</p> <ul style="list-style-type: none"> <li>- Renseigner la valeur de la Clé Maître carte.</li> <li>- Sélectionner la Crypto de la Clé Maître carte.</li> </ul> <p><b>Attention</b>        Cette action est définitive, aucun retour possible.</p>

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

## VIII. 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.

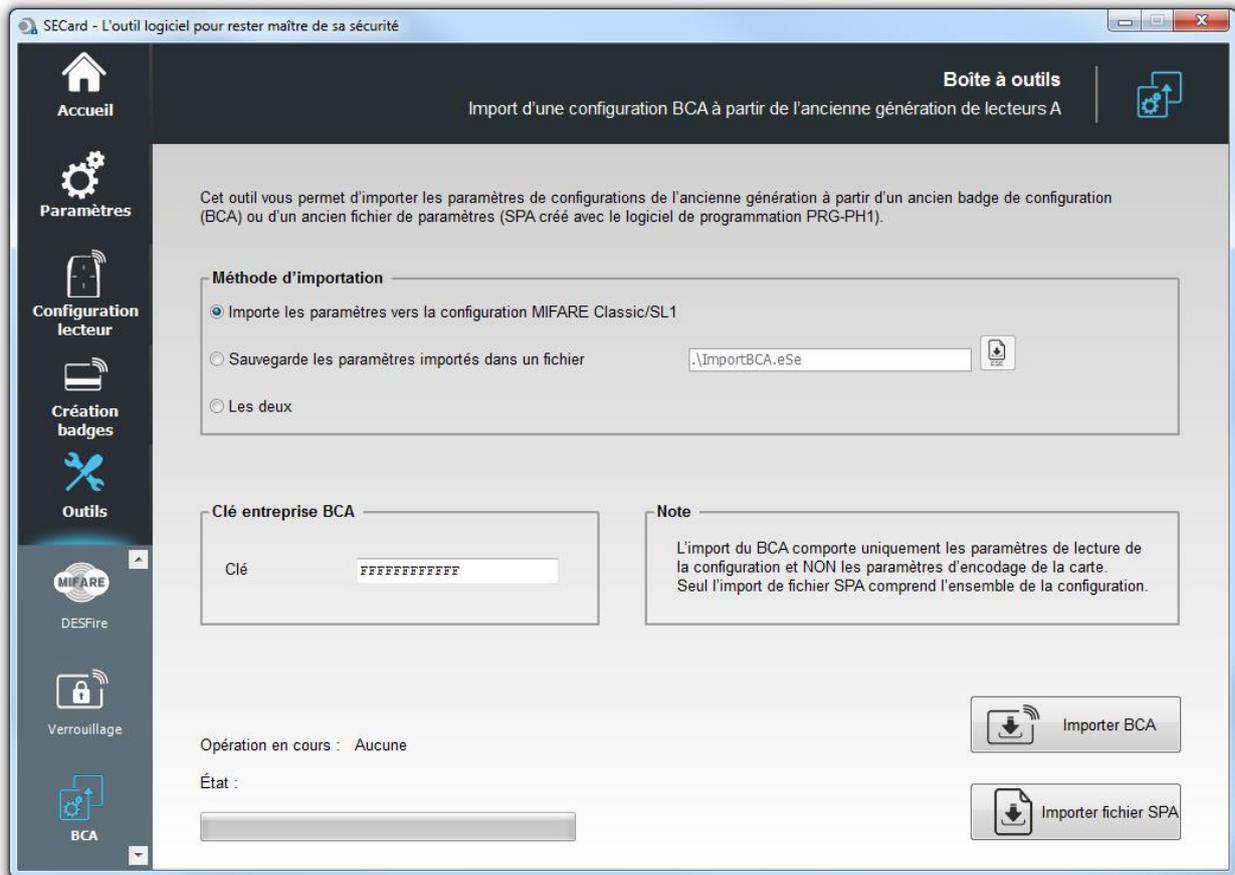
### Attention

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.

## VIII. 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.



Accueil



Paramètres



Configuration  
lecteur



Création  
badges



Outils



DESFire



Verrouillage



BCA

## 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.

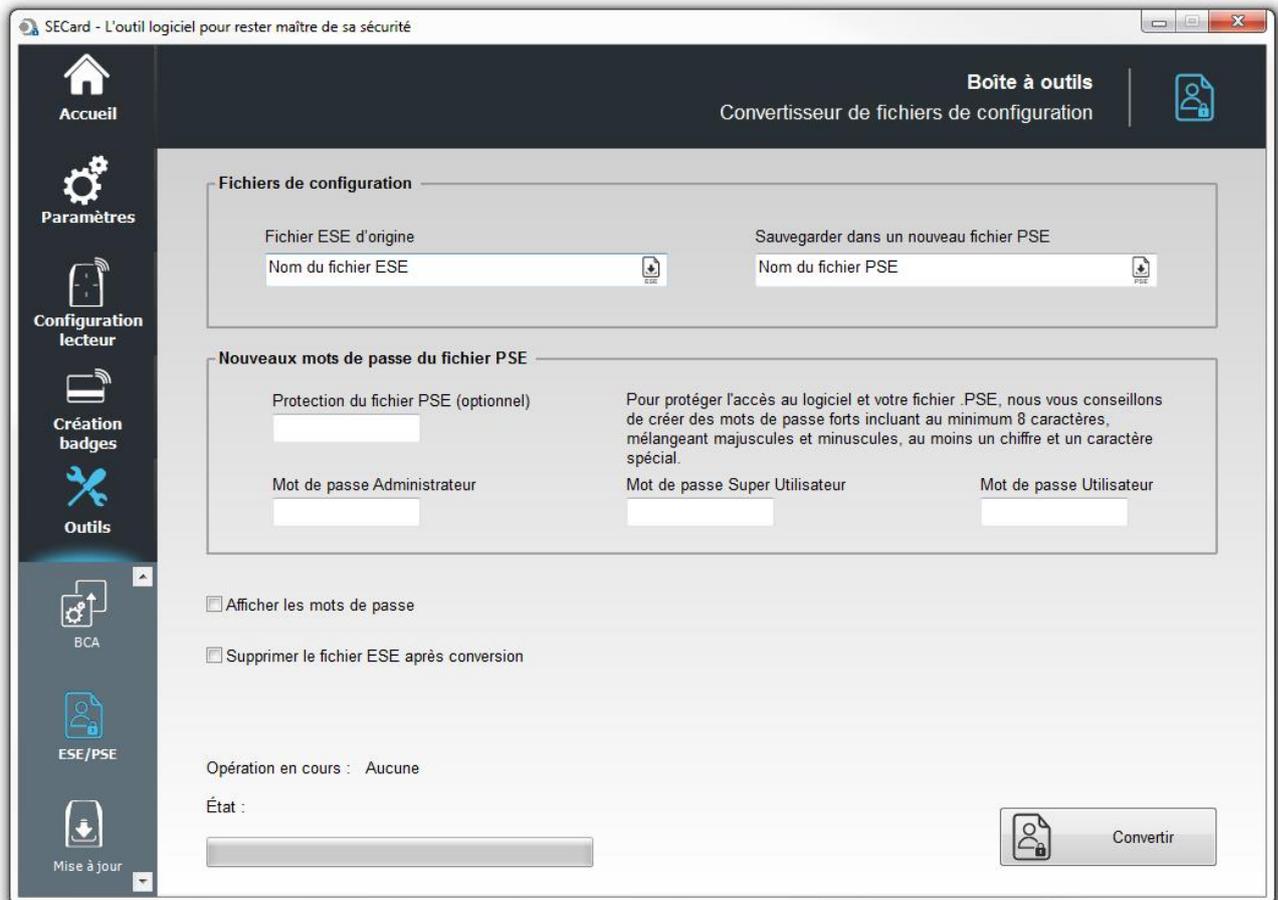
## Import SPA

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.

## VIII. 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

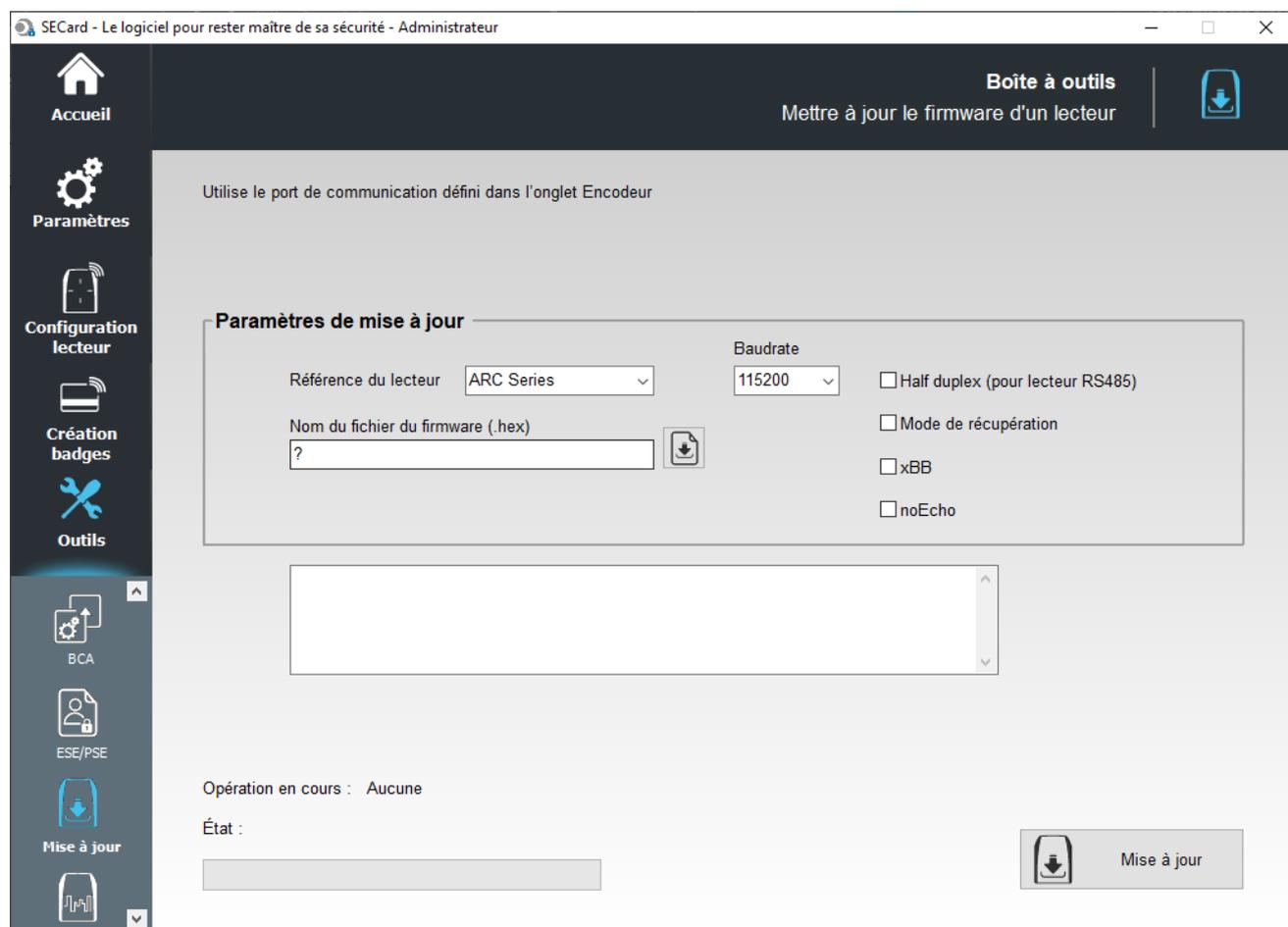
Permet de sélectionner le fichier de configuration .ese à importer et de lui attribuer un nouveau nom en pse.

### 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 ».

## VIII. 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 en cochant le mode de récupération.
- ❖ xBB : permet la reprogrammation des lecteurs transparents (5BB ou 7BB avec firmware min Z05).
- ❖ noEcho : "supprime" l'écho des commandes de reprog et donc réduit considérablement le temps de reprog.

