Gestion Code Pin sous Windows

V 1.0

22/05/2012
Français

Mention légale

Ce document ne peut être reproduit en totalité ou en partie sans le consentement écrit préalable et explicite de LuxTrust SA. Des droits d'auteur de tiers peuvent exister pour les parties de cette documentation. LuxTrust SA décline toute responsabilité pour les dommages directs, indirects, spéciaux, indirects ou consécutifs à des dommages matériels ou autres en quelque sorte liée à ou découlant de l'exécution de tous les conseils donnés dans le présent document. Ce document est fourni "tel quel" et rien n'est prévu en termes d'adéquation à un usage particulier ou de l'applicabilité. En faisant usage de ce document, l'utilisateur accepte de l'utiliser à ses propres risques et comprend que ce document ne peut être fourni sans ces limitations.

I.1 Eléments nécessaires avant d'exécuter la procédure de changement du code PIN

La présente procédure peut seulement être exécutée si vous avez auparavant :

- Valablement commandé un produit Signing Stick ou Smartcard (voir aussi http://orders.luxtrust.lu).
- Reçu par courrier la puce pour Signing Stick LuxTrust ou la Smartcard
- Reçu par courrier votre Signing Stick LuxTrust ou avoir acquis un lecteur Smartcard (voir aussi http://readers.luxtrust.lu) qui est branché à l'ordinateur.
- Reçu par courrier la lettre « LuxTrust Codes Document » qui contient le « PIN » (numéro personnel d'identification), « PUK » (clé de déblocage personnelle) et « Challenge ». Cette lettre vous parvient en général 2 à 3 jours après la réception de votre puce Signing Stick LuxTrust ou de votre Smartcard.
- Installé le middleware correspondant à votre système d'exploitation Microsoft Windows (voir aussi http://drivers.luxtrust.lu).

II Changer le PIN

Les utilisateurs qui veulent débloquer le code Pin à l'aide du code Puk, veuillez avancer jusqu'à la figure 6.

Branchez le Signing Stick à un port USB libre ou insérez la Smartcard dans le lecteur de cartes branché à l'ordinateur.

Lancez le Middleware « Classic Client Toolbox » à partir du menu « Start » (Démarrer) – « Programs » (Tous les programmes) – « Gemalto » *(voir flèche rouge dans la figure 1).*

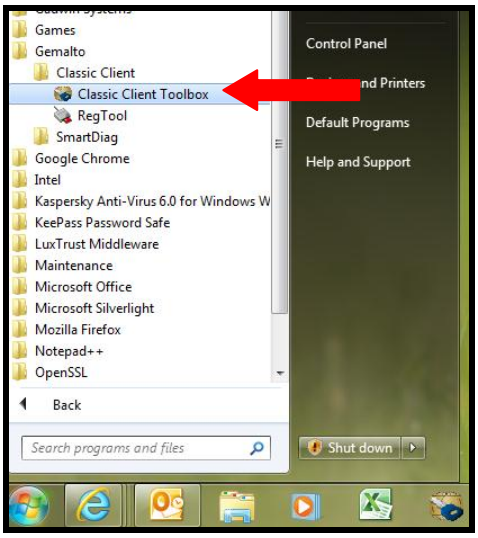

Figure 1

Vous verrez la fenêtre suivante s'afficher sur votre écran:

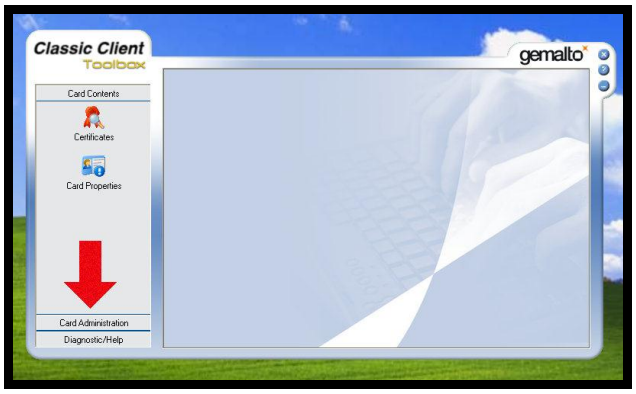

Figure 2

Cliquez sur « Card Administration » (Administration carte) *(voir flèche rouge dans la figure 2).*

