



Pin Code Verwaltung unter Windows

V 1.0

21/05/2012
Deutsch

Verzichterklärung

Dieses Dokument kann nicht im Ganzen oder in Teilen wiederhergestellt werden ohne die vorherige ausdrückliche schriftliche Zustimmung von LuxTrust SA. Urheberrechte können für Teile dieser Dokumentation existieren.. LuxTrust SA übernimmt keine Haftung für irgendwelche direkten, indirekten, besonderen, Neben-oder Folgeschäden materielle oder sonstige Schäden in irgendeiner Weise im Zusammenhang mit oder aus der Ausübung aller Ratschläge in diesem Dokument. Dieses Dokument wird "als keine" Vorschrift im Hinblick auf die Eignung für einen bestimmten Zweck oder Anwendbarkeit gemacht. Durch die Verwendung dieses Dokuments erklären Sie sich, es auf eigenes Risiko zu verwenden und es versteht sich dass dieses Dokument nicht ohne Einschränkungen zur Verfügung gestellt wird.

I.1 Elemente welche Sie im Vorfeld schon erledigt haben sollten

- Sie haben schon erfolgreich einen Signing Stick oder Smartcard auf unserer Internetseite bestellt (<https://orders.luxtrust.lu>).
- Sie haben Ihr Produkt schon per Post erhalten.
- Nutzer einer Smartcard, Sie haben schon das Lesegerät, welches Sie sich bereits gekauft haben in den PC gesteckt. (<https://readers.luxtrust.lu>).
- Sie haben den LuxTrust Brief mit den Initial Codes beihand : Initial Pin, Puk code und Challenge.
- Sie haben die Middleware installiert. (<https://drivers.luxtrust.lu>).

II Pin Code ändern

Nutzer die den Pin entsperren möchten, überspringen Sie bitte diese Schritte und fangen Sie beim Bild 6 an.

Verbinden Sie Ihr Produkt (Signing Stick oder Smartcard) mit PC über Ihren USB Port oder Lesegerät.

Öffnen Sie die Gemalto Middleware über das Start Feld, dann klicken Sie auf « Programs »(Alle Programme). Suchen Sie hier Gemalto. Klicken Sie dann hierdrauf und dann auf Classic Client und dann auf Classic Client Toolbox (sieh roter Pfeil im Bild 1).

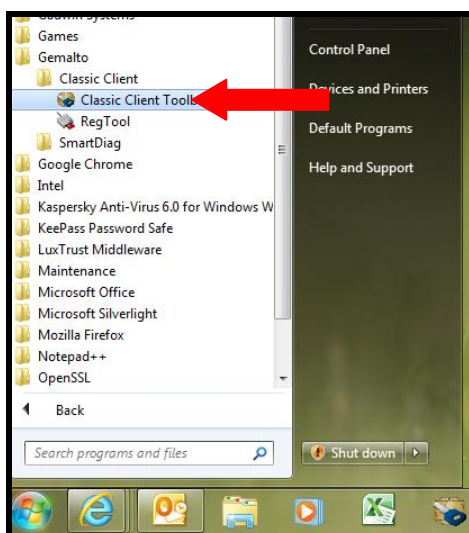


Bild 1

Folgendes Fenster sehen Sie auf Ihrem Bildschirm

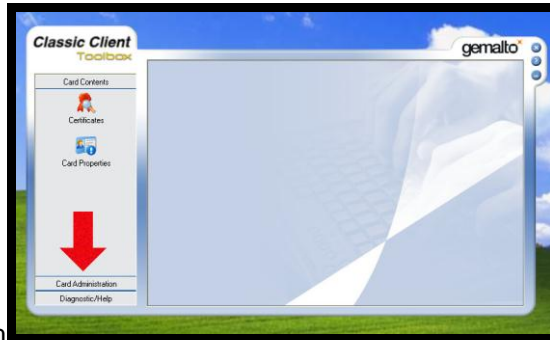


Bild 2

Klicken Sie auf « Card Administration » (siehe roter Pfeil im Bild 2).

Wählen Sie « PIN Management » aus (siehe erster roter Pfeil im Bild 3).

