

Guide utilisateur

Pin Management MAC OSX

Document reference:

UG-0237

Date issued:

09/02/2018

Version: 1.0

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 OF CONTENTS

Guide utilisateur	1
Pin Management MAC OSX.....	1
1. Elements required before executing the procedure	3
2. Changing the PIN.....	3
3. Unblocking the PIN using the PUK	5

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

You have received the “LuxTrust Codes” 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.

Installed the LuxTrust Middleware for the version of your MAC OS X operating system (see <http://drivers.luxtrust.lu>).

2. Changing the PIN

Customers, who want to unblock the Pin Code, please move on to Figure 3 Unblock Pin

Plug the Smartcard into your Smartcard reader or your Signing Stick into a free USB port. Launch the Middleware « Classic Client PIN Management » from the folder « Gemalto » inside of the folder « Applications ». A window like the one displayed in figure 1 will appear.

If you do not find Middleware “Classic Client PIN Management” in the place indicated, use “Spotlight” by clicking on the symbol “Magnifying glass” at the top on the right of the screen and type in “classic”. One of the first posted results is the Middleware «Classic Client PIN Management». Click above to find the window shown by the figure1.



Figure 1

1. Enter the initial PIN in the box entitled “**Current Pin**” as shown by the first red arrow in figure 1. The current PIN can be found in the scratch-off box of the PIN-Mailer, in the first line to the right of word “PIN”.
2. Enter a new PIN in the box entitled “**New Pin**” as indicated by the second red arrow in figure 1. You can select the new PIN in line with the instructions provided in the right-hand section:
 - a. “must be at least 6 characters long” – see the first blue arrow in figure 1;
 - b. “must be less than or equal to 8 characters long” – see the second blue arrow in figure 1;
 - c. “must contain only numeric characters” – see the third blue arrow in figure 1;

- d. “must not reuse last PIN code”– see the fourth blue arrow in figure 1
 - e. “must not be in the weak PIN list” – see the fifth blue arrow in figure 1.
3. Enter the new PIN again in the box entitled “**Confirm New Pin**” (see *third red arrow in figure 1*).
 4. Click on the “**Change Pin**” button (see *fourth red arrow in figure 1*) to confirm the change of your PIN code.

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 or Smartcard. 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 and to enable you to log into an application (for example: web banking, ccp connect, s-net, Bil Net, guichet.lu, etc.).

The message shown in figure 2 confirms that the PIN has been changed. Click on the “**OK**” button as shown by the red arrow in figure 2 to complete the PIN change process.

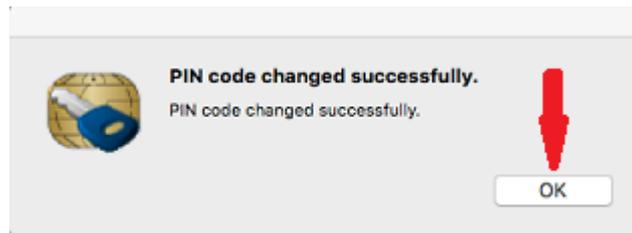


Figure 2

3. Unblocking the PIN using the PUK

Plug the Smartcard into your Smartcard reader or your Signing Stick to a free USB port. Launch the Middleware « Classic Client PIN Management » from the folder « Gemalto » inside of the folder « Applications ». A window like the one displayed in figure 3 will appear. If you do not find Middleware “Classic Client PIN Management” in the place indicated, use “Spotlight” by clicking on the symbol “Magnifying glass” at the top on the right of the screen and type in “classic”. One of the first posted results is the Middleware «Classic Client PIN Management». Click above to find the window shown by the figure 3.

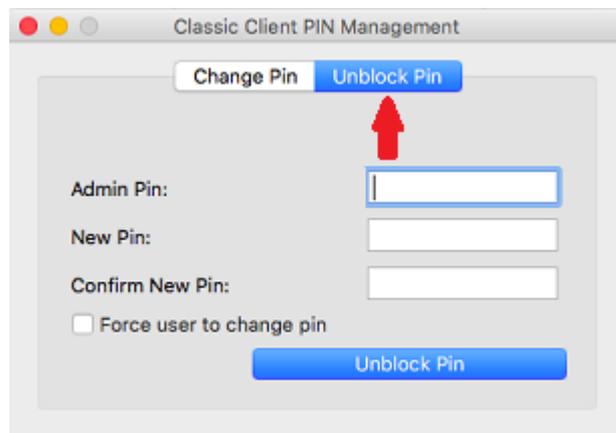


Figure 3

Click on the « **Unlock Pin** » button (see red arrow in figure 3). A window like the one displayed in figure 4 will appear.

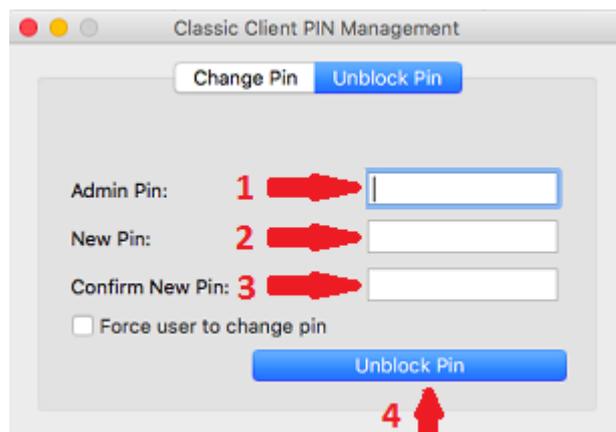


Figure 4

1. Enter the “Admin PIN Code (PUK)” written on the LuxTrust Codes letter received by post (see *first red arrow in figure 4*) in the box entitled “**Admin Pin**”. Enter a new PIN in the box entitled “**New Pin**” (see *second red arrow in figure 4*).

You can select the new PIN in line with the instructions provided in the right-hand section :

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

3. Enter the new PIN again in the box entitled “**Confirm New Pin**” (see *third red arrow in figure 4*).
4. Click on the “**Unblock Pin**” button to confirm the change of your PIN code (see *fourth red arrow in figure 4*)

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. Anyone who finds the Signing Stick or Smartcard could use it straight away.
- never store the PIN with the Signing Stick or Smartcard. 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, Bil Net, guichet.lu, etc.). or for signing (MS Outlook, MS Word etc.).

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



Figure 5