Puis sélectionnez « PIN Management » *(voir première flèche rouge sur la figure 3).*

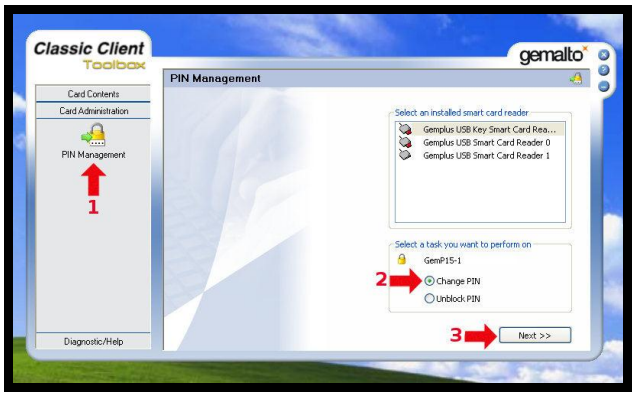

Figure 3

Cochez le bouton « Change PIN » (Changer PIN) *(voir deuxième flèche rouge sur la figure 3)* et cliquez sur le bouton « Next » (Suivant) *(voir troisième flèche rouge sur la figure 3).* La fenêtre suivante s'affichera :

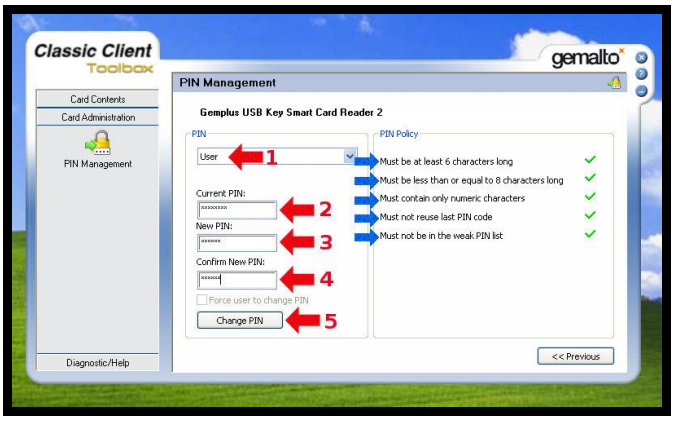

Figure 4

Assurez-vous que le menu déroulant affiche bien « User » et non **pas** « Admin ». *(voir première flèche rouge dans la figure 4)*

Entrez le « Current PIN » (PIN actuel) *(voir deuxième flèche rouge sur la figure 4).*

Entrez un nouveau PIN dans la case intitulée « New PIN » (nouveau PIN) *(voir troisième flèche rouge dans la figure 4).* Le nouveau PIN est choisi par vous-même en respectant les consignes telles que renseignées sur la partie droite *(voir flèches bleues dans la figure 4)* :

- « must be at least 6 characters long » (doit avoir au moins six caractères) *(voir première flèche bleue sur la figure 4).*
- « must be less than or equal to 8 characters long » (doit avoir moins de huit ou exactement huit caractères) *(voir la deuxième flèche bleue sur la figure 4).*
- « must contain only numeric characters » (doit contenir uniquement des caractères numériques) *(voir la troisième flèche bleue sur la figure 4).*
- « must not reuse last PIN code » (ne doit pas réutiliser le dernier code PIN) *(voir la quatrième flèche bleue sur la figure 4).*
- « must not be in the weak PIN list » (ne doit pas être dans la liste des PINs faibles) *(voir la cinquième flèche bleue sur la figure 4).*

La liste des PINs faibles contient des PINs facilement devinables. Ces PINs sont refusés par l'application.