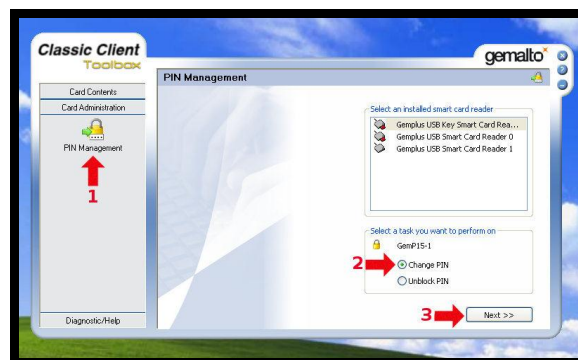


Bild 3

Haken Sie das Feld « Change PIN » an (siehe zweiter roter Pfeil im Bild 2) und klicken Sie auf « Next » (siehe dritter roter Pfeil im Bild 3). Nächster Fenster erscheint :

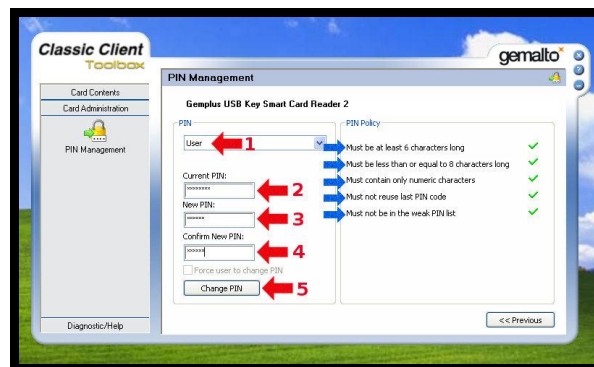


Bild 4

Vergessen Sie sich, dass « User » im ersten Feld steht und **nicht** « Admin ». (siehe erster roter Pfeil im Bild 4)

Geben Sie den aktuellen Pin im Feld « Current PIN » (siehe zweiter roter Pfeil im Bild 4).

Geben Sie den neuen PIN im Feld « New PIN » ein (siehe dritter roter Pfeil im Bild 4). Der neue PIN muss folgende Bedingungen erfüllen (siehe blaue Pfeile im Bild 4) :

- « must be at least 6 characters long » (muss wenigstens 6 Zeichen haben) (siehe erster blauer Pfeil im Bild 4).
- « must be less than or equal to 8 characters long » (darf weniger oder maximal 8 Zeichen haben) (siehe zweiter blauer Pfeil im Bild 4).

- « must contain only numeric characters » (darf nur numerische Zeichen haben) (siehe dritter blauer Pfeil a Bild 4).
- « must not reuse last PIN code » (der letzt gewählte PIN darf nicht erneut benutzt werden) (siehe 4 blauer Pfeil im Bild 4).
- « must not be in the weak PIN list » (darf kein schwacher Pin sein (223322,123456,000011)) (siehe fünfter Pfeil im Bild 4).

Einige Ratschläge welche PINs Sie nicht nehmen sollten:

- Je mehr Zeichen Ihr PIN enthält, desto sicher ist er;
- Vermeiden Sie Kombinationen die einfach zu erraten sind, wie zum Beispiel , Geburtsdatum, Telefonnummer usw.
- Vermeiden Sie logische avoid using logical Abläufe wie: 123456, 12131415, 102030 usw.
- Vermeiden Sie Pins wo sich die Ziffern wiederholen wie: 222888, 55555555 etc.
- Vermeiden Sie sich wiederholende Zahlenmuster wie: 01010101, 45674567, 8091908, etc.
- Vermeiden Sie gut bekannte Zahlenmuster wie: 112112, 925925, etc.

Sicherheitshinweise:

- Schreiben Sie niemals den the PIN auf den Signing Stick oder Smartcard. Jeder der den Signing Stick oder Smartcard findet kann indem Fall das Produkt gleich benutzen.
- Notieren Sie niemals den Pin neben dem Signing Stick oder Smartcard. Jeder der den Signing Stick oder Smartcard mit der Notiz findet kann indem Fall das Produkt gleich benutzen.
- Schreiben Sie den PIN nie auf, den jede Person die beides findet kann den Signing Stick oder Smartcard indem Fall das Produkt gleich benutzen.
- Geben Sie den PIN nie an eine andere Person weiter. Es ist ein persönlicher PIN.

