



PIN Code Management under Microsoft Windows

V 1.0

22/05/2012
English

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.

I.1 Elements required before executing the procedure

This procedure can only be executed if beforehand you have:

- Successfully ordered a Smartcard or a Signing Stick (see <http://orders.luxtrust.lu>).
- Received by post your Smartcard or Signing Stick chip
- A Smartcard Reader connected to your PC or received by post the Signing Stick
- Received the “PIN-Mailer” letter by post that contains the PIN, the PUK and the Challenge. This letter will usually reach you within 2 to 3 days following receipt of your Smartcard or Signing Stick chip.
- Installed the LuxTrust Middleware for the version of your Microsoft Windows operating system (see <http://drivers.luxtrust.lu>)

II Changing the PIN

Users, who want to unblock the PIN, please move on to Figure 6 “Unblock PIN”

Connect the Signing Stick to a free USB port or insert the Smartcard into the card reader.

Launch the “Classic Client Toolbox” MiddleWare from the Start menu – “Programs” (All programs) – “Gemalto” as indicated by the red arrow in figure 1.

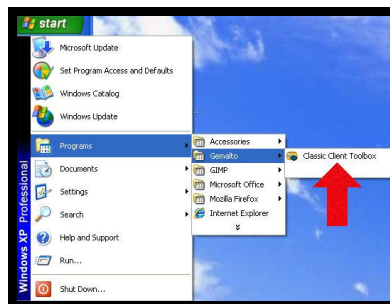


Figure 1

The following window will be displayed on your screen:

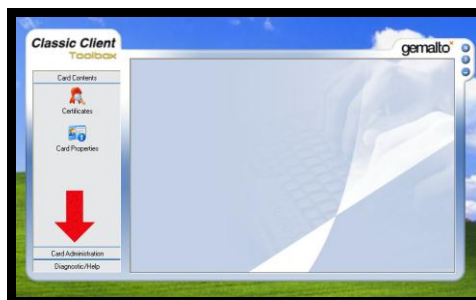


Figure 2

Click on “Card Administration” (see red arrow in figure 2). Then select “PIN Management” (see first red arrow in figure 3).

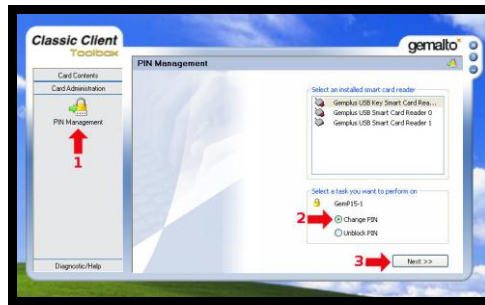


Figure 3

Check the “Change PIN” button (see second red arrow in figure 3) and click on the “Next” button (see third red arrow in figure 3). The following window is displayed:

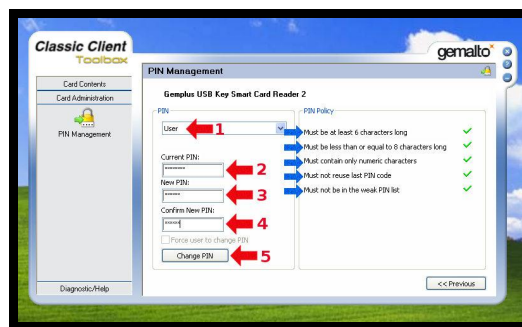


Figure 4

Check that the drop-down menu displays “User” and not “Admin” (see first red arrow in figure 4.).

Enter the “Current PIN” (see second red arrow in figure 4). Enter a new PIN in the box entitled “New PIN” as indicated by the third red arrow in figure 4. You can select the new PIN in line with the instructions provided in the right-hand section (see blue arrows) of figure 4:

- “must be at least 6 characters long” – see the first blue arrow in figure 4;
- “must be less than or equal to 8 characters long” – see the second blue arrow in figure 4;
- “must contain only numeric characters” – see the third blue arrow in figure 4;
- “must not reuse last PIN code” – see the fourth blue arrow in figure 4;
- “must not be in the weak PIN list” – see the fifth blue arrow in figure 4.

The weak PIN list contains PINs that may be guessed easily. Such PINs are refused by the application.

Some advice on choosing a suitable PIN:

- The more characters you use in the PIN, the more secure it will be;
- avoid using a combination of numbers that can be easily guessed, for example, your date of birth, telephone number etc.
- avoid using logical sequences such as for example 123456, 12131415, 102030 etc.
- avoid repeating the same number several times such as for example 222888, 55555555 etc.

- avoid using repetitive or symmetrical number patterns such as for example 01010101, 45674567, 8091908, etc.
- avoid using well-known character sequences such as for example 112112, 925925, etc.

Some security advice:

- never write the PIN on the Signing Stick or Smartcard. Anyone who finds the Signing Stick or Smartcard could use it straight away.
- never store the PIN with the Signing Stick. Anyone who finds the Signing Stick Signing Stick or Smartcard will also find the PIN to use it.
- never write the PIN down anywhere. An unauthorised individual may find this note and use it with the Signing Stick or Smartcard.
- never disclose the PIN to any other individual. The Signing Stick and the Smartcard are for your personal use and should not be passed on to any other individual.