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

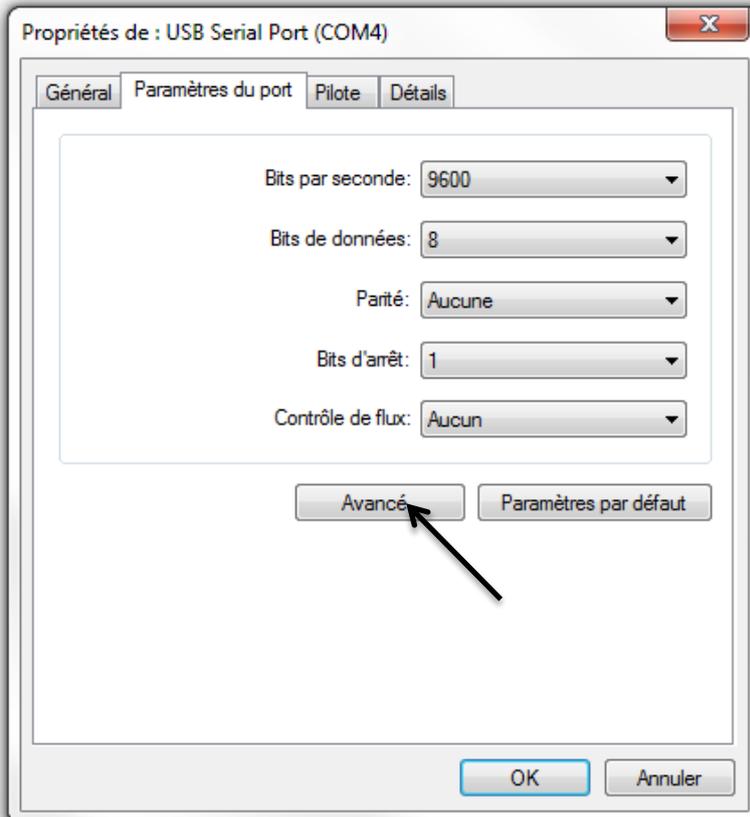
- pendant que la LED clignote en orange pour les lecteurs séries.
- à n'importe quel moment pour les lecteurs TTL.

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

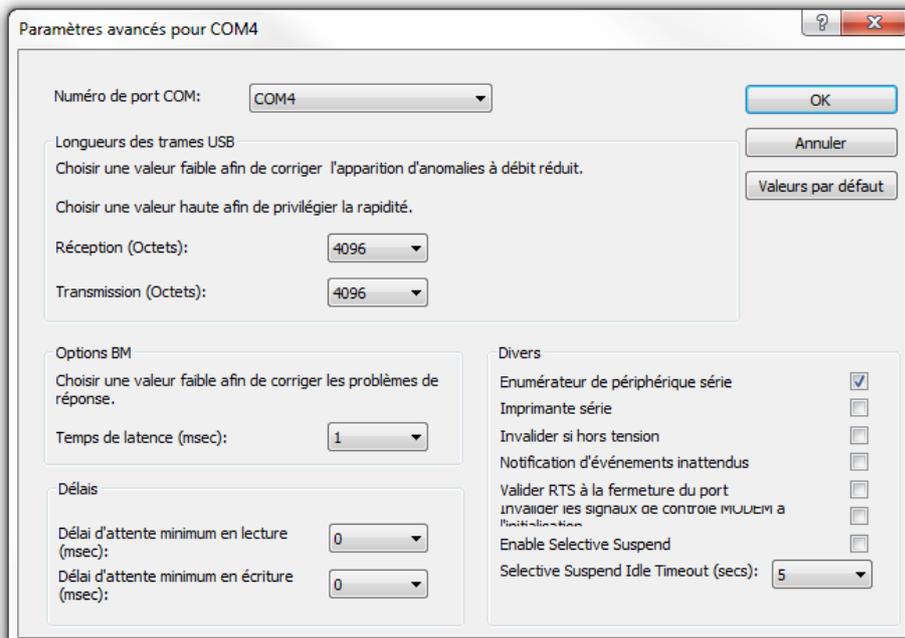
Configuration du port de communication lors de l'utilisations d'un câble convertisseur RS485 / USB :

- Ports (COM et LPT)
  - PCIe to High Speed Serial Port (COM1)
  - PCIe to High Speed Serial Port (COM2)
  - PCIe to Multi Mode Parallel Port (LPT3)
  - USB Serial Port (COM16)
  - USB Serial Port (COM4)

\* Double cliquer sur le port COM correspondant au lecteur.



Ouvrir les paramètres Avancé...



Mettre le temps de latence sur 1



Accueil



Paramètres



Configuration lecteur



Création badges



Outils



ESE/PSE



Mise à jour



UHF config

## 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

**Update parameters**

Reader reference:  Baudrate:   Half duplex (for RS485 readers)

Firmware filename:    Recover mode

xBB

- 2- Configurer le port COM

Note: pour un lecteur W vous pouvez utiliser CTRL + ?

**Paramètres de communication série**

Port:   Baudrate:   Mode de sécurité:

Le protocole de communication sécurisé SSCP définit le niveau de sécurité de la communication entre l'encodeur et SECard.

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

Current operation: Programming...

Status:

Current operation: Verifying...

Status:

Current operation: Firmware update completed

Status:

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

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

**Update parameters**  
Reader reference:  Baudrate:   
 Half duplex (for RS485 readers)  
Firmware filename:    
 Recover mode  
 xBB

- 2- Configurer le port COM à 38400

**Paramètres de communication série**  
Port:  ? Baudrate:  set Mode de sécurité:   
Le protocole de communication sécurisé SSCP définit le niveau de sécurité de la communication entre l'encodeur et SECard.

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

Current operation: Programming...

Status:

Current operation: Verifying...

Status:

Current operation: Firmware update completed

Status:

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

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

**Update parameters**  
Reader reference:  Baudrate:   
 Half duplex (for RS485 readers)  
Firmware filename:   Recover mode  
 xBB

2- Configurer le port COM

**Paramètres de communication série**  
Port:  ? Baudrate:  set Mode de sécurité:   
Le protocole de communication sécurisé SSCP définit le niveau de sécurité de la communication entre l'encodeur et SECard.

3- Cliquer sur Mise à jour

Current operation: Programming...

Status:

Current operation: Verifying...

Status:

Current operation: Firmware update completed

Status:

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

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

**Update parameters**

Reader reference	ARC Series	Baudrate	115200	<input checked="" type="checkbox"/> Half duplex (for RS485 readers)
Firmware filename	<input type="text"/>		<input type="button" value="↓"/>	<input type="checkbox"/> Recover mode
				<input type="checkbox"/> xBB

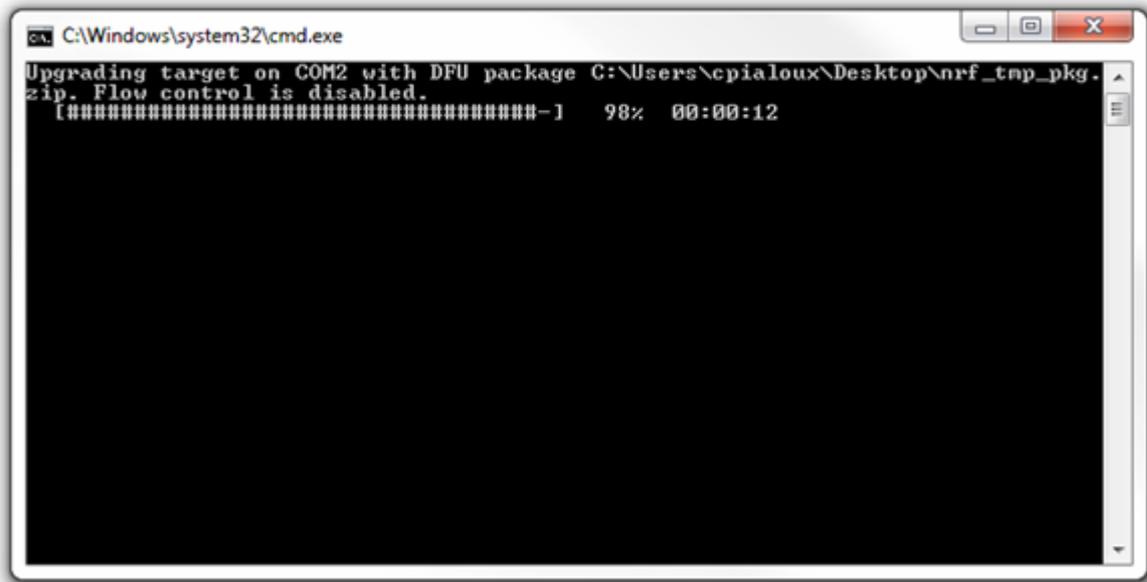
2- Configurer le port COM

**Paramètres de communication série**

Port	COM5	Baudrate	38400	Mode de sécurité	Clair	Le protocole de communication sécurisé SSCP définit le niveau de sécurité de la communication entre l'encodeur et SECard.
	<input style="border: 1px solid #ccc;" type="button" value="?"/>		<input type="button" value="set"/>			

3- Cliquer sur Mise à jour

Une fenêtre DOS s'ouvre :



```

C:\Windows\system32\cmd.exe
Upgrading target on COM2 with DFU package C:\Users\cpialoux\Desktop\nrf_tnp_pkg.zip. Flow control is disabled.
[#####-] 98% 00:00:12
  
```

Opération en cours : Connexion...

État :

0 %

Opération en cours : Mise à jour firmware OK

État :

100 %



Accueil



Paramètres



Configuration  
lecteur



Création  
badges



Outils



ESE/PSE



Mise à jour



UHF config

## Message d'erreur



Current operation: Connecting...

Status: **Error while connecting**

0 %

Cancel

- 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 :

Current operation:

Status: **Error = -20**

0 %

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.



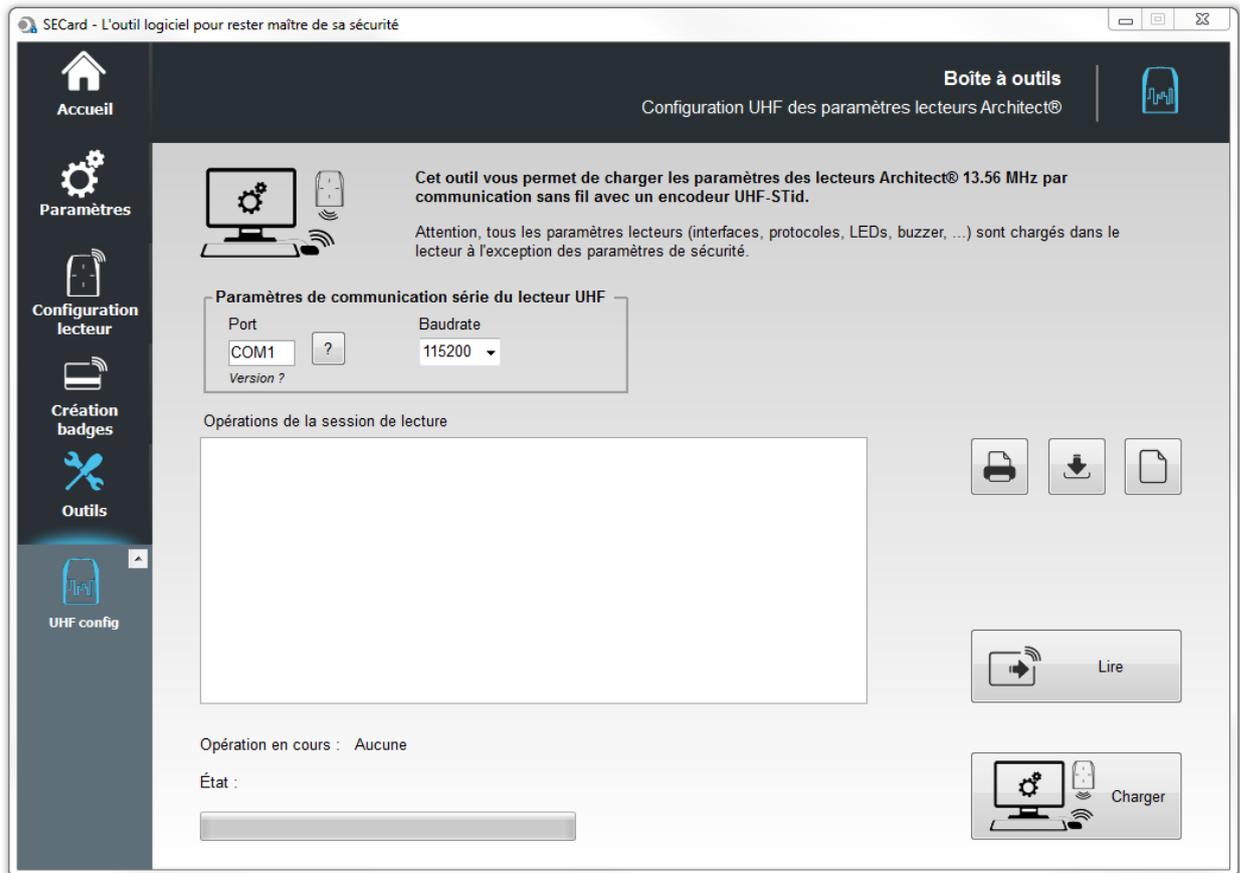
Current operation:

Status: **Error = Command (-18)**

0 %

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

## VIII. 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.

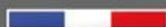


# SECARD



## MANUEL UTILISATEUR

Partie 2 : Technique



*Designed in France  
Made in France*

[www.stid-security.com](http://www.stid-security.com)

## T1- Lecteurs configurables par SECard

### T1.1- Configurable par SCB

Le logiciel SECard dispose d'un module de création de badges de configuration (SCB) permettant de configurer en fonction des paramètres de sécurité les lecteurs, en lecture seule, de la gamme Architect® et WAL.

