



Guide utilisateur

Gestion Pin Mac OSX

Document reference:

UG-0236

Date issued:

24/03/2017

Version: 1.0

LuxTrust S.A
IVY Building | 13-15, Parc d'activités | L-8308 Capellen
Luxembourg | VAT LU 20976985 | RCS B112233
Business Number N°00135240/0
Phone: +352 26 68 15 – 1
Fax: +352 26 68 15 – 789

Mention légale

Ce document ne doit pas être reproduit, ni dans son entièreté, ni en partie, sans l'accord préalable écrit et explicite de LuxTrust S.A. Des droits d'auteur de parties tierces peuvent exister pour des éléments de cette documentation. LuxTrust S.A. décline toute responsabilité pour dommages directs, indirects, spéciaux, occasionnels ou résultant de dommages dus à du matériel informatique, des logiciels, des données (corruption ou perte) ou pour d'autres dommages liés ou étant la conséquence de l'exécution de quelque conseil donné dans ce document. Ce document est mis à disposition « tel quel » et aucune garantie n'est donnée en termes d'adaptation à une finalité particulière ou d'applicabilité. En faisant usage de ce document, l'utilisateur accepte de l'utiliser sous sa seule responsabilité et reconnaît que ce document ne pouvait pas être mis à disposition sans de telles restrictions.

TABLE OF CONTENTS

Guide utilisateur.....	1
-------------------------------	----------

Comment commander un produit Signing Server Token ?Error! Bookmark not defined.

1. Commande sur le site Internet LuxTrust.....	4
---	----------

2. Détails avant de commencer la commande Error! Bookmark not defined.	
---	--

3. Commander un Token.....	Error! Bookmark not defined.
-----------------------------------	-------------------------------------

Etape 1 – Données qui apparaîtront dans le certificat**Error! Bookmark not defined.**

Etape 2 – Données qui n'apparaîtront pas dans le certificat**Error! Bookmark not defined.**

Etape 3 – Gestion des adresses **Error! Bookmark not defined.**

Etape 4 – Choix de l'autorité d'enregistrement**Error! Bookmark not defined.**

Récapitulatif **Error! Bookmark not defined.**

Choix du mode paiement..... **Error! Bookmark not defined.**

Confirmation de la commande... **Error! Bookmark not defined.**

1. Éléments 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>).

2. Changer le Code Pin

Clients qui veulent débloquer le code Pin, veuillez avancer à la Figure 3 : Débloquent 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).

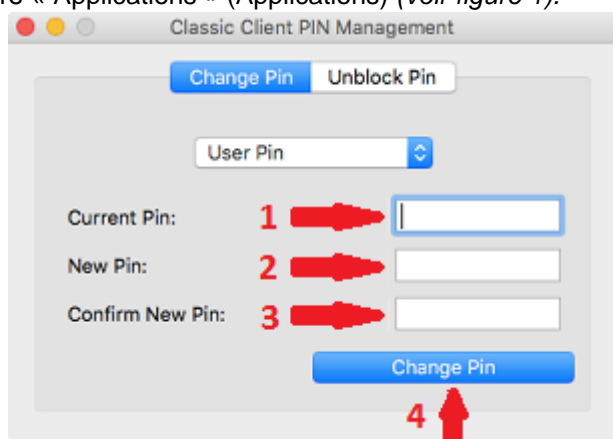


Figure 1

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 Pin** » (voir première flèche rouge sur la figure 1).
2. Entrez le nouveau PIN dans la case intitulée « **New Pin** » (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 New Pin** » (voir troisième flèche rouge sur la figure 1).
 4. Validez votre changement du code Pin en cliquant sur « **Change Pin** » (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.

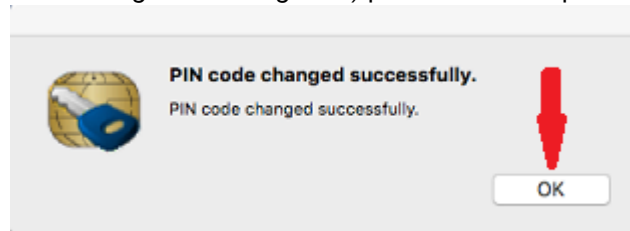


Figure 2

3. 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*).

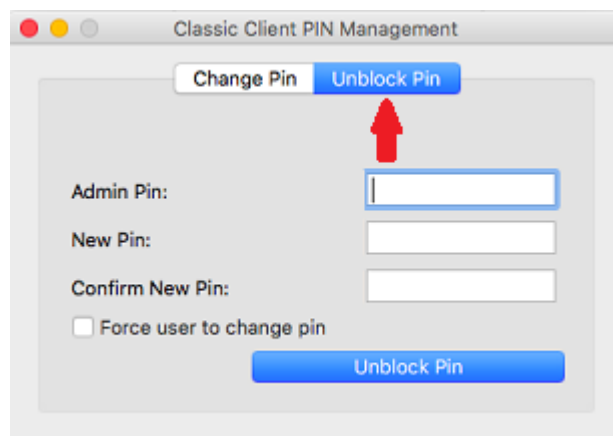


Figure 3

Cliquer sur « **Unblock Pin** » (voir *flèche rouge dans la figure 3*).

La fenêtre suivante va apparaître:

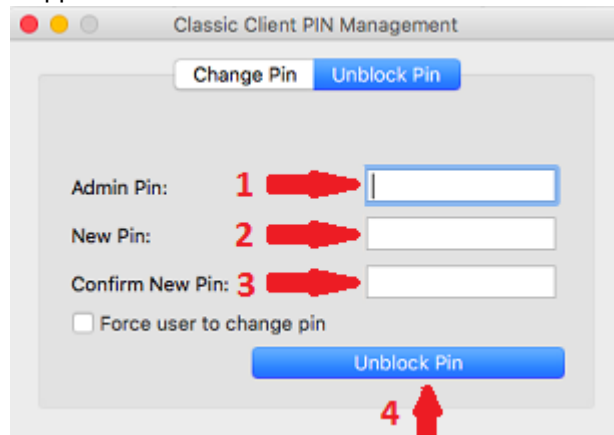


Figure 4

5. Entrez l'Admin Pin/PUK de la Lettre LuxTrust Codes dans la case libellée « **Admin Pin** » (voir première flèche rouge sur la figure 4).
6. Entrez un nouveau PIN dans la case intitulée « **New Pin** » (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 New Pin** » (voir troisième flèche rouge sur la figure 4).
8. Validez votre changement du code Pin en cliquant sur « **Unblock Pin** » (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.

Mémo r i s e z l e n o u v e a u P I N !!!

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.

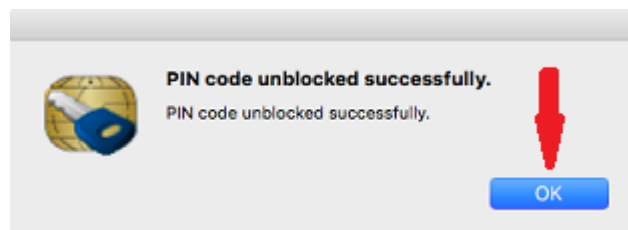


Figure 5

4.