Memorise the new PIN!!!

In the future, the new PIN that you have chosen yourself must be used to activate the Signing Stick or Smartcard and to enable you to log into an application (for example: web banking, ccp connect, s-net, bilnet, guichet.lu, etc.). or for signing (MS Outlook, MS Word etc.).

Enter the new PIN again in the box entitled “confirm new PIN” and shown by the fourth red arrow in figure 4.

Click on the “Unblock PIN” button to confirm the change of your PIN code (see fifth red arrow in figure 4).

The message shown in figure 5 confirms that the PIN has been changed. Click on the “OK” button as shown by the red arrow in figure 5 to complete the PIN change process.



Figure 5

III Unblock Pin

Connect the Signing Stick to a free USB port or insert the Smartcard into the card reader.

Launch the “Classic Client Toolbox” MiddleWare from the Start menu – “Programs” (All programs) – “Gemalto” as indicated by the red arrow in figure 6

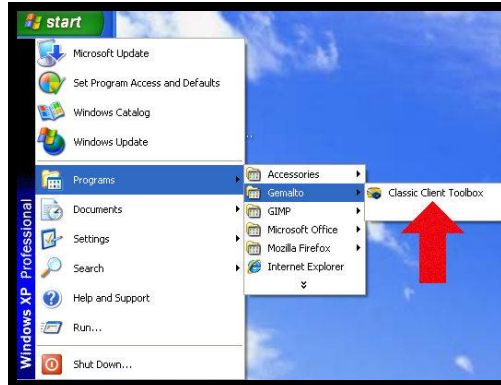


Figure 6

The following window will be displayed on your screen:



Figure 7

Click on “Card Properties” (see red arrow in figure 7).

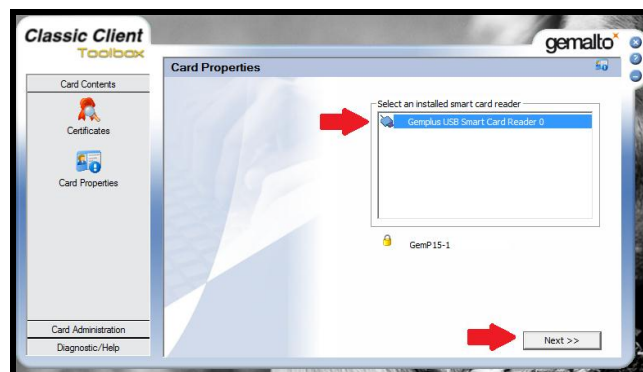


Figure 8

Select the driver (see first red arrow in figure 8) and click on the “Next” button (see second red arrow in figure 8). The following window is displayed:

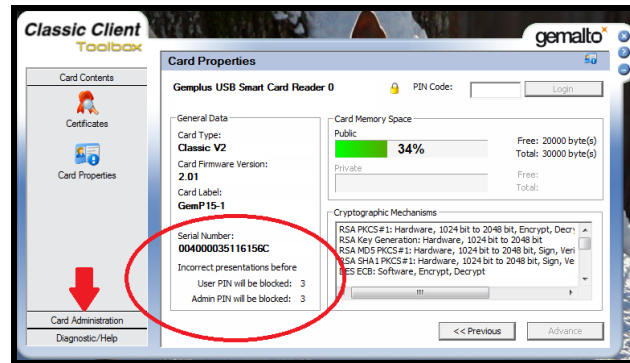


Figure 9

On this window, you see in the red circle, how many tries you still have to unblock the pin code.

If the Admin Pin is at 0 or grey, the Smartcard or Signing Stick is completely blocked and it is no more possible to unblock.

To start the an block procedure please click on “Card Administration” (see red arrow in figure 9)

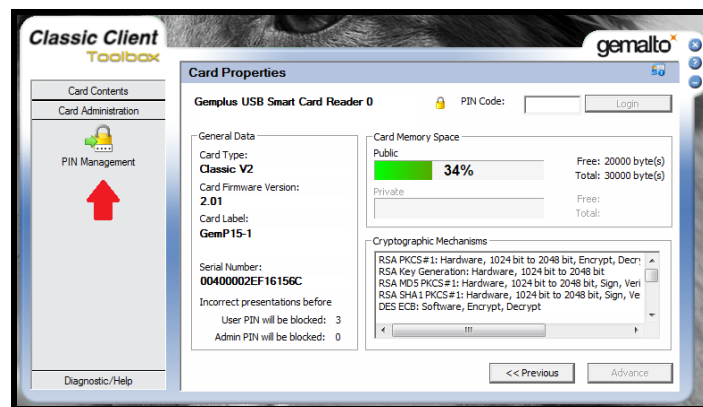


Figure 10

Click on “Pin Management” (see red arrow in figure 10)

