



Configuration Adobe DC

Document reference:

UG-0622

Date issued:

06/06/2018

Version: 1.0

LuxTrust S.A
IVY Building | 13-15, Parc d'activités | L-8308 Capellen
Luxembourg | VAT LU 20976985 | RCS B112233
Business Number N°00135240/0
Phone: +352 26 68 15 – 1
Fax: +352 26 68 15 – 789

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.

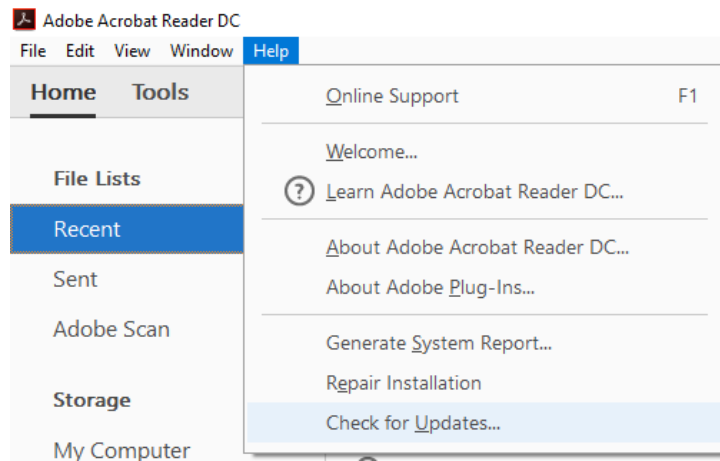
TABLE OF CONTENTS

Configuration Adobe DC	1
1. Preliminary step (Version verification of Adobe DC).....	4
2. Adding the PKCS#11 module for the « Smartcard » or the « Signing Stick ».....	5
Smartcard / Signing stick detection	5
Configure the right Digital Signature Format	6
Updating the European Trusted List (EUTL)	7
Verification Behaviour	8
Steps to add the PKCS#11 module in Adobe DC:	9
3. Signing a document	12

1. Preliminary step (Version verification of Adobe DC)

Open Adobe DC.


In order to be able to sign documents we recommend doing the updates to have the latest version installed. To do so, open the Help tab and click on Check for Updates... :



2. Adding the PKCS#11 module for the « Smartcard » or the « Signing Stick »

Beforehand, check whether Gemalto is correctly installed and working in order to take the necessary steps.


Smartcard / Signing stick detection

- Click on the  symbol in the Windows taskbar to open the LuxTrust Middleware.

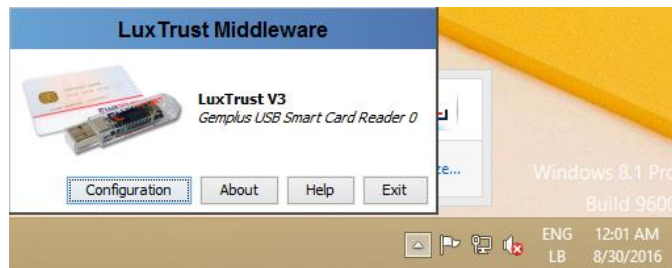


- If it shows “no terminal connected” insert your Smartcard or Signing Stick.

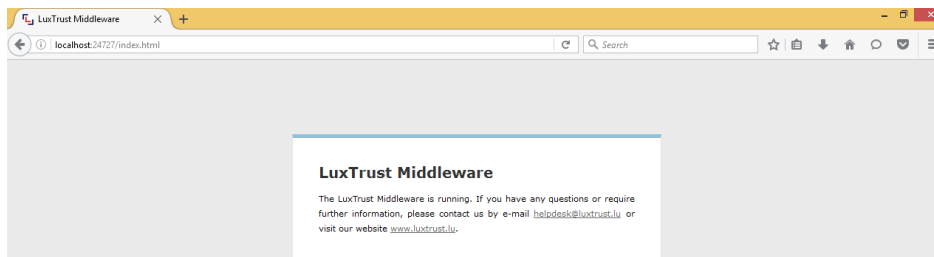


- Click on the  symbol in the Windows taskbar to open the LuxTrust Middleware.



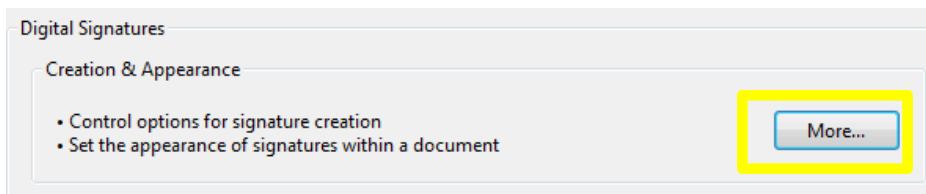


- Check if the LuxTrust Middleware is working by entering the following address in your browser : <http://localhost:24727/index.html>