Quelques conseils pour le choix d'un bon PIN :

- il est préférable de choisir plutôt un PIN avec 8 chiffres que d'en choisir un avec 6 ou 7 chiffres;
- évitez une suite de chiffres facilement devinables comme, par exemple, la date de naissance, le numéro de téléphone, …
- évitez des suites logiques comme par exemple 123456, 12131415, 102030, …
- évitez de répéter le même chiffre plusieurs fois comme par exemple 222888, 55555555, …
- évitez l'usage de canevas répétitifs ou symétriques comme par exemple 01010101, 45674567, 8091908, …
- évitez l'usage de suites de chiffres très connues comme par exemple 112112, 925925, …

Quelques conseils de sécurité :

- ne jamais noter le PIN sur le Signing Stick ou Smartcard. Celui qui trouve le Signing Stick ou la Smartcard pourra tout de suite l'utiliser.
- ne jamais conserver le PIN ensemble avec le Signing Stick ou Smartcard. Une personne qui trouve le Signing Stick ou Smartcard, trouve également le PIN pour l'utiliser.
- ne jamais noter le PIN quelque part. Une personne étrangère pourra trouver cette note et l'utiliser avec le Signing Stick ou la Smartcard.
- ne jamais communiquer le PIN à une autre personne. Le Signing Stick ou la Smartcard est nominatif et ne peut pas être transmis à une autre personne.

Mémorisez le nouveau PIN !!!

Dans le futur, c'est le nouveau PIN que vous avez choisi vous-même qu'il faudra utiliser pour vous connecter à une application (par exemple : web banking, ccp connect, s-net, dexiaplus, guichet.lu, …) ou pour signer (MS Outlook, MS Word, …).

Entrez le nouveau PIN encore une fois dans la case libellée « confirm New PIN » (Confirmer le nouveau PIN) *(voir quatrième flèche rouge sur la figure 4).*

Cliquez sur le bouton « Unblock PIN » (débloquer PIN) pour valider le changement du code PIN *(voir cinquième flèche rouge sur figure 4).*

Le message représenté par la figure 5 confirme que le PIN a bien été changé. Cliquez sur le bouton « OK » *(voir flèche rouge dans la figure 5)* pour terminer le processus de changement de PIN.

Figure 5

III Débloquer le code PIN

Branchez le Signing Stick à un port USB libre ou insérez la Smartcard dans le lecteur de cartes branché à l'ordinateur.

Lancez le Middleware « Classic Client Toolbox » à partir du menu « Start » (Démarrer) – « Programs » (Tous les programmes) – « Gemalto » *(voir flèche rouge dans la figure 6).*

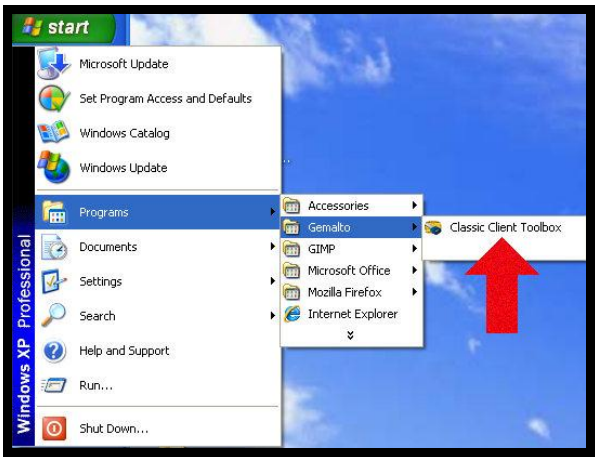

Figure 6

Vous verrez la fenêtre suivante s'afficher sur votre écran:

