



Procédure de déblocage du PIN sous un
système d'exploitation
Microsoft Windows

V 1.0

10/02/2010
français

Disclaimer

This document may not be reproduced as a whole or parts of it without the prior written and explicit consent of LuxTrust S.A.. Third party copyrights may exist for parts of this documentation. LuxTrust S.A. declines all responsibility for direct, indirect, special, incidental or consequential damages to hardware or other damages somehow related to or resulting from the execution of any advice given in this document. This document is provided “as is” and no provision is made in terms of fitness for a particular purpose or applicability. By making use of this document the user accepts using it to its own risk and understands that this document could not be provided without such limitations.

Table des matières

I	Avant de commencer : pré-requis.....	3
I.1	Champ de couverture de ce guide	3
I.2	Éléments nécessaires avant d’exécuter la procédure d’activation.....	3
I.3	Vocabulaire.....	4
II	Changer le PIN	5

I Avant de commencer : pré-requis

I.1 Champ de couverture de ce guide

Le présent document couvre les étapes nécessaires au déblocage du code PIN.

Le présent document est applicable pour les **systèmes d'exploitation** suivants :

- Microsoft Windows XP
- Microsoft Windows Vista 32 bit
- Microsoft Windows Vista 64 bit
- Microsoft Windows 7 32 bit
- Microsoft Windows 7 64 bit

D'autres guides pour d'autres produits respectivement pour le système d'exploitation MAC OSX sont disponibles sous le lien <http://support.luxtrust.lu> rubrique « Guides ».

I.2 Eléments nécessaires avant d'exécuter la procédure d'activation

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>) branché à l'ordinateur.
- Reçu par courrier la lettre « LuxTrust PIN-Mailer » qui contient le « PIN » (numéro personnel d'identification), « PUK » (clé de déblocage) 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>).

I.3 Vocabulaire

Activation	action par laquelle les certificats passent du statut suspendu au statut activé
JAVA	langue de programmation objet développée par Sun Microsystems, très portable, indépendante de la plateforme exploitée
MiddleWare	logiciel permettant la communication entre la puce et l'application
Navigateur Internet	logiciel permettant de naviguer sur internet
PIN	(personal identification number) numéro personnel d'identification
PIN-Mailer	courrier par lequel le PIN est communiqué au client
puce	circuit intégré (anglais : chip) contenant les certificats
PUK	(personal unblocking key) clé de déblocage personnelle
Signing Stick	dénomination commerciale pour le produit LuxTrust ainsi désigné
Smartcard	dénomination commerciale pour le produit LuxTrust ainsi désigné
Système d'exploitation	logiciel contrôlant les composants physiques d'un ordinateur afin que l'utilisateur et les applications installées puissent faire usage de l'ordinateur