Vergessen Sie Ihren neuen PIN nicht!!!

Dieser neue Pin den Sie selbst ausgesucht haben benutzen Sie dann bei Ihren Anwendunge um sich einzuloggen. (web banking, ccp connect, s-net, bilnet, guichet.lu, ...) oder um E-mails oder Word Dokumente zu unterschreiben.

Bestätigen Sie den neuen PIN im Feld « confirm New PIN » (Bestätigen neuen PIN) (siehe vierter roter Pfeil im Bild 4).

Klicken Sie auf « Change PIN » um die Änderung zu bestätigen siehe fünfter roter Pfeil im Bild 4).

Klicken Sie auf « OK » (siehe roter Pfeil im Bild 5) um die Prozedur auszuschliessen. Jetzt können Sie die Gemalto Toolbox schliessen.



Bild 5

III Pin Code Entsperren

Verbinden Sie Ihr Produkt (Signing Stick oder Smartcard) mit PC über Ihren USB Port oder Lesegerät.

Öffnen Sie die Gemalto Middleware über das Start Feld, dann klicken Sie auf « Programs »(Alle Programme). Suchen Sie hier Gemalto. Klicken Sie dann hierdrauf und dann auf Classic Client und dann auf Classic Client Toolbox (siehe roter Pfeil im Bild 6).

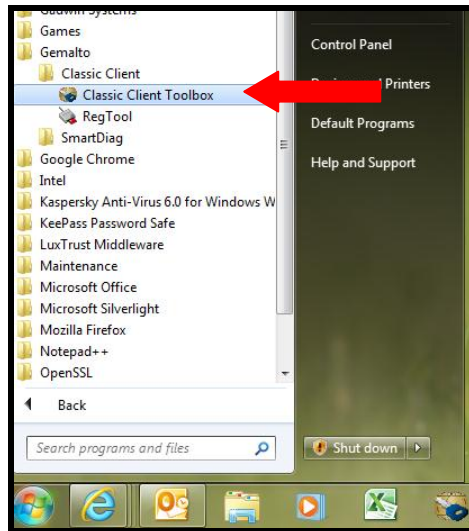


Bild 6

Folgendes Fenster sehen Sie auf Ihrem Bildschirm.

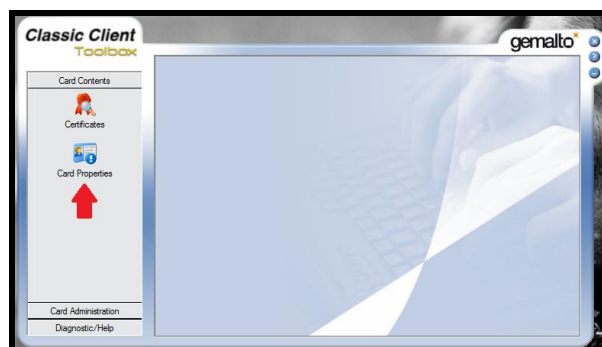


Bild 7

Klicken Sie auf « Card Properties » (siehe roter Pfeil im Bild 8).

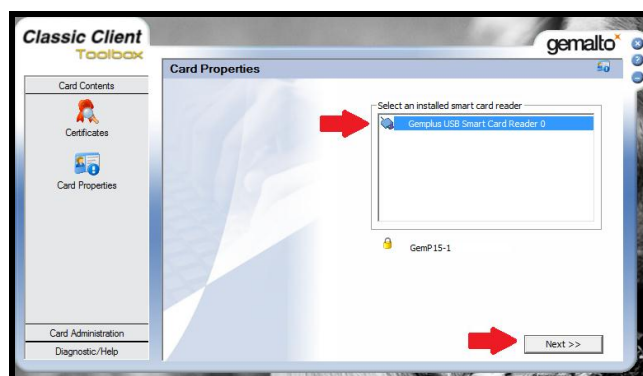


Bild 8

Wählen Sie das Lesegerät aus und klicken Sie auf « Next » (siehe rote Pfeile im Bild 8)