Figure 7

Cliquez sur « Card Properties » *(voir flèche rouge dans la figure 7).*

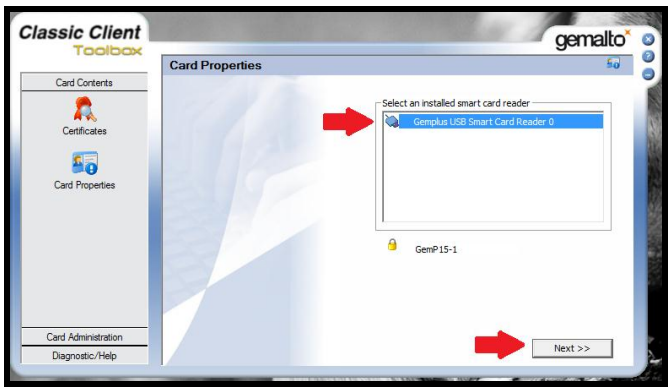

Figure 8

Sélectionnez le lecteur et puis validez votre choix en cliquant sur « Next » (voir flêches rouges sur la figure 8)

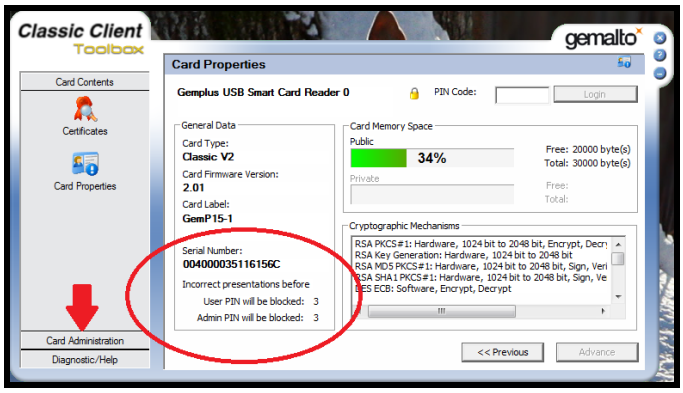

Figure 9

Les compteurs qui s'affichent dans le Middleware dans le menu « Card Properties » devraient afficher 0 pour le champ « User PIN will be blocked » et 3 pour le champ « Admin PIN will be blocked » *(voir oval rouge dans la figure 9).* Ces compteurs vous affichent les nombres d'essais restants pour entrer le bon code PIN ou Admin PIN (PUK).

Cliquez sur « Card Administration » (Administration carte) *(voir flèche rouge sur la figure 9*).

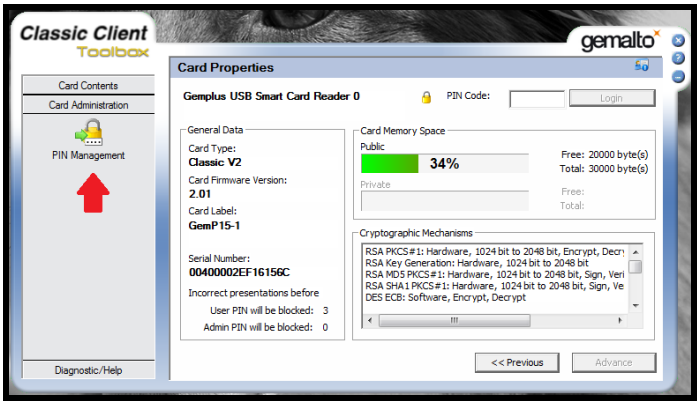

Figure 10

Puis sélectionnez « PIN Management » *(voir première flèche rouge sur la figure 10).*

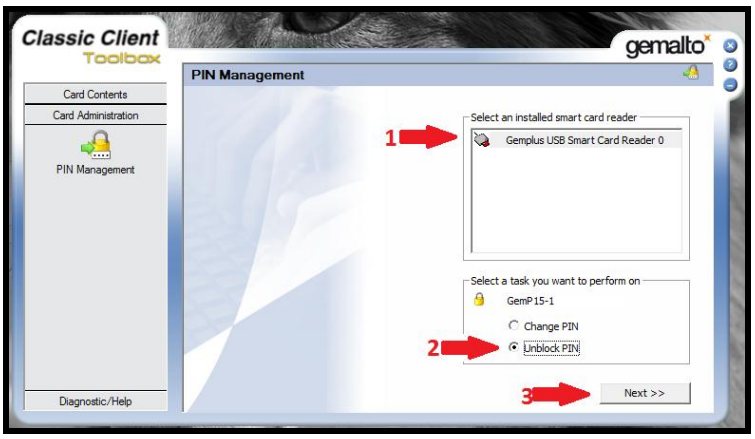

Figure 11

Sélectionnez le lecteur (voir flèche rouge 1 sur la figure 6) puis cochez le bouton « Unblock Pin » (voir flèche rouge 2 sur la figure 11) et validez en cliquant sur « Next » (voir flèche rouge 3 sur la figure 11).