Référence type : ARCS-**R**3x-x/BT1-xx ou ARCS-**S**3x-x/BT1-xx

### T1.2- Configurable par OCB

Le logiciel SECard dispose d'un module de création de badges de configuration (OCB) permettant de configurer en fonction des paramètres de sécurité les lecteurs osdp™ de la gamme Architect® et WAL.

Référence type : ARCS-W33-x/BT1-**7OS** à partir du firmware Z05

### T1.3- Configurable par SCB R/W

Le logiciel SECard dispose d'un module de création de badges de configuration (SCB R/W) permettant de configurer les paramètres Blue/NFC des lecteurs pilotable de la gamme Architect® Bluetooth®.

Référence type : ARCS-W33-x/BT1-**7AA** ou ARCS-W33-x/BT1-**7AD** à partir du firmware Z06

## T2 - Au sujet des lecteurs

### T2.1 - Mise sous tension des lecteurs lecture seule

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

- 1) Activation de la LED blanche 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.

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.

- ❖ SE8/SE8M

Si un ancien SCB/OCB qui n'active pas le 125 kHz est présenté devant un lecteur équipé d'un SE8M, le lecteur fonctionnera normalement en 13.56 MHz.

Si un lecteur a déjà une ancienne configuration et qu'un SE8M est ensuite connecté au lecteur, le SE8M ne fonctionnera pas tant qu'un nouveau SCB/OCB ne sera pas présenté devant le lecteur.

Si un lecteur équipé d'un SE8M reçoit un SCB/OCB avec activation d'un SE8, le 125 kHz du SE8M ne sera pas activé. Même fonctionnement si un lecteur équipé d'un SE8 reçoit une configuration pour un SE8M. Le lecteur clignotera 3 fois rouge pour dire qu'un mauvais type de lecteur a été activé par le SCB/OCB. La partie 13.56 MHz sera fonctionnelle.

## T2.3 - Lecteur ARC1

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

- |                        |   |   |
|------------------------|---|---|
| • MIFARE® Classic      | - | <u>Lecture d'un numéro de série UID et d'un ID privé</u>                    |
| • MIFARE Plus®         | - | Lecture d'un numéro de série UID <u>seulement</u>                           |
| • MIFARE® DESFire® Ev1 | - | Lecture d'un numéro de série UID <u>seulement</u>                           |
| • MIFARE Ultralight® C | - | Lecture d'un numéro de série UID <u>seulement</u>                           |
| • 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

Sector	Bloc	Bytes														Description		
		0	1	2	3	4	5	6	7	8	9	10	11	12	13			14
0	0	N° de Série (UID)			-	-	R	E	S	E	R	V	E	D	-	-	Bloc Constructeur	16 Sectors de 4 blocs (1ko)
	1	CRC Info	AID S.1	AID S.2	AID S.3	AID S.4	AID S.5	AID S.6	AID S.7								MAD1 data (typ.)	
	2	AID S.8	AID S.9	AID S.10	AID S.11	AID S.12	AID S.13	AID S.14	AID S.15								MAD1 data (typ.)	
	3	Key A				Access Bits			Data	Key B				Trailer Bloc				
1	0															User Data	16 Sectors de 4 blocs (1ko)	
	1															User Data		
	2															User Data		
	3	Key A				Access Bits			Data	Key B				Trailer Bloc				
15	0															User Data	16 Sectors de 4 blocs (1ko)	
	1															User Data		
	2															User Data		
	3	Key A				Access Bits			Data	Key B				Trailer Bloc				
16	0	CRC RFU	AID S.17	AID S.18	AID S.19	AID S.20	AID S.21	AID S.22	AID S.23								MAD2 data (typ.)	16 Sectors de 4 blocs (1ko)
	1	AID S.24	AID S.25	AID S.26	AID S.27	AID S.28	AID S.29	AID S.30	AID S.31								MAD2 data (typ.)	
	2	AID S.32	AID S.33	AID S.34	AID S.35	AID S.36	AID S.37	AID S.38	AID S.39								MAD2 data (typ.)	
	3	Key A				Access Bits			Data	Key B				Trailer Bloc				
30	0															User Data	16 Sectors de 4 blocs (1ko)	
	1															User Data		
	2															User Data		
	3	Key A				Access Bits			Data	Key B				Trailer Bloc				
31	0															User Data	16 Sectors de 4 blocs (1ko)	
	1															User Data		
	2															User Data		
	3	Key A				Access Bits			Data	Key B				Trailer Bloc				
32	0															User Data	8 Sectors de 16 blocs (2ko)	
	1															User Data		
	2															User Data		
	3															User Data		
	4															User Data		
	5															User Data		
	6															User Data		
	7															User Data		
	8															User Data		
	9															User Data		
	10															User Data		
	11															User Data		
	12															User Data		
	13															User Data		
	14															User Data		
	15	Key A				Access Bits			Data	Key B				Trailer Bloc				
39	0															User Data	8 Sectors de 16 blocs (2ko)	
	1															User Data		
	2															User Data		
	3															User Data		
	4															User Data		
	5															User Data		
	6															User Data		
	7															User Data		
	8															User Data		
	9															User Data		
	10															User Data		
	11															User Data		
	12															User Data		
	13															User Data		
	14															User Data		
	15	Key A				Access Bits			Data	Key B				Trailer Bloc				

## Exemple de mémoire découpée : MIFARE Plus® Level 1

Sector	Bloc	Bytes															Description		
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14		15	
0	0	N° de Série (UID)					-	-	R	E	S	E	R	V	E	D	-	-	Bloc Constructeur
	1	CRC	Info	51 BC														MAD1 data (typ.)	
	2													MAD1 data (typ.)					
	3	A0 A1 A2 A3 A4 A5					Access Bits		Data	FF FF FF FF FF FF					Trailer Bloc				
1	0	89	5A	1A	23	7E													User Data
	1													User Data					
	2													User Data					
	3	B1 42 A6 80 CD 90					Access Bits		Data	4F 66 36 0F 9C C2					Trailer Bloc				
...	...	...															...		
15	0													User Data					
	1													User Data					
	2													User Data					
	3	Key A					Access Bits		Data	Key B					Trailer Bloc				
16	0	CRC	RFU													MAD2 data (typ.)			
	1													MAD2 data (typ.)					
	2													MAD2 data (typ.)					
	3	A0 A1 A2 A3 A4 A5					Access Bits		Data	FF FF FF FF FF FF					Trailer Bloc				
...	...	...															...		
30	0	4E	8A	7B	55	9F													User Data
	1													User Data					
	2													User Data					
	3	BC 23 C9 BE D4 D9					Access Bits		Data	D9 16 7C A8 38 B4					Trailer Bloc				
31	0													User Data					
	1													User Data					
	2													User Data					
	3	Key A					Access Bits		Data	Key B					Trailer Bloc				

16 Sectors de 4 blocs (1ko)

16 Sectors de 4 blocs (1ko)

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

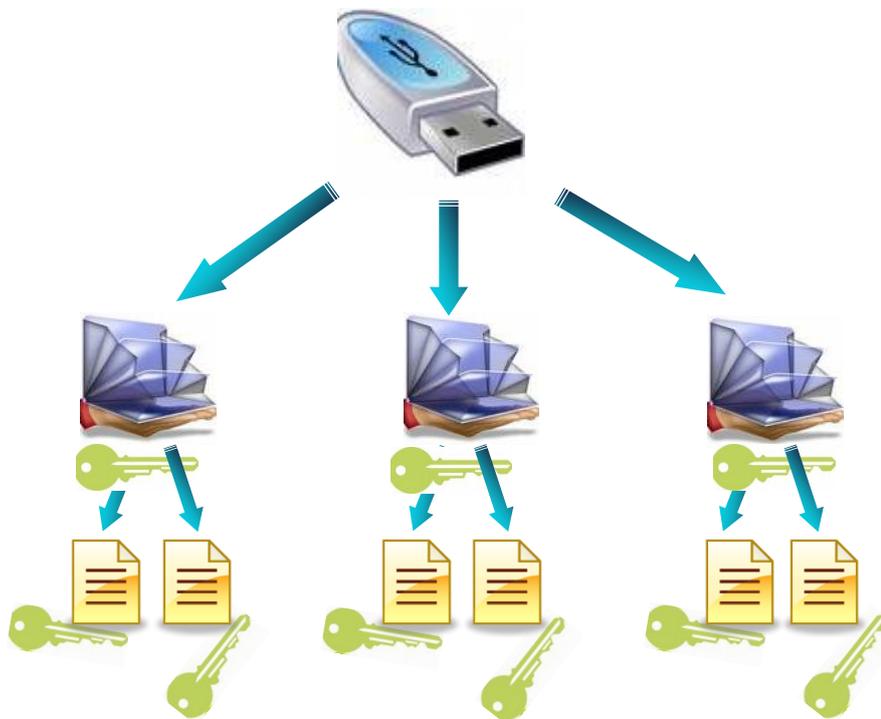
Sector	Bloc	Bytes															Description	
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14		15
0	0	N° de Série (UID)															Bloc Constructeur	
	1	CRC	Info	51 BC														MAD1 data (typ.)
	2																	MAD1 data (typ.)
	3						Access Bits		Data							Trailer Bloc		
1	0	89	5A	1A	23	7E											User Data	
	1																User Data	
	2																User Data	
	3						Access Bits		Data							Trailer Bloc		
...	...	...															...	
15	0																User Data	
	1																User Data	
	2																User Data	
	3						Access Bits		Data							Trailer Bloc		
16	0	CRC	RFU														MAD2 data (typ.)	
	1												BD 01				MAD2 data (typ.)	
	2																MAD2 data (typ.)	
	3						Access Bits		Data							Trailer Bloc		
...	...	...															...	
30	0	4E	8A	7B	55	9F											User Data	
	1																User Data	
	2																User Data	
	3						Access Bits		Data							Trailer Bloc		
31	0																User Data	
	1																User Data	
	2																User Data	
	3						Access Bits		Data							Trailer Bloc		

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 »
  
- ✓ 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® EVx

### Plan mémoire global



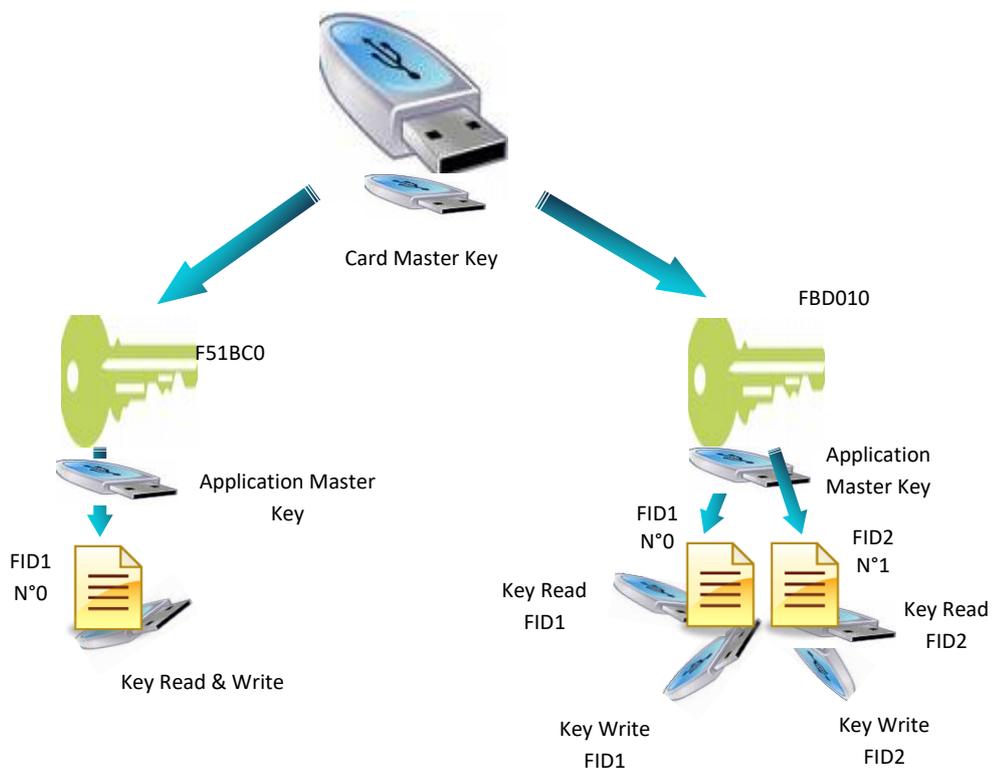
→ Une application racine.