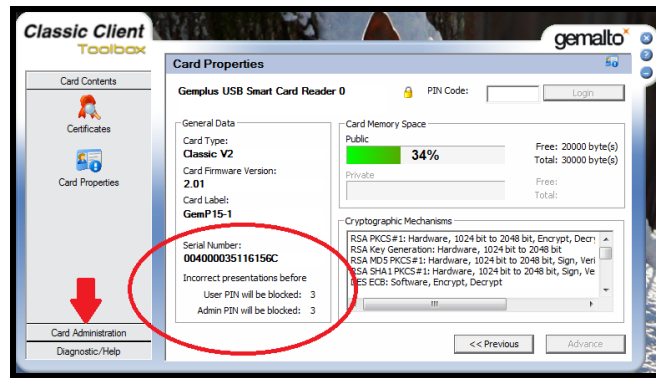


Bild 9

Unten rechts befinden sich die Statusanzeigen der noch möglichen Pin Codes Änderungen

Haben Sie noch 3 bei "User PIN will be blocked" und 3 bei "Admin Pin will be blocked" stehen, so können Sie noch 3 mal den Pin und auch 3 mal den Admin eingeben bevor Sie das Produkt definitiv blockiert haben.

Haben Sie bei " Admin Pin will be blocked" 0 stehen, so ist Ihr Produkt endgültig gesperrt und kann nicht mehr entsperrt werden.

Klicken Sie auf « Card Administration » (siehe roter Pfeil im Bild 9).

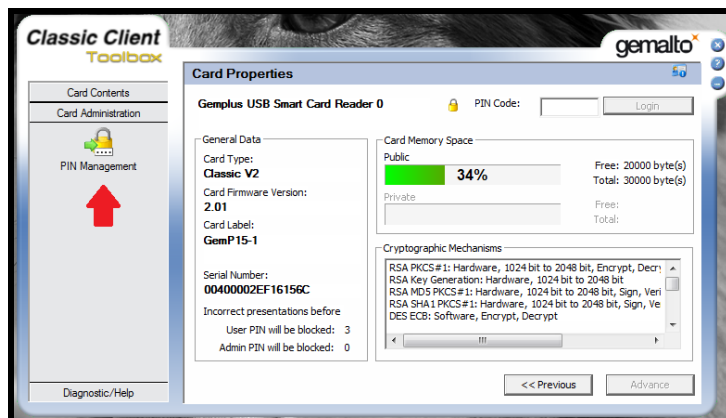


Bild 10

Wählen Sie nun « PIN Management » (siehe erster roter Pfeil im Bild 10).

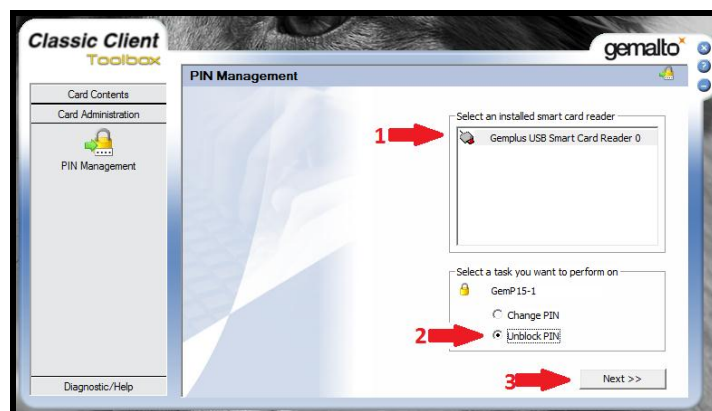


Bild 11

Wählen Sie das Lesegerät aus, (siehe erster roter Pfeil im Bild 11), klicken Sie dann auf « Unblock Pin » und dann auf „Next“ (siehe rote Pfeil 2 und 3 im Bild 11).