La fenêtre suivante s'affichera:

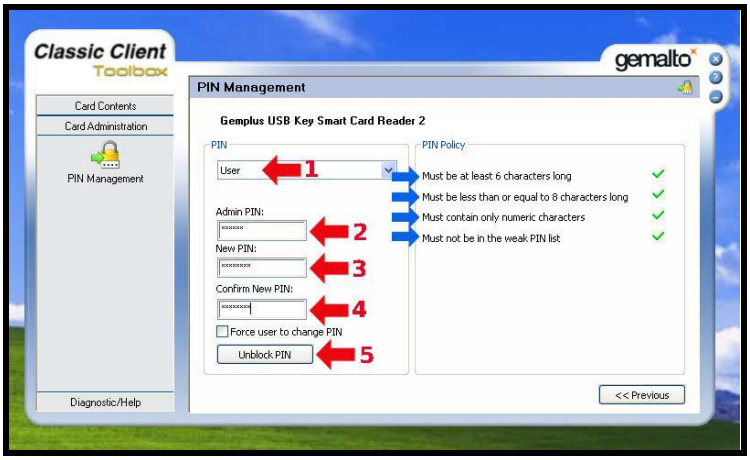

Figure 12

Assurez-vous que le menu déroulant affiche bien « User ». *(voir première flèche rouge dans la figure 12)*

Entrez le « Admin Pin » (Code PUK) *(voir deuxième flèche rouge sur la figure 12).*

Entrez un nouveau PIN dans la case intitulée « New PIN » (nouveau PIN) *(voir troisième flèche rouge dans la figure 12).* Le nouveau PIN est choisi par vous-même en respectant les consignes telles que renseignées sur la partie droite *(voir flèches bleues dans la figure 12)* :

- « must be at least 6 characters long » (doit avoir au moins six caractères) *(voir première flèche bleue sur la figure 12).*
- « must be less than or equal to 8 characters long » (doit avoir moins de huit ou exactement huit caractères) *(voir la deuxième flèche bleue sur la figure 12).*
- « must contain only numeric characters » (doit contenir uniquement des caractères numériques) *(voir la troisième flèche bleue sur la figure 12).*
- « must not reuse last PIN code » (ne doit pas réutiliser le dernier code PIN) *(voir la quatrième flèche bleue sur la figure 12).*
- « must not be in the weak PIN list » (ne doit pas être dans la liste des PINs faibles) *(voir la cinquième flèche bleue sur la figure 12).*

La liste des PINs faibles contient des PINs facilement devinables. Ces PINs sont refusés par l'application.

Quelques conseils pour le choix d'un bon PIN :

- il est préférable de choisir plutôt un PIN avec 8 chiffres que d'en choisir un avec 6 ou 7 chiffres;
- évitez une suite de chiffres facilement devinables comme, par exemple, la date de naissance, le numéro de téléphone, …
- évitez des suites logiques comme par exemple 123456, 12131415, 102030, …
- évitez de répéter le même chiffre plusieurs fois comme par exemple 222888, 55555555, …
- évitez l'usage de canevas répétitifs ou symétriques comme par exemple 01010101, 45674567, 8091908, …
- évitez l'usage de suites de chiffres très connues comme par exemple 112112, 925925, …

Quelques conseils de sécurité :

- ne jamais noter le PIN sur le Signing Stick ou Smartcard. Celui qui trouve le Signing Stick ou la Smartcard pourra tout de suite l'utiliser.
- ne jamais conserver le PIN ensemble avec le Signing Stick ou Smartcard. Une personne qui trouve le Signing Stick ou Smartcard, trouve également le PIN pour l'utiliser.
- ne jamais noter le PIN quelque part. Une personne étrangère pourra trouver cette note et l'utiliser avec le Signing Stick ou la Smartcard.
- ne jamais communiquer le PIN à une autre personne. Le Signing Stick ou la Smartcard est nominatif et ne peut pas être transmis à une autre personne.