II Changer le PIN

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

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

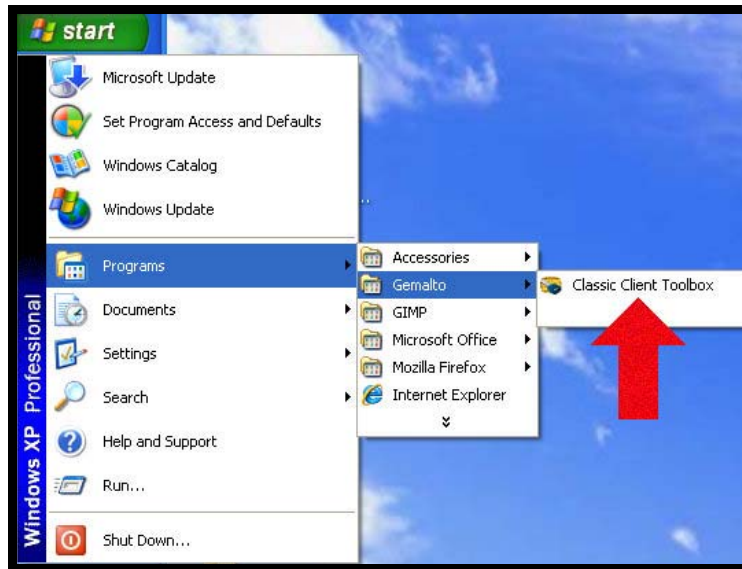


Figure II.1.a

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

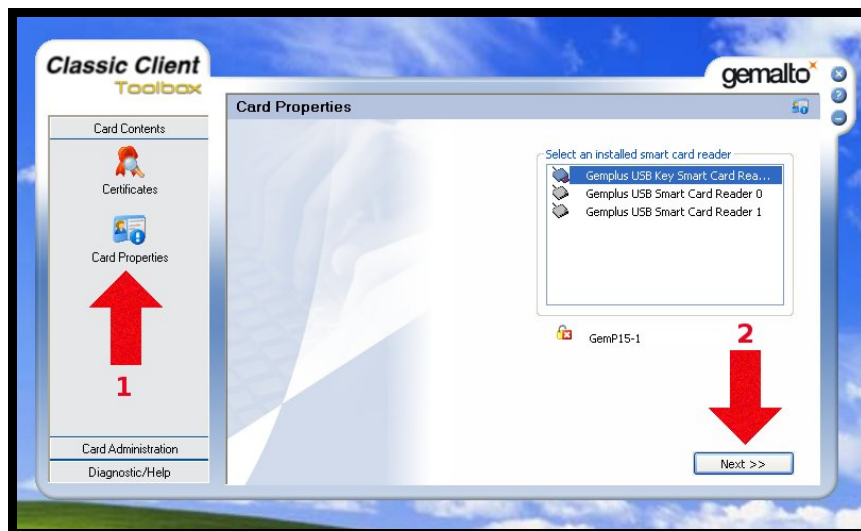


Figure II.1.b

Cliquez d'abord sur « Card Properties » (Propriétés cartes) (voir première flèche rouge sur la figure II.1.b) et puis sur « Next » (voir deuxième flèche rouge dans la figure II.1.b.).

Cliquez sur le bouton « OK » (ok) tel qu'indiqué (voir flèche rouge sur la figure II.1.c) pour prendre connaissance du fait que le PIN est bloqué et qu'il faut le débloquer.

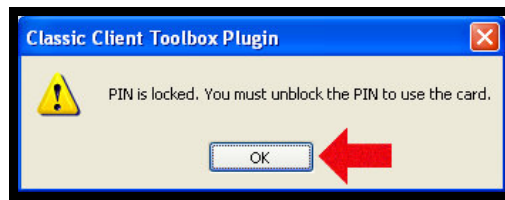


Figure II.1.c

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 cadre rouge dans la figure II.1.d). Ces compteurs vous affichent les nombres d'essais restants pour entrer le bon code PIN ou Admin PIN (PUK).

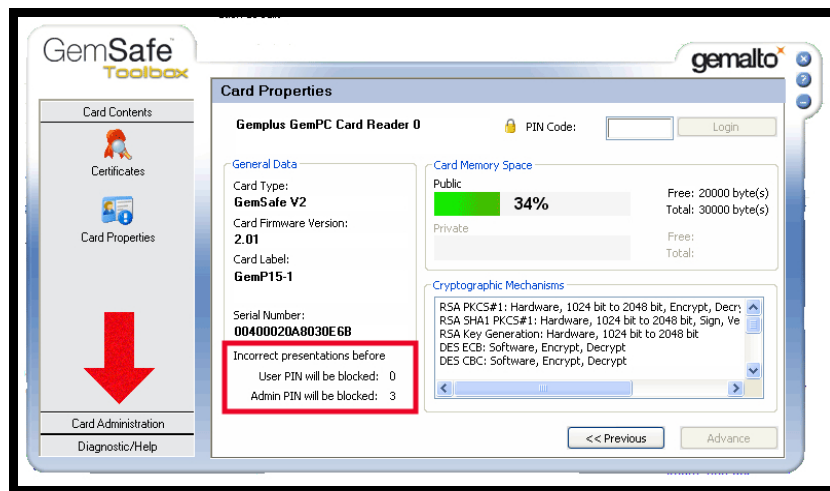


Figure II.1.d

Cliquez sur « Card Administration » (Administration carte) (voir flèche rouge sur la figure II.1.d).

Puis sélectionnez « PIN Management » (voir première flèche rouge sur la figure II.1.e).