→ 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				Pages	
		0	1	2	3		
<b>Mifare Ultralight®</b>	Chip serial Number 7 bytes	CSN0	CSN1	CSN2	BCC0	0	
		CSN3	CSN4	CSN5	CSN6	1	
<b>Mifare Ultralight C®</b>	Internal Lock bytes	BCC1	INTERNAL	LOCK0	LOCK1	2	
	OTP	OTP0	OTP1	OTP2	OTP3	3	
<b>Mifare Ultralight C®</b>	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

	Bytes				Pages
	0	1	2	3	
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
	...	...	...	...	...
	...	...	...	...	...
	...	...	...	...	...
	...	...	...	...	...
	...	...	...	...	...
	...	...	...	...	...
	...	...	...	...	...
	...	...	...	...	...
	...	...	...	...	...
	...	...	...	...	...
	0x8F	0x61	0x40	0x1E	20
	...	...	...	...	...
	...	...	...	...	...
	...	...	...	...	...
	...	...	...	...	39
Lock bytes Auth. Configuration Counter	LOCK / AUTH / COUNTER				40-43
Security Key	3DES AUTHENTICATION KEY				44-47

Mifare UltraLight C®

Unprotected

Protected

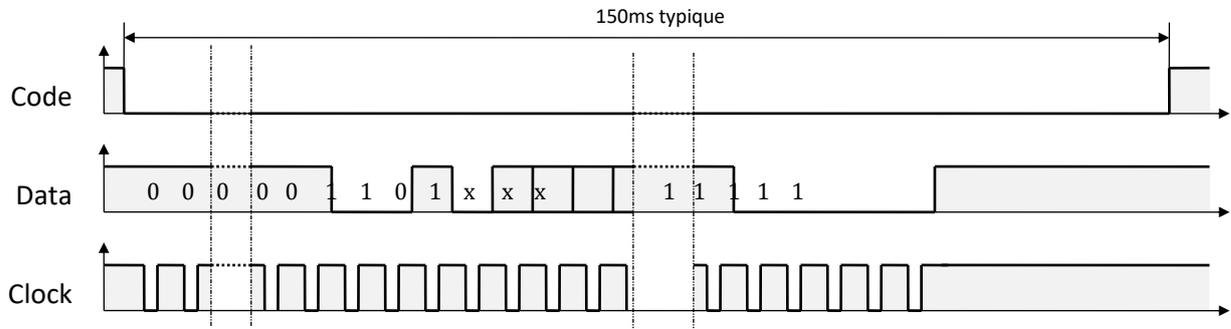
Dans le cas ci-dessus, la zone de la *Page 4* à la *Page 19* incluse n'est pas protégée en lecture et ne nécessitera donc pas d'authentification avec la clé *3DES*. Le code privé en *Page 4* sera donc lisible sans aucune contrainte.

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*.

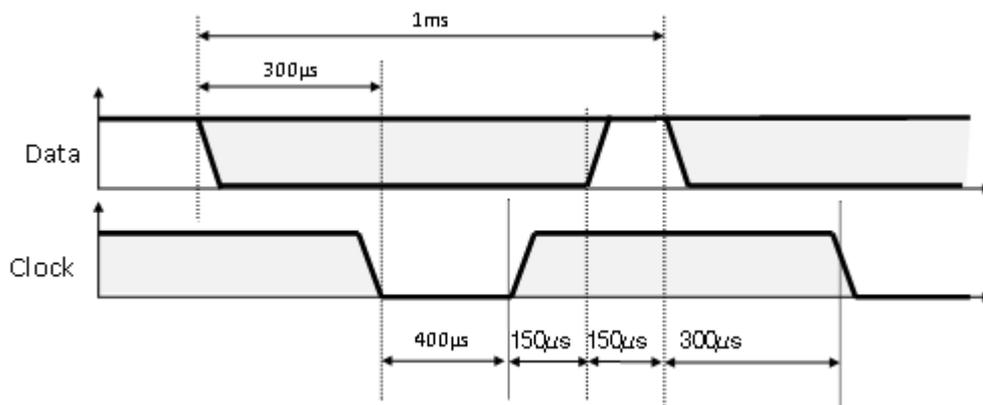
## T4 - Au sujet des protocoles de communication TTL

### 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 125 kHz

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 tronqué 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.

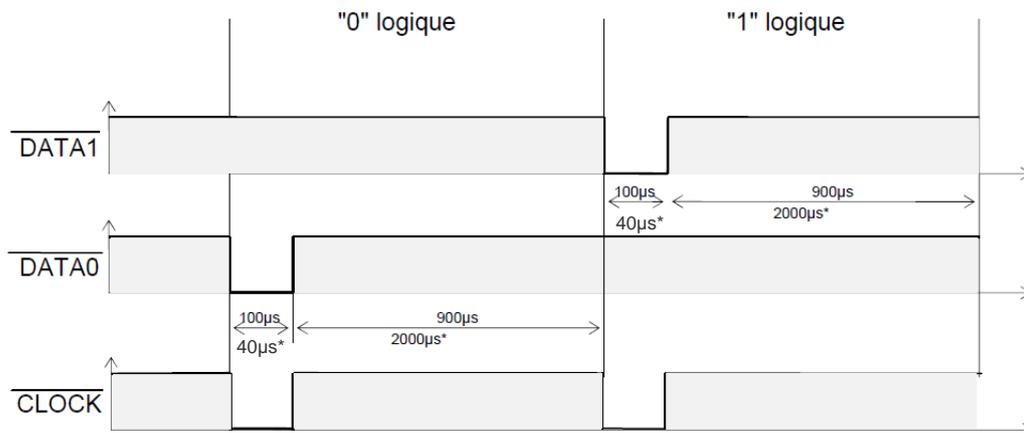
### Exemple

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 :

- 1<sup>ère</sup> parité** : 1 bit de parité paire sur les 12 bits suivants
- Données** : 6 caractères hexadécimaux « MSByte first »
- 2<sup>nde</sup> 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 :

Valeur	Type de puce
0x40	MIFARE® Classic
0x41	MIFARE® DESFire® / DESFire® EV1 & EV2 & EV3
0x42	125 kHz (EM/Nedap/HID)
0x43	MIFARE Ultralight® / Ultralight® C
0x44	MIFARE Plus® Level 0 / Level 2 / Level 3
0x45	PUPI ISO 14443-3B
0x46	CPS3
0x47	Moneo
0x48	AMC (Application Multi-services Citoyenne)
0x4A	3,25 MHz (uniquement sur gamme standard)
0x4E	HCE
0x50	Type de tag non défini
0x60	BLE (Bluetooth®)
0x70	Arrachement
0x80	QR Code (en mode UID)

### 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 :

- 1<sup>ère</sup> parité** : 1 bit de parité paire sur les 16 bits suivants
- Données** : 8 caractères hexadécimaux « MSByte first »
- 2<sup>nd</sup>e 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 :

- 1<sup>ère</sup> parité** : 1 bit de parité paire sur les 18 bits suivants
- Données** : 9 caractères hexadécimaux « MSByte first »
- 2<sup>nd</sup>e parité** : 1 bit de parité impaire sur les 18 bits précédents

### Exemple

Pour un code hexadécimal « 0x0F3129DD3B », 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 :

<i>Data</i> 12 octets	<i>Valeur aléatoire</i> 2 octets	<i>CRC</i> 2 octets
--------------------------	-------------------------------------	------------------------

*Trame 1 chiffrée*

<i>Data</i> 12 octets	<i>Valeur aléatoire</i> 2 octets	<i>CRC</i> 2 octets
--------------------------	-------------------------------------	------------------------

*Trame 2 chiffrée*

<i>Data</i> 12 octets	<i>Valeur aléatoire</i> 2 octets	<i>CRC</i> 2 octets
--------------------------	-------------------------------------	------------------------

*Trame 3 chiffrée*

### T4.4 - Protocole PAC / PAC64

Les protocoles PAC/PAC64 sont disponibles pour des lecteurs TTL en lecture seule (R31). Il n'y a pas de compatibilité avec les interfaces (INT ou mode sécurisé S31).

Plusieurs options ne sont pas supportées dans ces protocoles :

- Pas de mode clavier.
- Pas de gestion des signaux de vie et d'arrachement.

#### Protocole PAC

- Disponible pour tous les types de puce.
- Pas d'authentification
- Sortie scramble
- Données sur 4 octets transmises sur la sortie Tx du lecteur.

#### Protocole PAC64

- Disponible uniquement pour les puces DESFire® et Mobile ID.
- Pour la DESFire en UID : lecture de l'UID après authentification avec la clé maitre carte puis envoi de la donnée obfusquée sur la sortie Tx.
- Pour la DESFire en ID privé : lecture de la donnée basée sur les principes de sécurité SECard puis envoi de la donnée obfusquée sur la sortie Tx.
- Pour la Mobile ID : lecture basée sur les principes de sécurité SECard puis envoi de la donnée obfusquée sur la sortie Tx.
- La clé PAC64 utilisée pour l'authentification et l'obfuscation est à renseigner

dans SECard :

<b>PAC64 master key</b>	
Current	923F6B795B70B27E549CE32B3138DE43

- Données sur 7 octets transmises sur la sortie Tx du lecteur. L'octet 8 est calculé par le protocole et correspond à l'index de cryptage (encryptionIndex).

## 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.

Pour le Prefix, Suffix, ID-Len and ID-Tag voir [SCB – Etape 3](#) Ajout fonctionnalité 3.6

## 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 gèrera 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 utilisés.