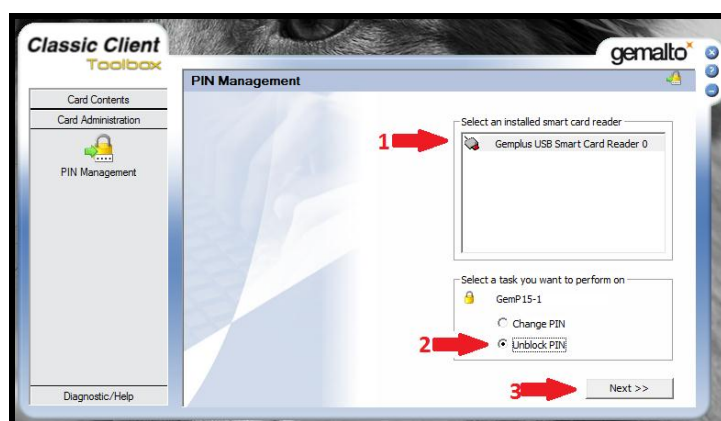


Figure 11

Select your driver (see first red arrow in figure 11), click on “unblock Pin” (see second red arrow in figure 6) and validate with “Next” (see third red arrow in figure 11)

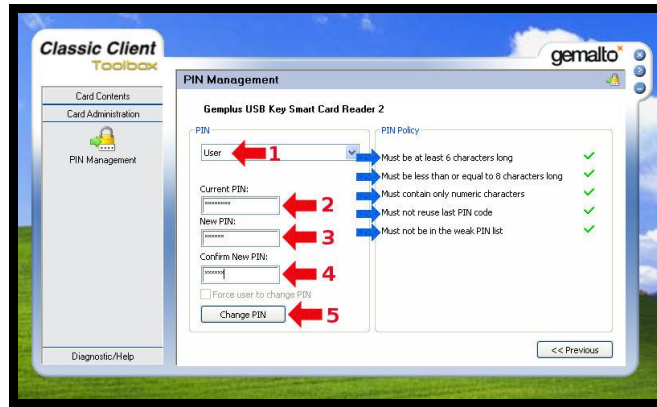


Figure 12

Check that the drop-down menu displays “User” and not “Admin” (see first red arrow in figure 12.).

Enter the “Current PIN” (see second red arrow in figure 12).

Enter a new PIN in the box entitled “New PIN” as indicated by the third red arrow in figure 12. You can select the new PIN in line with the instructions provided in the right-hand section (see blue arrows) of figure 12:

- “must be at least 6 characters long” – see the first blue arrow in figure 12;
- “must be less than or equal to 8 characters long” – see the second blue arrow in figure 12.;
- “must contain only numeric characters” – see the third blue arrow in figure 12;
- “must not reuse last PIN code” – see the fourth blue arrow in figure 12.;
- “must not be in the weak PIN list” – see the fifth blue arrow in figure 12.

The weak PIN list contains PINs that may be guessed easily. Such PINs are refused by the application.

Some advice on choosing a suitable PIN:

- The more characters you use in the PIN, the more secure it will be;
- avoid using a combination of numbers that can be easily guessed, for example, your date of birth, telephone number etc.
- avoid using logical sequences such as for example 123456, 12131415, 102030 etc.
- avoid repeating the same number several times such as for example 222888, 55555555 etc.
- avoid using repetitive or symmetrical number patterns such as for example 01010101, 45674567, 8091908, etc.
- avoid using well-known character sequences such as for example 112112, 925925, etc.

Some security advice:

- never write the PIN on the Signing Stick or Smartcard. Anyone who finds the Signing Stick or Smartcard could use it straight away.
- never store the PIN with the Signing Stick. Anyone who finds the Signing Stick or Smartcard will also find the PIN to use it.
- never write the PIN down anywhere. An unauthorised individual may find this note and use it with the Signing Stick or Smartcard.

- never disclose the PIN to any other individual. The Signing Stick and the Smartcard are for your personal use and should not be passed on to any other individual.

Memorise the new PIN!!!

In the future, the new PIN that you have chosen yourself must be used to activate the Signing Stick or Smartcard and to enable you to log into an application (for example: web banking, ccp connect, s-net, bilnet, guichet.lu, etc.). or for signing (MS Outlook, MS Word etc.).

Enter the new PIN again in the box entitled “confirm new PIN” and shown by the fourth red arrow in figure 12.

Click on the “Unblock PIN” button to confirm the change of your PIN code (see fifth red arrow in figure 12).

The message shown in figure 13 confirms that the PIN has been changed. Click on the “OK” button as shown by the red arrow in figure 13 to complete the PIN change process.

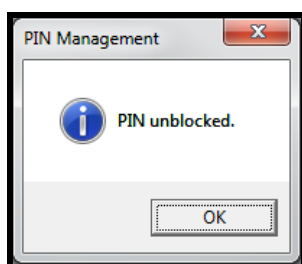


Figure 13