



Unblocking the PIN of your Smartcard or Signing Stick on the operating system MAC OS X

V 1.0

10/02/2010
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.

Content

I	Before getting started: pre-requisites.....	3
I.1	Coverage of this guide.....	3
I.2	Elements required before executing the procedure	3
I.3	Vocabulary.....	4
II	Unlocking the PIN using the PUK	5

I Before getting started: pre-requisites

I.1 Coverage of this guide

This document covers the stages required for unblocking the PIN of your Smartcard or Signing Stick.

This document is applicable for the following **operating systems**:

- MAC OS X 10.5
- MAC OS X 10.6

Other guides for other products respectively for the Mac OS operating system are available under the <http://support.luxtrust.lu> link in the “Guides” section.

I.2 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.
- Installed the LuxTrust Middleware for the version of your MAC OS X operating system (see <http://drivers.luxtrust.lu>)

I.3 Vocabulary

MiddleWare	software that enables communication between the chip and the application
Internet browser	software that allows you to browse the Internet
PIN	personal identification number
PIN-Mailer	mail through which the PIN is communicated to the customer
chip	Integrated circuit (chip) that contains the certificates
PUK	personal unblocking key
Signing Stick	trade name for the LuxTrust product designated as such
Smartcard	trade name for the LuxTrust product designated as such
Operating system	software that controls a computer's physical components so that the users and installed applications are able to make use of the computer system.

II 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 II.1.a will appear. Click on the « Unblock PIN » button (see red arrow in figure II.1.a).

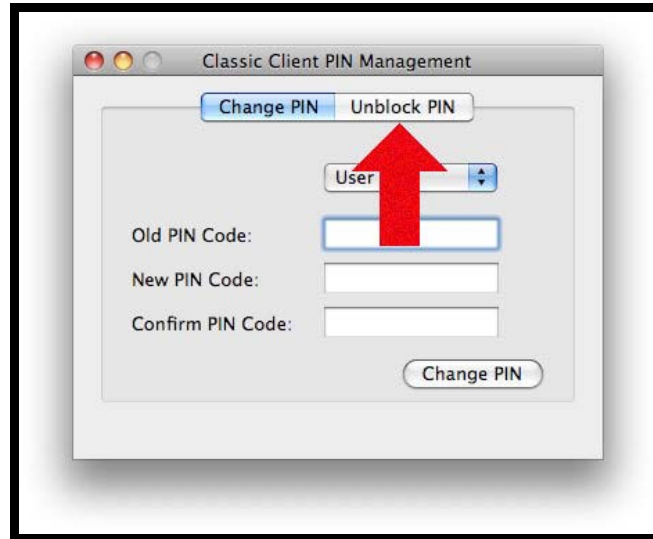


Figure II.1.a

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 II.1.a.

A window like the one displayed in figure II.1.b will appear.

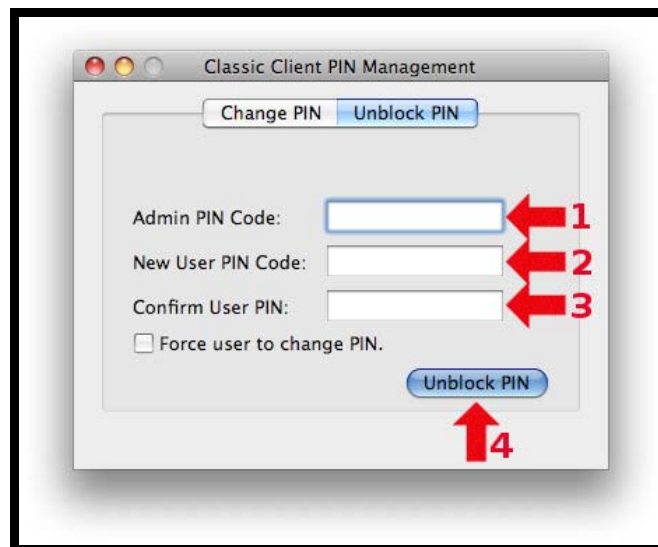


Figure II.1.b

Enter the “Admin PIN Code (PUK)” written on the PIN-Mailer letter received by post (see *first red arrow in figure II.1.b*).

Enter a new PIN in the box entitled “New User PIN Code” (see *second red arrow in figure II.1.b*). You can select the new PIN in line with the instructions provided in the right-hand section (see *blue arrows in figure II.1.b*):

- “must be at least 6 characters long” – see the first blue arrow in figure II.1.b;
- “must be less than or equal to 8 characters long” – see the second blue arrow in figure II.1.b;
- “must contain only numeric characters” – see the third blue arrow in figure II.1.b;
- “must not reuse last PIN code” – see the fourth blue arrow in figure II.1.b;
- “must not be in the weak PIN list” – see the fifth blue arrow in figure II.1.b.

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. 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, dexiplus, guichet.lu, etc.). or for signing (MS Outlook, MS Word etc.).

Enter the new PIN again in the box entitled “Confirm PIN Code” (see *third red arrow in figure II.1.b*).

Click on the “Unblock PIN” button to confirm the change of your PIN code (see *fourth red arrow in figure II.1.b*).

The message shown in figure II.1.c confirms that the PIN has been changed. Click on the “OK” button (see *red arrow in figure II.1.c*) to complete the PIN change process.



Figure II.1.c