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 leHost. 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	Lout	Dataout	CRC
1 octet	2 octets	2 octets	4 octets	2 octets	2 octets	Lout octets	2 octets

*Trame complète envoyée par le système*

#02	Len	CTRL	ACK	L <sub>in</sub>	Data <sub>in</sub>	Status	CRC
1 octet	2 octets	2 octets	2 octets	2 octets	L <sub>in</sub> 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	Lout	Dataout	HMAC-SHA-1 <sub>k</sub> (Commande)	CRC
1 octet	2 octets	2 octets	4 octets	2 octets	2 octets	Lout octets	10 octets	2 octets

*Trame complète envoyée par le système*

#02	Len	CTRL	ACK	L <sub>in</sub>	Data <sub>in</sub>	Status	Signature HMAC-SHA-1 <sub>k</sub> (Réponse)	CRC
1 octet	2 octets	2 octets	2 octets	2 octets	L <sub>in</sub> 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  $k_s$  de signature sur 10 octets
- ✓  $K_c$  (Chiff Key) clé utilisateur utilisée pour générer la clé  $k_c$  de cryptographie sur 16 octets

**Attention**

Par défaut les clés utilisateur ont pour valeur :

$K_s = 0x$  FFFFFFFFFFFFFFFFFF

$K_c = 0x$  FFFFFFFFFFFFFFFFFF

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 <sub>out</sub>	Data <sub>out</sub>	CRC
1 octet	2 octets	2 octets	4 octets	2 octets	2 octets	L <sub>out</sub> 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)	<table border="1"> <thead> <tr> <th>b7 – b1</th> <th>b0</th> </tr> </thead> <tbody> <tr> <td>Adresse du lecteur RS485 1111 111" à "0000 000</td> <td>Liaison série utilisée "0" RS232 "1" RS485</td> </tr> </tbody> </table>	b7 – b1	b0	Adresse du lecteur RS485 1111 111" à "0000 000	Liaison série utilisée "0" RS232 "1" RS485
	b7 – b1	b0					
Adresse du lecteur RS485 1111 111" à "0000 000	Liaison série utilisée "0" RS232 "1" RS485						
CTRL Mode	Détermine le mode de communication (un octet)	<ul style="list-style-type: none"> <li>○ 00h → Mode non sécurisé message transmis en clair.</li> <li>○ 01h → Mode signé</li> <li>○ 02h → Mode chiffré</li> <li>○ 03h → Mode signé et chiffré</li> </ul>					
CMD	Mot de quatre octets englobant deux octets déterminant le type de commande (lecteur, <i>Mifare DESFire &amp; DESFire Ev1</i> , <i>Mifare Classic</i> , <i>Mifare Ultralight C</i> ou <i>Mifare PLUS</i> ) et deux octets définissant le code de la commande à transmettre						
	RFU	1 octet	00h				
	Type	Détermine le type de commande (1 octet)	<ul style="list-style-type: none"> <li>00h → Commande lecteur</li> <li>01h → Commande <i>Mifare® Classic</i></li> <li>02h → Commande <i>Mifare DESFire® &amp; DESFire® Ev1</i></li> <li>03h → Commande <i>Mifare Plus®</i></li> <li>05h → Commande <i>Mifare Ultralight® C</i></li> <li>09h → Commande <i>CPS3</i></li> <li>0Bh → Commande biométrique</li> </ul>				
Code	Détermine le code commande à transmettre au lecteur (deux octets)						
Reserved	AAh 55h (deux octets).						
L <sub>out</sub>	Détermine la taille des données envoyées par le host (deux octets).						
Data <sub>out</sub>	Représente les données envoyées par le host (dans le cas d'une écriture par exemple) (L <sub>out</sub> octets)						
CRC	CRC- <sup>16</sup> -CCITT [Len....Command] <b>[Polynôme « <math>x^{16} + x^{12} + x^5 + 1</math> » 0x1021]</b> ; Valeur Initiale 0xFFFF						

Les informations transmises par le lecteur sont formatées de la façon suivante :

#02	Len	CTRL	ACK	L <sub>in</sub>	Data <sub>in</sub>	Status	CRC
1 octet	2 octets	2 octets	2 octets	2 octets	L <sub>in</sub> 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)	<table border="1"> <thead> <tr> <th>b7 – b1</th> <th>b0</th> </tr> </thead> <tbody> <tr> <td>Adresse du lecteur RS485 1111 111" à "0000 000</td> <td>Liaison série utilisée "0" RS232 "1" RS485</td> </tr> </tbody> </table>		b7 – b1	b0	Adresse du lecteur RS485 1111 111" à "0000 000	Liaison série utilisée "0" RS232 "1" RS485			
	b7 – b1	b0									
Adresse du lecteur RS485 1111 111" à "0000 000	Liaison série utilisée "0" RS232 "1" RS485										
CTRL Mode	Détermine le mode de communication (un octet)	<ul style="list-style-type: none"> <li>○ 00h → Mode non sécurisé message transmis en clair.</li> <li>○ 01h → Mode signé</li> <li>○ 02h → Mode chiffré</li> <li>○ 03h → Mode signé et chiffré</li> </ul>									
ACK	Acquittement de début de trame, égal au code commande envoyé par le host.										
L <sub>in</sub>	Détermine la taille des données que le host va recevoir (deux octets).										
Data <sub>in</sub>	Données envoyées par le lecteur en réponse à la commande du host (L <sub>in</sub> octets).										
Status	Données envoyées par le lecteur en réponse à la commande du host (L <sub>in</sub> octets).										
	RFU	1 octet	00h								
	Type	Détermine le type de commande (un octet)	<ul style="list-style-type: none"> <li>00h → Commande lecteur</li> <li>01h → Commande Mifare® Classic</li> <li>02h → Commande Mifare DESFire &amp; DESFire® Ev1</li> <li>03h → Commande Mifare Plus®</li> <li>05h → Commande Mifare Ultralight® C</li> <li>09h → Commande CPS3</li> <li>0Bh → Commande biométrique</li> </ul>								
	Code	Détermine le code erreur (un octet)									
CRC	CRC-16-CCITT [Len....Command] <b>[Polynôme « <math>x^{16} + x^{12} + x^5 + 1</math> » 0x1021]; Valeur Initiale 0xFFFF</b>										

### 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<sub>out</sub> Data<sub>out</sub>

<b>CMD</b> 2 octets :	01h 00h
<b>L<sub>out</sub></b> 2 octets :	Data <sub>Len</sub> Egal au nombre d'octets de Data
<b>Data<sub>out</sub></b> x octets :	Valeur de l'ID lu par le lecteur en hexadécimal.

#### Système : CMD L<sub>in</sub> LedColor LedDuration BuzzerDuration 00h 00h

<b>CMD</b> 2 octets :	01h 00h
<b>L<sub>in</sub></b> 2 octets :	00h 03h (LedColor + LedDuration + BuzzerDuration)
<b>LedColor</b> 1 octet :	Octet déterminant la couleur de la LED. [00h ... 03h] <ul style="list-style-type: none"><li>➤ 00h LED éteinte</li><li>➤ 01h LED verte</li><li>➤ 02h LED rouge</li><li>➤ 03h LED orange</li></ul>
<b>LedDuration</b> 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).
<b>BuzzerDuration</b> 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<sub>out</sub> Data<sub>out</sub>

<b>CMD</b> 2 octets :	01h 02h
<b>L<sub>out</sub></b> 2 octets :	00h 02h Egal au nombre d'octets de Data
<b>Data<sub>out</sub></b> 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<sub>in</sub> 00h 00h

<b>CMD</b> 2 octets :	01h 02h
<b>L<sub>in</sub></b> 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<sub>out</sub> 00h

<b>CMD</b> 2 octets :	01h 03h
<b>L<sub>out</sub></b> 2 octets :	00h 01h Egal au nombre d'octets de Data

### Système : CMD L<sub>in</sub> 00h 00h 00h 00h

<b>CMD</b> 2 octets :	01h 03h
<b>L<sub>in</sub></b> 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 transmis 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<sub>in</sub> LedGreen LedRed Buzzer 00h 00h

**CMD 2 octets**: 01h 04h

**L<sub>in</sub> 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

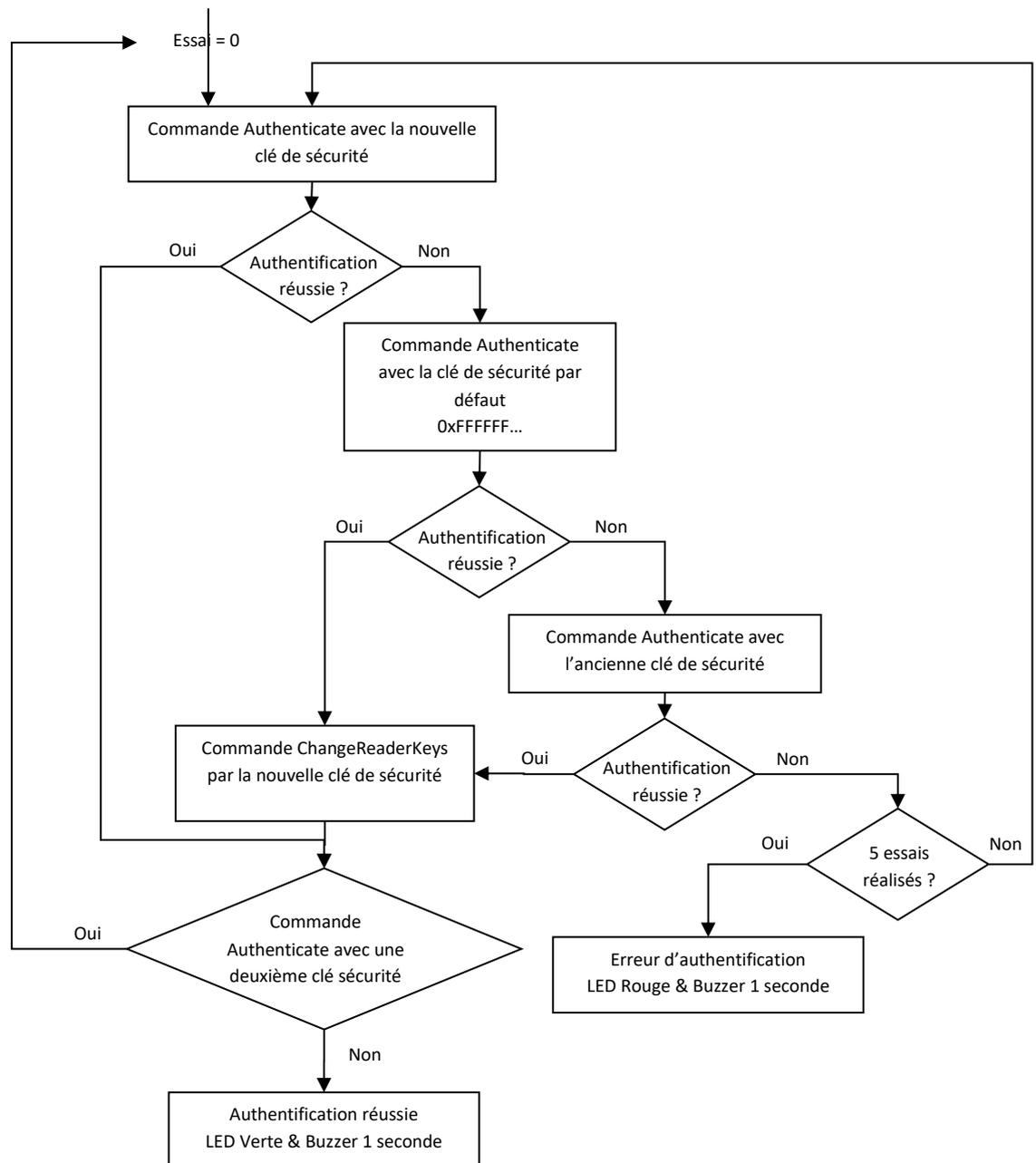
Les valeurs des clés utilisateurs de chiffrement et de signature peuvent être changées dans SECard. La modification de ces clés sera effectuée par une commande lecteur spéciale **ChangeReaderKeys** (décrite dans les spécifications protocoles **SSCP®**) transmise signée et chiffrée.

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 *Ajout fonctionnalité 3.6*

### 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 frame »**

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

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 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'

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

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 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'

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

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 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.

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.

000...	1101 0	0010 0	1010 1	1001 1	1111 1	xxxx x	000...
Zéros	Start	'4'	'5'	'9'	End	LRC	Zéros

0	0000	0000	0000	0100	0101	1001	1
Parité	'0'	'0'	'0'	'4'	'5'	'9'	Parité

Remarque

✓ Nombre de touches maximum = 8.

✓ \*x<sub>max</sub> = 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 – Touche ET Badge

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 <i>Format 4 bits</i>	Touche n°2 <i>Format 4 bits</i>	...	Identifiant <i>Format n bits</i> <i>(taille du protocole)</i>
------------------------------------	------------------------------------	-----	---

Exemple :

Trois touches : 7, 8, 9 / Identifiant 0x11223344 en hexadécimal soit 287454020 en décimal

Protocole Wiegand 3Cb → output = 0x**7890011223344**(+LRC)

Protocole Iso 2b → output = **7890000287454020**

## T6.3 - Lecteurs TTL - R31 - Badge OU Touche - Mode 26-bits Wiegand Nouveau 3.6

Dans ce mode, le code clavier est envoyé au système sous la forme d'un identifiant badge accolé à un code site défini dans le champ « Code site (FC) ».