Mémorisez le nouveau PIN !!!

Dans le futur, c'est le nouveau PIN que vous avez choisi vous-même qu'il faudra utiliser pour vous connecter à une application (par exemple : web banking, ccp connect, s-net, bilnet guichet.lu, …) ou pour signer (MS Outlook, MS Word, …).

Entrez le nouveau PIN encore une fois dans la case libellée « confirm New PIN » (Confirmer le nouveau PIN) *(voir quatrième flèche rouge sur la figure 12).*

Cliquez sur le bouton « Unblock PIN » (débloquer PIN) pour valider le changement du code PIN *(voir cinquième flèche rouge sur figure 12).*

Le message représenté par la figure 13 confirme que le PIN a bien été changé. Cliquez sur le bouton « OK » *(voir flèche rouge dans la figure 13)* pour terminer le processus de changement de PIN.

Figure 13

UG-0236

Gestion Pin Mac OS X

V 1.0

23/05/2012
Français

Mention légale

Ce document ne peut être reproduit en totalité ou en partie sans le consentement écrit préalable et explicite de LuxTrust SA. Des droits d'auteur de tiers peuvent exister pour les parties de cette documentation. LuxTrust SA décline toute responsabilité pour les dommages directs, indirects, spéciaux, indirects ou consécutifs à des dommages matériels ou autres en quelque sorte liée à ou découlant de l'exécution de tous les conseils donnés dans le présent document. Ce document est fourni "tel quel" et rien n'est prévu en termes d'adéquation à un usage particulier ou de l'applicabilité. En faisant usage de ce document, l'utilisateur accepte de l'utiliser à ses propres risques et comprend que ce document ne peut être fourni sans ces limitations.

I Eléments nécessaires avant d'exécuter la procédure de changement du code PIN

La présente procédure peut seulement être exécutée si vous avez auparavant :

- Valablement commandé un produit Signing Stick ou Smartcard (voir aussi http://orders.luxtrust.lu).
- Reçu par courrier la puce pour Signing Stick LuxTrust ou la Smartcard
- Reçu par courrier votre Signing Stick LuxTrust ou avoir acquis un lecteur Smartcard (voir aussi http://readers.luxtrust.lu) qui est branché à l'ordinateur.
- Reçu par courrier la lettre « LuxTrust PIN-Mailer » qui contient le « PIN » (numéro personnel d'identification), « PUK » (clé de déblocage personnelle) et « Challenge ». Cette lettre vous parvient en général 2 à 3 jours après la réception de votre puce Signing Stick LuxTrust ou de votre Smartcard.
- Avoir installé le middleware correspondant à votre système d'exploitation Microsoft Windows (voir aussi http://drivers.luxtrust.lu).

II Changer le Code Pin

Clients qui veulent débloquer le code Pin, veuillez avancer à la Figure 3 : Débloquer Code Pin

Insérez le Signing Stick dans un port USB libre ou insérez la Smartcard dans le lecteur de carte.

Lancer le Middleware « Classic Client PIN Management » à partir du répertoire « Gemalto » à l'intérieur du répertoire « Applications » (Applications) *(voir figure 1).*

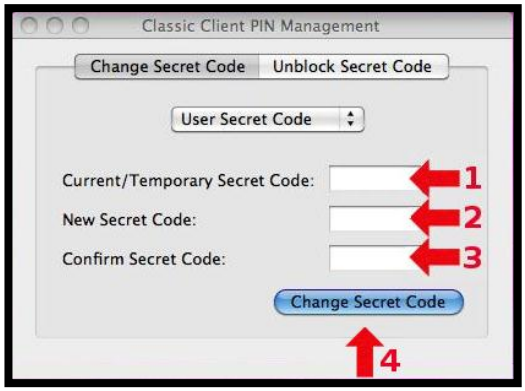

Figure 1

Si vous ne trouvez pas le Middleware « Classic Client PIN Management » dans l'endroit indiqué, veuillez utiliser « Spotlight » en cliquant sur le symbole « Loupe » en haut à droite de l'écran et tapez « classic ». Un des premiers résultats affichés est le Middleware « Classic Client PIN Management ». Cliquez dessus pour retrouver la fenêtre montrée par la figure 1.