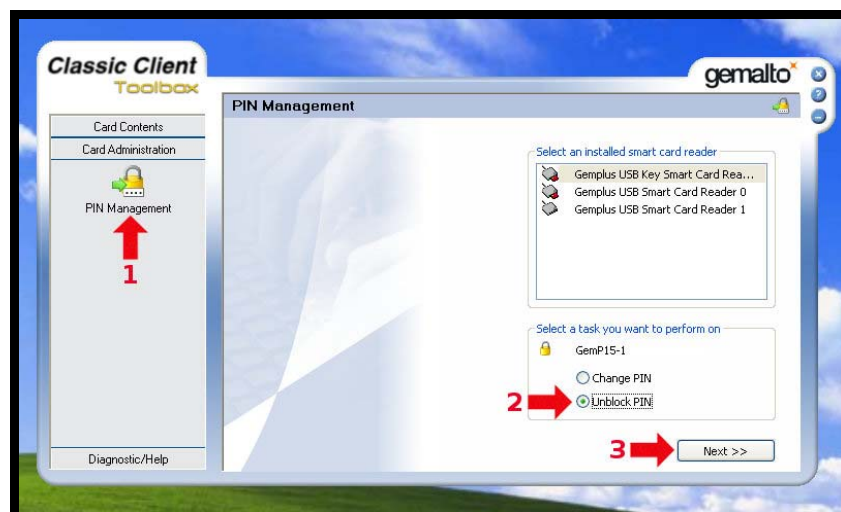


Figure II.1.e

Cochez le bouton « Unblock PIN » (Débloquer PIN) (voir deuxième flèche rouge dans la figure II.1.e) et cliquez sur le bouton « Next » (Suivant) (voir troisième flèche rouge dans la figure II.1.e). La fenêtre suivante s'affichera :

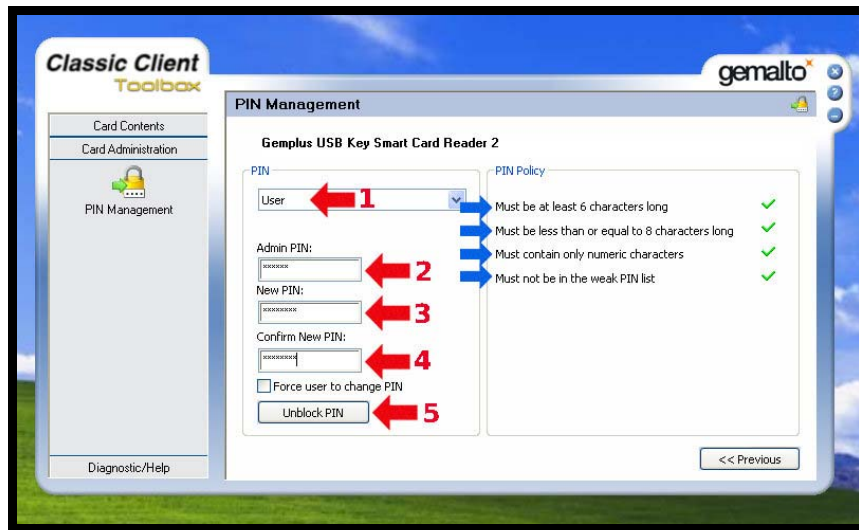


Figure II.1.f

Assurez-vous que le menu déroulant affiche bien « User » et non **pas** « Admin » (voir première flèche rouge dans la figure II.1.f).

Entrez le « Admin PIN Code » (PIN administrateur) qui se trouve sur votre PIN-Mailer dénommé « PUK (Admin PIN) » (voir deuxième flèche rouge sur la figure II.1.f).

Entrez un nouveau PIN dans la case intitulée « New PIN » (nouveau PIN) (voir troisième flèche rouge dans la figure II.1.f). Le nouveau PIN est choisi par vous-même en respectant les consignes telles que renseignées sur la partie droite (voir flèches bleues de la figure II.1.f) :

- « must be at least 6 characters long » (doit avoir au moins six caractères) (voir première flèche bleue sur la figure II.1.f).
- « must be less than or equal to 8 characters long » (doit avoir moins de huit ou exactement huit caractères) (voir deuxième flèche bleue sur la figure II.1.f).
- « must contain only numeric characters » (doit contenir uniquement des caractères numériques) (voir troisième flèche bleue sur la figure II.1.f).
- « must not be in the weak PIN list » (ne doit pas être dans la liste des PINs faibles) (voir la quatrième flèche bleue sur la figure II.1.f).

La liste des PIN 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 plus de caractères que d'en choisir un avec moins de caractères ;
- 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 caractères très connues comme par exemple 112112, 925925, ...

Quelques conseils de sécurité :

- ne jamais noter le PIN sur le Signing Stick ou la 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 la Smartcard. Une personne qui trouve le Signing Stick ou la 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 II.1.f).

Cliquez sur le bouton « Unblock PIN » (débloquer PIN) pour valider le déblocage et changement du code PIN (voir cinquième flèche rouge sur figure II.1.f).

Le message représenté par la figure II.1.g confirme que le PIN a bien été débloqué. Cliquez sur le bouton « ok » (voir flèche rouge sur la figure II.1.g) pour terminer le processus de déblocage de PIN.



Figure II.1.g