# : valide la saisie du code PIN.

\* : annule la saisie du code PIN entrée précédemment, le lecteur émet 4 bips pour indiquer la prise en compte.

bit 1	bit 2 ... bit 9	bit 10 ... bit 25	bit 26
<i>Parité paire sur bit 2 ... bit 13</i>	<i>Code site FC (0 à 255) Se configure dans SECard bit 2 = MSB</i>	<i>Code PIN (0 à 65 535) Entré au clavier bit 10 = MSB</i>	<i>Parité impaire sur bit 14 ... bit 25</i>

Le code PIN « 65 535 » est réservé pour indiquer une erreur :

- La touche # est pressée en premier sans code à retourner.
- Le code PIN rentré = 0
- Le code PIN est supérieur ou égal à « 65 535 »

La parité est calculée par le lecteur.

Le temps de sauvegarde d'un appui touche en mémoire (sans appui sur # ou \*) est de 6 secondes.

Si ce temps est dépassé, le lecteur bip 4 fois pour indiquer que le time-out est atteint.

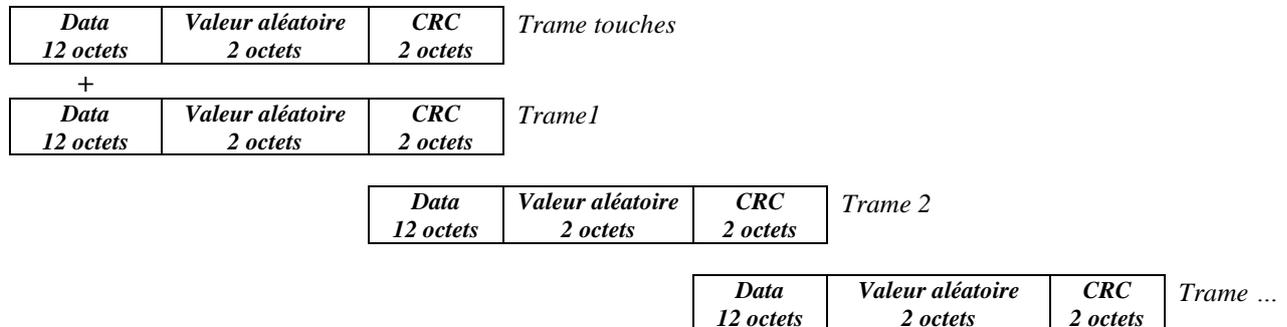
Sur un lecteur Ecran en mode Scramble, à l'appui sur la touche #, le lecteur, scramble le clavier.

Exemple avec Code Site= 121 et Code PIN 24568

1	0111	1001	0101	1111	1111	1000	0
<b>Parité</b>	'7'	'9'	'5'	'F'	'F'	'8'	<b>Parité</b>

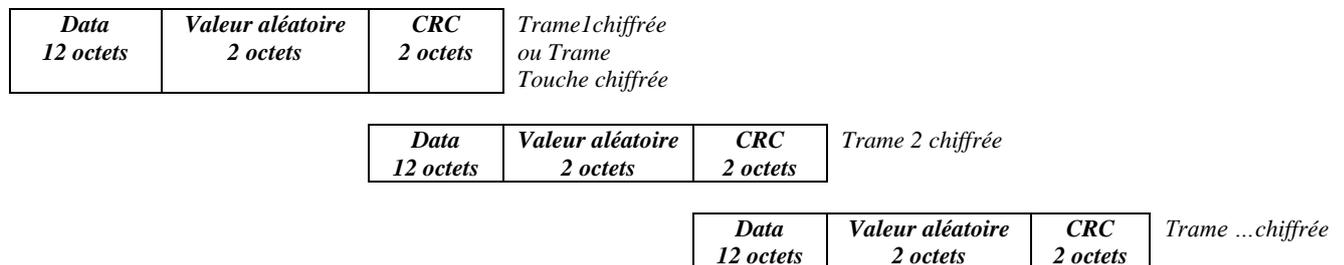
## T6.4 - Lecteurs TTL - S31 - Badge ET Touche

Les touches et l'UID/Id seront envoyés dans des trames qui se suivent.  
Le format des trames chiffrées sera :



## T6.5 - 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.



### 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

## T6.6 - 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<sub>out</sub> Data<sub>out</sub>

CommandCode 2 octets : 01h 07h

L<sub>out</sub> 2 octets : 00h 03h

Data<sub>out</sub> 3 octets : 00h 01h + Valeur de la touche lue récupérée au format 8 bits.

**Système** : ACK L<sub>in</sub> 00h 00h

ACK 2 octets : 01h 07h

L<sub>in</sub> 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.

## T6.7 - 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 : 0x87786911223344
- ✓ 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® EVx) 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® EVx ou secteur(s) MIFARE Plus® Level 3 :

<i>MSB</i>	<i>LSB</i>
<b>[LenTotale]   [Nb Template]   [LenTemplate<sub>x</sub>   Template<sub>x</sub>]<sup>n</sup></b>	

- ✓ **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<sub>x</sub>** est la longueur du Xème template sur 1 octet.
- ✓ **Template<sub>x</sub>** est le Xème template de longueur **LenTemplate<sub>x</sub>**.
- ✓ 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 :

$$\text{TemplateDerogation} = \text{SHA2}(\text{salt} \mid \text{UID}, \text{UIDLen})$$

- ✓ **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

### **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.

### **Mode 3** : Touche **OU** (Badge **ET** biométrie), mode 26-bit Wiegand

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.

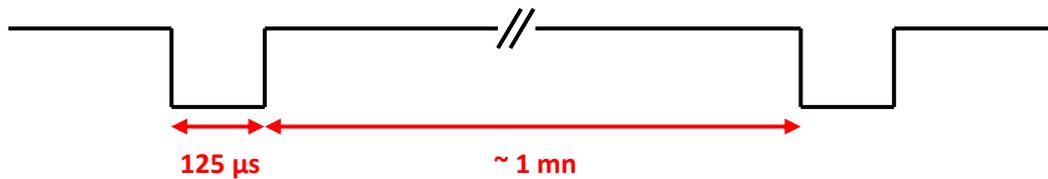
## T9 - Signal de vie

### T9.1 - Lecteur TTL

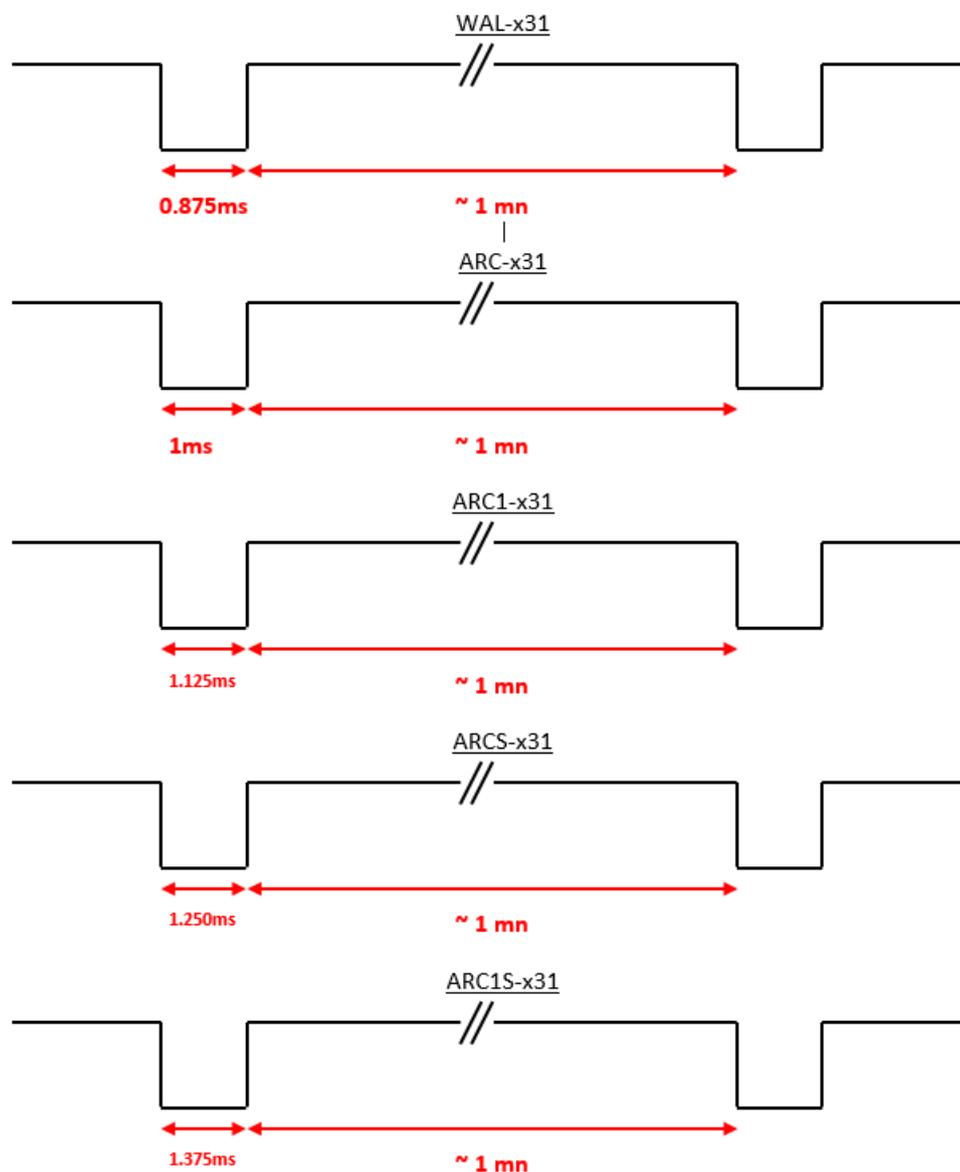
Lorsque cette fonction est activée, le lecteur émet un signal environ toutes les minutes sur les lignes Data/DATA1.

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*).

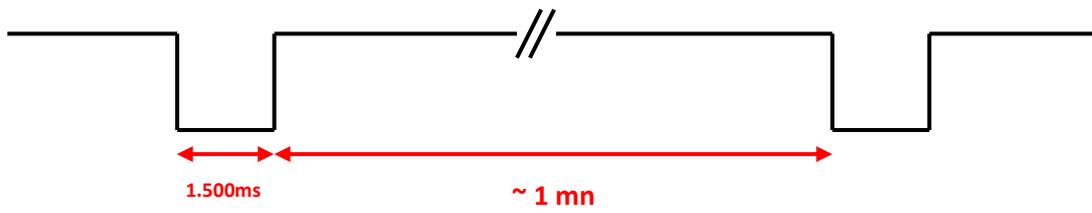
#### Signal de vie générique :



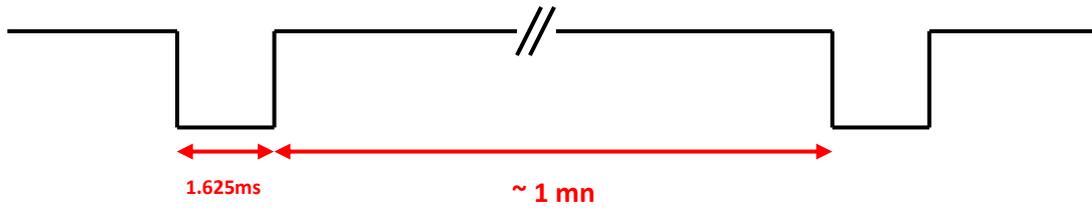
#### Signal de vie spécifique :



MS2-x31



MS2S-x31



## T9.2 - Lecteur série bidirectionnel

Le lecteur envoie en clair sur la série le code commande 0x0102.