Das folgende Fenster erscheint auf Ihrem Bildschirm:

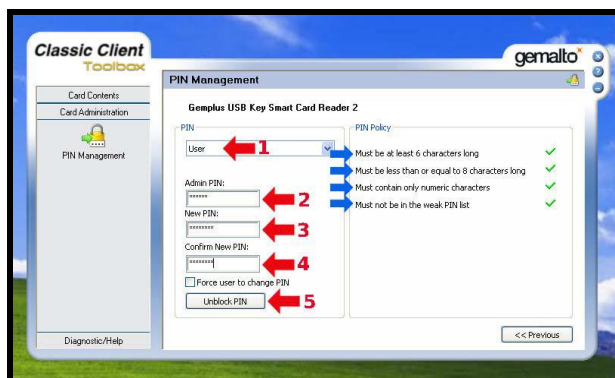


Bild 12

Vergisseren Sie sich, dass « User » im ersten Feld steht und **nicht** « Admin ». (siehe erster roter Pfeil im Bild 12)

Geben Sie den Admin Pin/PUK Code im Feld « Admin PIN » (siehe zweiter roter Pfeil im Bild 12).

Geben Sie den neuen PIN im Feld « New PIN » ein (siehe dritter roter Pfeil im Bild 12). Der neue PIN muss folgende Bedingungen erfüllen (siehe blaue Pfeile im Bild 12) :

- « must be at least 6 characters long » (muss wenigstens 6 Zeichen haben) (siehe erster blauer Pfeil im Bild 12).
- « must be less than or equal to 8 characters long » (darf weniger oder maximal 8 Zeichen haben) (siehe zweiter blauer Pfeil im Bild 12).
- « must contain only numeric characters » (darf nur numerische Zeichen haben) (siehe dritter blauer Pfeil im Bild 12).
- « must not reuse last PIN code » (der letzt gewählte PIN darf nicht erneut benutzt werden) (siehe 4 blauer Pfeil im Bild 12).
- « must not be in the weak PIN list » (darf kein schwacher Pin sein (223322,123456,000011)) (siehe fünfter Pfeil im Bild 12).

Einige Ratschläge welche PINs Sie nicht nehmen sollten:

- Je mehr Zeichen Ihr PIN enthält, desto sicher ist er;
- Vermeiden Sie Kombinationen die einfach zu erraten sind, wie zum Beispiel , Geburtsdatum, Telefonnummer usw.
- Vermeiden Sie logische avoid using logical Abläufe wie: 123456, 12131415, 102030 usw.
- Vermeiden Sie Pins wo sich die Ziffern wiederholen wie: 222888, 55555555 etc.
- Vermeiden Sie sich wiederholende Zahlenmuster wie: 01010101, 45674567, 8091908, etc.
- Vermeiden Sie gut bekannte Zahlenmuster wie: 112112, 925925, etc.

Sicherheitshinweise:

- Schreiben Sie niemals den the PIN auf den Signing Stick oder Smartcard. Jeder der den Signing Stick oder Smartcard findet kann indem Fall das Produkt gleich benutzen.
- Notieren Sie niemals den Pin neben dem Signing Stick oder Smartcard. Jeder der den Signing Stick oder Smartcard mit der Notiz findet kann indem Fall das Produkt gleich benutzen.
- Schreiben Sie den PIN nie auf, den jede Person die beides findet kann den Signing Stick oder Smartcard indem Fall das Produkt gleich benutzen.
- Geben Sie den PIN nie an eine andere Person weiter. Es ist ein persönlicher PIN.

Vergessen Sie Ihren neuen PIN nicht!!!

Dieser neue Pin den Sie selbst ausgesucht haben benutzen Sie dann bei Ihren Anwendungen um sich einzuloggen. (web banking, ccp connect, s-net, Bilnet, guichet.lu, ...) oder um E-mails oder Word Dokumente zu unterschreiben.

Bestätigen Sie den neuen PIN im Feld « confirm New PIN » (Bestätigen neuen PIN) (siehe 4 roter Pfeil im Bild 12).

Klicken Sie auf « Unblock PIN » um die Änderung zu bestätigen (siehe fünfter roter Pfeil im Bild 12).

Klicken Sie auf « OK » (siehe roter Pfeil im Bild 13) um die Prozedur auszuschliessen. Jetzt können Sie die Gemalto Toolbox schliessen.

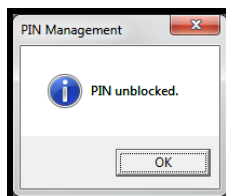


Bild 13