1. Entrez le PIN actuel dans la case libellée « Current/Temporary Secret Code » *(voir première flèche rouge sur la figure 1)*.
2. Entrez un nouveau PIN dans la case intitulée « New Secret Code» (Nouveau code secret) *(voir deuxième flèche rouge sur la figure 1).*

   a) doit avoir au moins six chiffres ;

   b) doit avoir moins de huit ou exactement huit chiffres ;

   c) doit contenir des uniquement des chiffres;

   d) ne doit pas réutiliser le dernier code PIN ;

   e) ne doit pas être dans la liste des PINs faibles.
3. Entrez le nouveau PIN encore une fois dans la case libellée « Confirm Secret Code » (Confirmer le nouveau code secret) (voir troisième flèche rouge sur la figure 1).
4. Validez votre changement du code Pin en cliquant sur « change Secret Code » (voir quatrième flèche rouge sur la figure 1)

La liste des PINs faibles contient des PINs facilement devinables (p.ex. 000000, 111111, …). Ces PINs sont automatiquement refusés par l'application.

Quelques conseils pour le choix d'un bon PIN :

- il est préférable de choisir plutôt un PIN avec 8 chiffres que d'en choisir un avec 6 ou 7 chiffres;
- évitez une suite de chiffres facilement devinables comme, par exemple, la date de naissance, le numéro de téléphone, …
- évitez des suites logiques comme par exemple 123456, 12131415, 102030, …
- évitez de répéter le même chiffre plusieurs fois comme par exemple 222888, 55555555, …
- évitez l'usage de canevas répétitifs ou symétriques comme par exemple 01010101, 45674567, 8091908, …
- évitez l'usage de suites de chiffres très connues comme par exemple 112112, 925925, …

Quelques conseils de sécurité :

- ne jamais noter le PIN sur la Smartcard ou le Signing Stick. Celui qui trouve la Smartcard ou le Signing Stick pourra tout de suite l'utiliser.
- ne jamais conserver le PIN ensemble avec la Smartcard. Une personne qui trouve la Smartcard ou le Signing Stick, trouve également le PIN pour l'utiliser.
- ne jamais noter le PIN quelque part. Une personne étrangère pourra trouver cette note et l'utiliser avec la Smartcard ou le Signing Stick.

- ne jamais communiquer le PIN à une autre personne. La Smartcard ou le Signing Stick est nominative et ne peut pas être transmise à une autre personne.

Mémorisez le nouveau PIN !!!

Dans le futur, c'est le nouveau PIN que vous avez choisi vous-même, qu'il faudra utiliser pour vous connecter à une application (par exemple : web banking, ccp connect, s-net, Bil net, guichet.lu, …).

Le message représenté par la figure 2 confirme que le PIN a bien été changé. Cliquez sur le bouton « OK » *(voir flèche rouge dans la figure 2)* pour terminer le processus.

Figure 2

III Débloquer le code Pin

Insérez le Signing Stick dans un port USB libre ou insérez la Smartcard dans le lecteur de carte.