Donnée =  $x * 125\text{us}$  (exemple : pour ARC-R32/R33,  $x = 8$ )

## T9.3 - Lecteur série unidirectionnel

Le lecteur envoie sur la série le code commande :

**Générique** : 0x50

**Spécifique** :

ARC-R32/R33= 0x61

ARC1-R33 = 0x62

ARCS-R33 = 0x63

ARC1S-R33 = 0x64

MS2-R31 = 0x65

MS2S-R31 = 0x66

**Spécifique Gamme E** :

LXS-R32/R33= 0x50

MS-R31 = 0x52

LXE-R32/R33 = 0x54

LXC-R32/R33 = 0x55

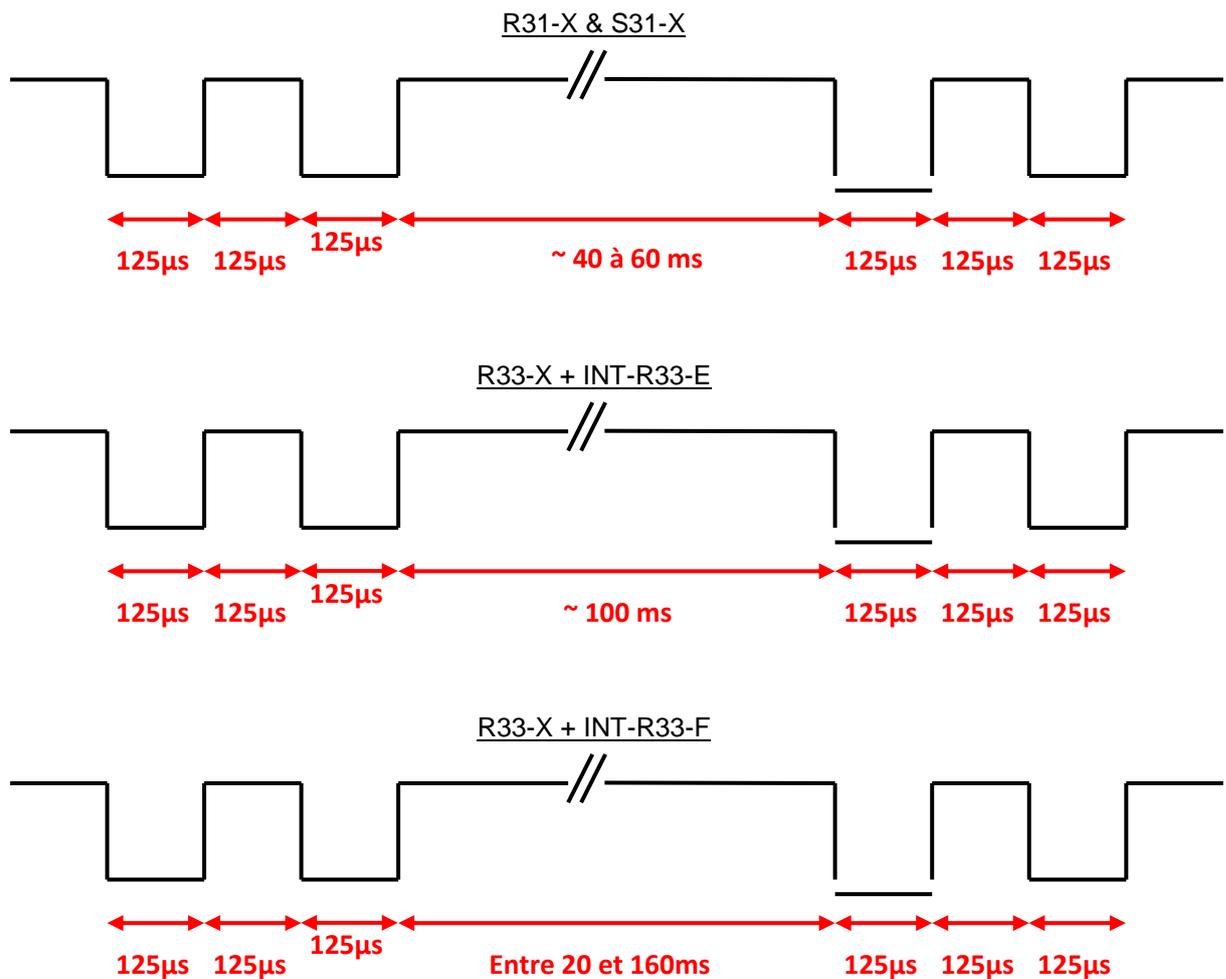
WAL-R32/R33 = 0x56

## T10 - Signal d'arrachement

Lorsque cette fonction est activée, le lecteur mémorise au démarrage l'état initial de son entrée « **Switch** » ou de l'accéléromètre.

### T10.1 - 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 :



### T10.2 - Lecteur série bidirectionnel

Le lecteur envoie en clair sur la série le code commande 0x0103.

### T10.3 - Lecteur série unidirectionnel

Le lecteur envoie sur la série le code commande 0xAA.

## T11 - 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.

## T12 - 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.

## T13 - Ligne de commande

### T13.1 - Description

SECard inclus un mode « ligne de commande » permettant une exécution « en tâche 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.

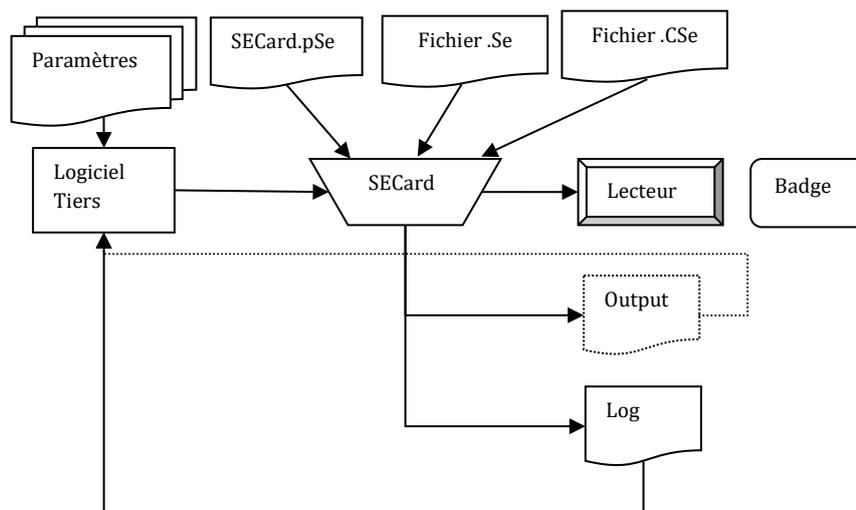
SECard permet de :

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 :



### T13.2 - 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 contenant les opérations réalisées par -a, si l'action réalisée est CSe2PSE le fichier de résultat sera le fichier PSE créé.

-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 gestion 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.

### T13.3 - Console de commande

Ouvrir une console de commande Windows : exécuter cmd.exe.

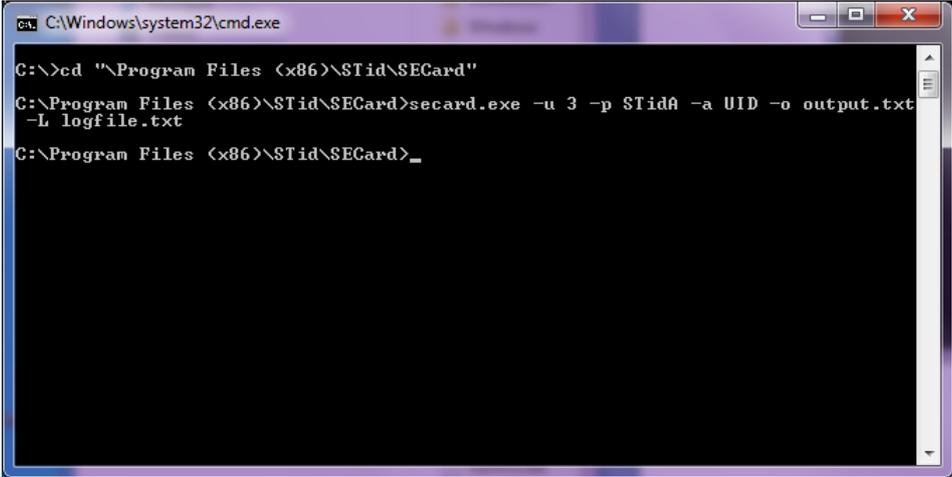
Dans la fenêtre qui s'ouvre, se positionner dans le répertoire d'installation de SECard :

```
cd \Program Files\STid\Secardvxxx\ ou cd \Program Files (x86)\SECardvxx\
```

Puis, taper la ligne de commande désirée.

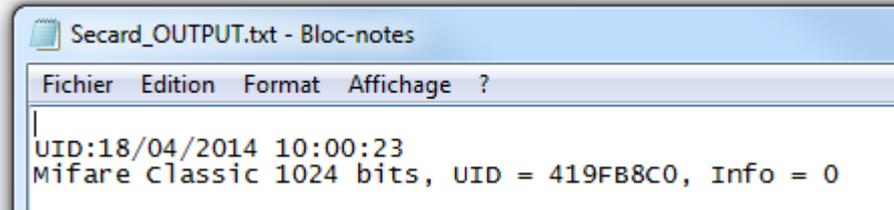
Par exemple, pour récupérer l'UID d'un badge :

Mettre un badge RFID devant le lecteur allumé et configuré dans SECard puis taper :



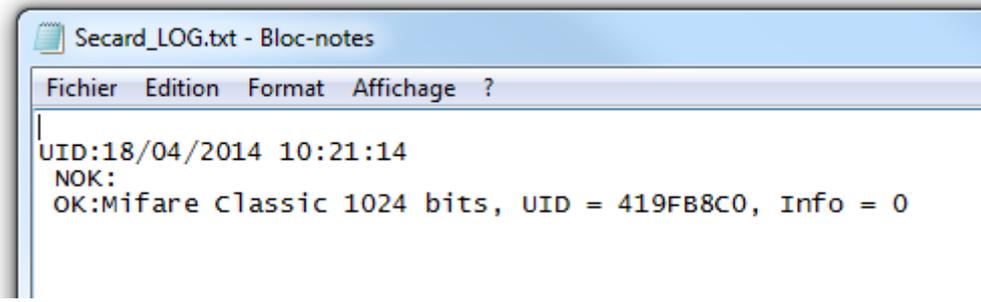
```
C:\Windows\system32\cmd.exe
C:\>cd "\Program Files (x86)\STid\SECard"
C:\Program Files (x86)\STid\SECard>secard.exe -u 3 -p STid0 -a UID -o output.txt
-L logfile.txt
C:\Program Files (x86)\STid\SECard>_
```

Le résultat de l'opération (donc l'UID du badge présenté au lecteur) est consigné dans le fichier output.txt.



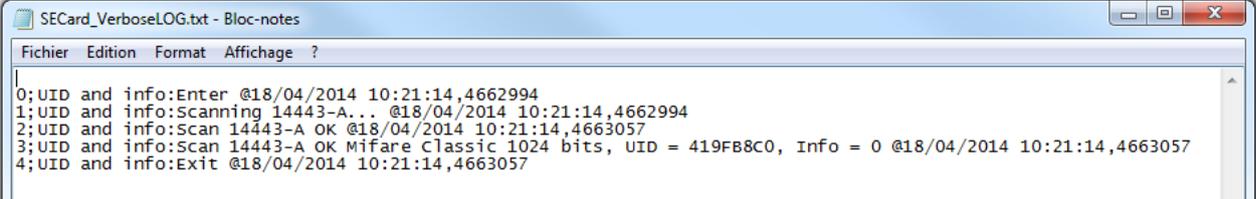
```
Secard_OUTPUT.txt - Bloc-notes
Fichier Edition Format Affichage ?
UID:18/04/2014 10:00:23
Mifare Classic 1024 bits, UID = 419FB8C0, Info = 0
```

Si l'opération s'est correctement déroulée, cela sera consigné dans le fichier de log logfile.txt.



```
UID:18/04/2014 10:21:14
NOK:
OK:Mifare Classic 1024 bits, UID = 419FB8C0, Info = 0
```

Si l'option -v verbose est utilisée le fichier de log créé est :



```
0;UID and info:Enter @18/04/2014 10:21:14,4662994
1;UID and info:Scanning 14443-A... @18/04/2014 10:21:14,4662994
2;UID and info:Scan 14443-A OK @18/04/2014 10:21:14,4663057
3;UID and info:Scan 14443-A OK Mifare Classic 1024 bits, UID = 419FB8C0, Info = 0 @18/04/2014 10:21:14,4663057
4;UID and info:Exit @18/04/2014 10:21:14,4663057
```

## T13.4 - Fichier batch

Grâce aux fichiers batch (exécutables 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
)
```

## T13.5 - 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` 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 apparaît (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) suivi 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 défini 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.

## T13.6 - 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.

```
:: SECard command line import configuration file
:: defines all parameters available in SECard command line mode from V3.6.0

[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
; 6 = SECard v3.3.0
; 7 = SECard v3.4.0
; 8 = SECard v3.5.0
ARCCompatibilityVersion=3
```

```
; For WAL family
; 0 = SECard v2.1.0
; 1 = SECard v2.2.0
WALCompatibilityVersion=0
```

```
[SSCP]
COMPort=COM4
```

```
;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  
;BKmode, =0 Badge OR Key, =1 Badge AND Key  
;SECard v3.6.0, add BKmode=2 =W3i card OR key, see below for KeyboardSiteCode  
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=0
NFC_HCEEnable=0
;SECard v3.6.0, Application Multiservices Citoyenne tag types to enable/disable 1/0
AMCTagEnable=0
```

```
;V3.0.0
;TagType
BlueMobileID=1
;Blue MobileID Configuration Activation
BlueMobileIDActivation=1
;DESFire Configuration Activation
DESFireConfigurationActivation=1
```

```
;PUPI ISO14443-3B
PUPIEnable=0
PUPIMSB=1
PUPISign=0
PUPISignKey=FFFFFFFFFFFFFFFFFFFFFFF
```

```
;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,11=Wiegand custom size,12=Wiegand 34 bits - 3Eb,13=Wiegand 35 bits - 3W,14=Wiegand 37 bits - 3V,
;+V3.3.0 16=PAC 32bits-5Pa, 17=PAC 64bits-5Pb
;+V3.6.0 18=W3Y Wiegand 38bits, 19=W3Z Wiegand 72bits
ProtocolID=5
```

```
;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=FFFFFFFFFFFFFFFFFFFFFFF
```

```

SCChangeSignKey=0
SCNewSignKey=FFFFFFFFFFFFFFFFFFFFFFF
SCEncKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
SCChangeEncKey=0
SCNewEncKey=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

;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
```

```
; V3.3.0  
; Duress biometric, 0 = disabled, 1 = enabled  
BioDuress=0  
; Auto change serial communication key 0 = disabled, 1 = enabled. For serial bidirectional readers or INTx  
AutoChangeSerialCommKey=1
```

```
;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 hexadecimal 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=0.2m, 2=0.3m, 3=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

::Added in SECard V3.4.0, begin  
;Biometric FakeFinger Detection (MorphoSagemIdemiaDevice/SupremaDevice), 0=Disabled, 1 =Low/Weak,  
2=Medium/Normal, 3=High/Strong,4 Critical  
BioFFD=0

;Mute all reader sound, to mute set to 1  
MuteAll=0

;CardDetectionCloseRelay close relay @ card detection during a delay, duration is in second from 1 to 20  
CardDetectionCloseRelay=0  
CardDetectionCloseRelayDuration=1

;BlueTooth External Hand, hand detection managed by external  
BTEExternalHand=0  
;Manage additionnal SAK and ATQA for specific smartphone, up to 3 new ATQASAK (hex value), 000000  
means not used, 4578A9 means new SAK=45 and new ATQA=78A9  
ATQASAK1=000000  
ATQASAK2=000000  
ATQASAK3=000000

::Added in SECard V3.4.0, end

::Added in SECard V3.5.0, begin  
; Reader Matrix Code settings : disable=0, enable=1  
DataMatrix=1

```
QRCode=1
AztecCode=1
Code128=1

;0=hex , 1=dev, 2=ASCII
MaxtrixCodeFormat=1

;DataMatrix Lightning Brightness 0/1
DataMatrixLB=1
;DataMatrix Lightning Target/aim 0,1,2
DataMatrixLT=2
;DataMatrix Detection sensitivity 0,1,2
DataMatrixDS=1
;DataMatrix Ambien light 0,1,2
DataMatrixAL=1
;;Added in SECard V3.5.0, end

;;Added in SECard V3.6.0, begin
;;Reader Prefix Suffix , max 5 bytes hexa string, ex Prefix=0A0102040F
Prefix=
Suffix=

;Reader adds IDLen, boolean value 1/0 to enable/disable
IDLen=0
;Reader adds IDTag, boolean value 1/0 to enable/disable
IDTag=0
;Command line Se import will use IDTagList defined in PSE

;W3i keyboard mode, site code value, one byte 0..255
KeyboardSiteCode=0

;Matrix code 39, boolean value 1/0 to enable/disable
Code39=1

;Keyboard backlight duration enable/diablenn 1/0, and value in second
TimedBacklight=0
BacklightDuration=6

;;Added in SECard V3.6.0, 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
8000000000000000000000000000000000000000000000000000000000000000
NXPPadding=0000000000000000000000000000000000000000000000000000000000000000

;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
GetUIDCurrentValue=0000000000000000000000000000000000000000000000000000000000000000
ChangeGetUIDKeyValue=0
GetUIDNewKeyValue=0000000000000000000000000000000000000000000000000000000000000000

;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 IDPrime 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=0
; 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

;; SECard v3.5.0
; UID MSB First ofr DESFire UID read mode, 0=disabled, 1=enabled

```

```
DESFireUIDMSBFirst=0
; If selected crypto is 3DES user can select divAV1 diversification; set to 1 to enable
DESFiredivAV1=0

[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 v3.2.1, ask user to first unlock (=1) his smartphone before authentication
BMIDLockVCard=0
;Added in SECard v3.3.0, forbid user (=1) to delete VCard from the mobile app
BMIDProhibitVCardDeletion=0

;;Added in SECard V3.1.0, begin
; If ARCBBlueMode=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 ARCBBlueMode=2=Open Mobile Protocol
;Complete local name, max 5 char
OMP_CLN=ARCoa
;Site Code two hexa bytes
OMP_SiteCode=51BC
;3 General purpose bytes
OMP_GPBS=000000
;To enable secure communication set to 1
OMP_SecureComm=0
;To set TX power dbm : 0=-16, 1=-12,2=-8,3=-4,4=0,5=4
OMP_TXPower=5
;To set CompanyID : two hexadecimal bytes, STid ID by default
OMP_CompanyId=51BC

;;Added in SECard V3.2.0, end

;;Added in SECard v3.4.0
;Request user for biometric smartphone unlock before any authentication
BMIDBioLockVCard=0
```

## T13.7 - 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  
192A31AB805D8239DC52D1F7F55DED1452DC2309824AB655E719371BD9A103D6AC0308EEDEA  
E57E0B14B978DA47A2DBE73377471132D05

;RSA\_priv1=PRIVATE

; Key for RSA 2048 bits

```
;RSA_pub2=E511A50D7CE6C94D37B99EA0206F5CBDB1402C5D20BA92CEFD29C1D553A645BCA  
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.

## T14 - Recommandations sur la sauvegarde des fichiers PSE

### T14.1 - 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 cryptés avec AES-CBC à l'aide de la clé utilisateur (k). Cette clé est générée à partir du mot de passe de connexion de l'utilisateur et utilise PBKDF2.

Ces fichiers sont inutilisables sans SECard. De plus, ils peuvent être verrouillés par un mot de passe de lecture, celui-ci sera alors demandé à l'ouverture, ce mot de passe utilise une clé de hachage.

### T14.2 - 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.

### T14.3 - 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..).

## T15 - 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.
- ✓ **AES-CBC** : Advanced Encryption Standard - Cipher Block Chaining (Enchaînement des blocs),
- ✓ **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.
- ✓ **Authentication** : 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® EVx.
- ✓ **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® EVx.
- ✓ **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.
- ✓ **OCB** : Badge de configuration des lecteurs OSDP.
- ✓ **PBKDF2**: fonction de dérivation de clé (Password-Based Key Derivation Function 2)
- ✓ **Private ID** : Code privé.
- ✓ **PUPI** : Numéro de série de la puce utilisé en 14443-B.
- ✓ **SCB** : Secured Configuration Badge (Badge de configuration des lecteurs).
- ✓ **SCB-R/W** : Badge de configuration des lecteurs Read/Write

- ✓ **SSCP**<sup>®</sup> : 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<sup>®</sup> DESFire<sup>®</sup> EV1 et MIFARE Plus<sup>®</sup> : AN-165310.pdf Méthode NXP MIFARE<sup>®</sup> SAM.
  - MIFARE<sup>®</sup> Classic : P5DF072EV2.pdf §8.6.1
  - MIFARE Ultralight<sup>®</sup> C : P5DF072EV2.pdf §8.6.2

## SECard V3.6 évolutions – version firmware Z17 / osdp-Z11

Date	Description
08/07/2021	<p><b>Ajout :</b></p> <ul style="list-style-type: none"> <li>- Compatibilité badges AMC.</li> <li>- Ajout ID-Tag, ID-Len, Préfixes et suffixes en mode série (R32/R33) et osdp.</li> <li>- Compatibilité des lecteurs écrans avec les caractères Islandais Ð Þ ð þ et Allemands Ü, ü, ß, ° et §</li> <li>- QR Code : Compatibilité avec le code 39.</li> <li>- QR Code : Gestion des Préfixes et suffixes.</li> <li>- Clavier : mode spécifique 26-bit Wiegand.</li> <li>- Clavier : mode rétro-éclairage avec timing.</li> <li>- Protocoles Wiegand 38 bits (W3Y) et Wiegand 72 bits (W3Z)</li> <li>- osdp : Création du fichier de configuration pour la commande FileTransfer.</li> <li>- osdp : Compatibilité avec STid Settings pour la configuration des lecteurs.</li> <li>- osdp : Modification du numéro IEEE + gestion du Legacy.</li> </ul>
	<p><b>Modification:</b></p> <ul style="list-style-type: none"> <li>- Utilisation uniquement de badge DESFire EV2/3 8 ko pour la création des SCB/OCB</li> <li>- CPS3 modification au niveau du timeout RF</li> </ul>
	<p><b>Suppression :</b></p> <ul style="list-style-type: none"> <li>- Mode Bio Hors CNIL (biométrie dans le lecteur)</li> </ul>

## REVISION

Date	Version	Description
10/03/2014	5.0	Création.
18/04/2014	5.1	<p>Modification des imprimés écran suite au retrait du point d'interrogation « A propos »</p> <p>Ajout « signal de vie et arrachement mutualisés » pour les lecteurs R33+HNTR33E (p25, 37, 128)</p> <p>Modification du champ Taille données (p22, 24, 34, 36)</p> <p>Ajout option -v verbeux en ligne de commande (p130, 132)</p>
28/11/2014	5.2	<p>Ajout référence encodeur ARC / Ajout installation certificat de sécurité / Modification tableau de compatibilité</p> <p>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 imprimés écrans.</p>
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	<p>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) /</p> <p>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. /</p> <p>Modification de tous les imprimés écrans</p>
19/12/2016	6.0	<p>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.</p> <p>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.</p>
04/08/2017	6.1	<p>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</p>
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	<p>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</p> <p>Partie 2 : T4.2 Ajout Protocol 3Eb 3V 3W // T13.6 Fichier d'import configuration modifié</p>
13/07/2018	6.4	Ajout NFC Mobile ID
17/12/2018	7.0	Ajout assistant OCB et SBC R/W // Ajout protocole PAC/PAC64 // Ajout Biométrie sous contrainte // Suppression de toutes les pages relatives aux lecteurs standards.
03/01/2020	7.1	Ajout fonctionnalités évolution 3.4
01/10/2020	7.2	Ajout fonctionnalités évolution 3.5
08/07/2021	7.3	Ajout fonctionnalités évolution 3.6

**Siège Social / EMEA**

13850 Gréasque, France  
Tél. : +33 (0)4 42 12 60 60

**Agence PARIS-IDF**

92290 Châtenay-Malabry, France  
Tél. : +33 (0)1 43 50 11 43

**STid UK Ltd. LONDRES**

Hayes UB11 1FW, UK  
Tél. : +44 (0) 192 621 7884

**STid UK Ltd.**

Gallows Hill, Warwick CV34 6UW, UK  
Tél. : +44 (0) 192 621 7884

**Agence AMÉRIQUE DU NORD**

Irving, Texas 75063-2670, USA  
Tél. : +1 469 524 3442

**Agence AMÉRIQUE LATINE**

Cuauhtémoc 06600 CDMX, México  
Tél. : +521 (55) 5256 4706



[info@stid.com](mailto:info@stid.com)

[www.stid-security.com](http://www.stid-security.com)