Lancer le Middleware « Classic Client PIN Management » à partir du répertoire « Gemalto » à l'intérieur du répertoire « Applications » (Applications) *(voir figure 3).*

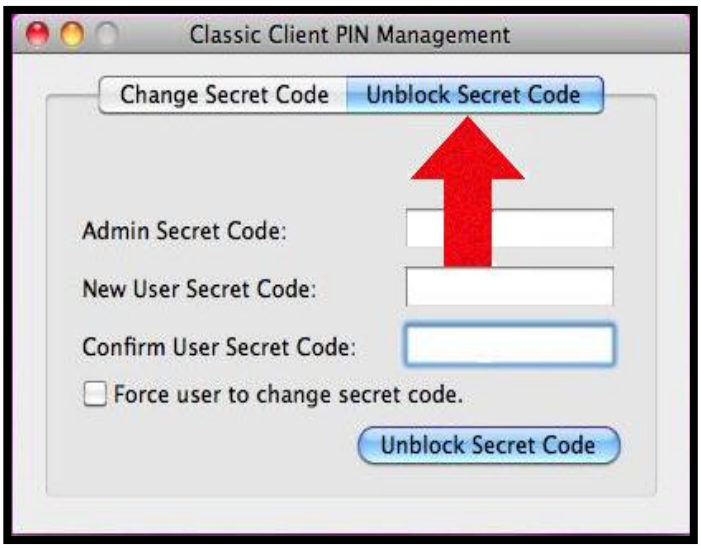

Figure 3

Cliquer sur « Unblock Secret Code » *(voir fleche rouge dans la figure 3).*

La fenêtre suivante va apparaître:

Figure 4

5. Entrez l'Admin Pin/PUK de la Lettre LuxTrust Codes dans la case libellée « Admin Secret Code » *(voir première flèche rouge sur la figure 4)*.

6. Entrez un nouveau PIN dans la case intitulée « New User Secret Code» (Nouveau code secret) *(voir deuxième flèche rouge sur la figure 4).*

   f) doit avoir au moins six chiffres ;

   g) doit avoir moins de huit ou exactement huit chiffres ;

   h) doit contenir des uniquement des chiffres;

   i) ne doit pas réutiliser le dernier code PIN ;

   j) ne doit pas être dans la liste des PINs faibles.

7. Entrez le nouveau PIN encore une fois dans la case libellée « Confirm User Secret Code » (Confirmer le nouveau code secret) (voir troisième flèche rouge sur la figure 4).

8. Validez votre changement du code Pin en cliquant sur « Unblock Secret Code » (voir quatrième flèche rouge sur la figure 4)

La liste des PINs faibles contient des PINs facilement devinables (p.ex. 000000, 111111, …). Ces PINs sont automatiquement refusés par l'application.

Quelques conseils pour le choix d'un bon PIN :

- il est préférable de choisir plutôt un PIN avec 8 chiffres que d'en choisir un avec 6 ou 7 chiffres;
- évitez une suite de chiffres facilement devinables comme, par exemple, la date de naissance, le numéro de téléphone, …
- évitez des suites logiques comme par exemple 123456, 12131415, 102030, …

- évitez de répéter le même chiffre plusieurs fois comme par exemple 222888, 55555555, …
- évitez l'usage de canevas répétitifs ou symétriques comme par exemple 01010101, 45674567, 8091908, …
- évitez l'usage de suites de chiffres très connues comme par exemple 112112, 925925, …

Quelques conseils de sécurité :

- ne jamais noter le PIN sur la Smartcard ou le Signing Stick. Celui qui trouve la Smartcard ou le Signing Stick pourra tout de suite l'utiliser.
- ne jamais conserver le PIN ensemble avec la Smartcard. Une personne qui trouve la Smartcard ou le Signing Stick, trouve également le PIN pour l'utiliser.
- ne jamais noter le PIN quelque part. Une personne étrangère pourra trouver cette note et l'utiliser avec la Smartcard ou le Signing Stick.
- ne jamais communiquer le PIN à une autre personne. La Smartcard ou le Signing Stick est nominative et ne peut pas être transmise à une autre personne.

Mémorisez le nouveau PIN !!!

Dans le futur, c'est le nouveau PIN que vous avez choisi vous-même, qu'il faudra utiliser pour vous connecter à une application (par exemple : web banking, ccp connect, s-net, Bil net, guichet.lu, …).

Le message représenté par la figure 5 confirme que le PIN a bien été débloqué. Cliquez sur le bouton « OK » *(voir flèche rouge dans la figure 5)* pour terminer le processus.

.

Figure 5