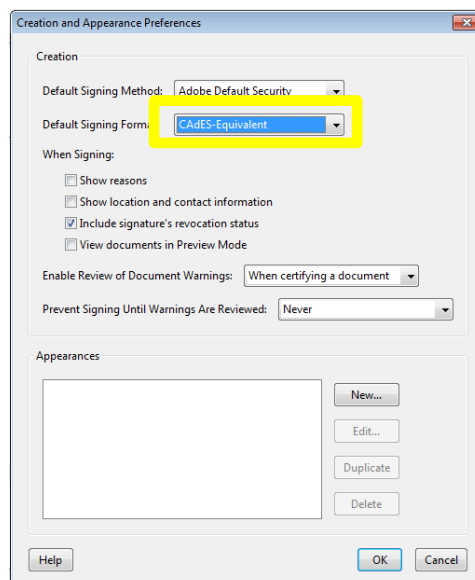


Configure the right Digital Signature Format

Open the Edit Tab: → Preferences → Signatures → Digital Signature → Creation& Appearance and click on “More...”

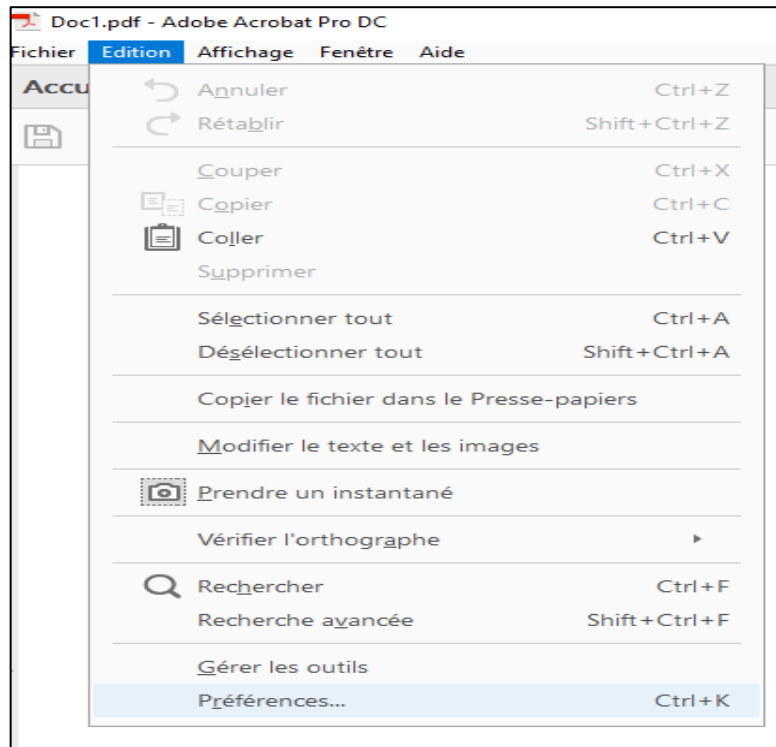


Set then Default Signing Format to: CAdES-Equivalent and validate with “Ok”.

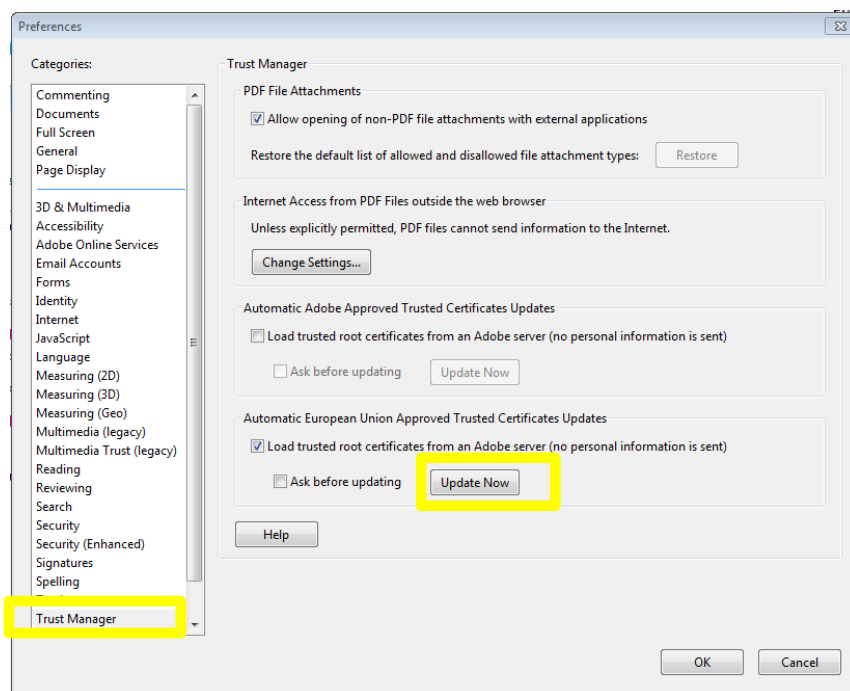


Updating the European Trusted List (EUTL)

- Open the Edit Tab → Preferences

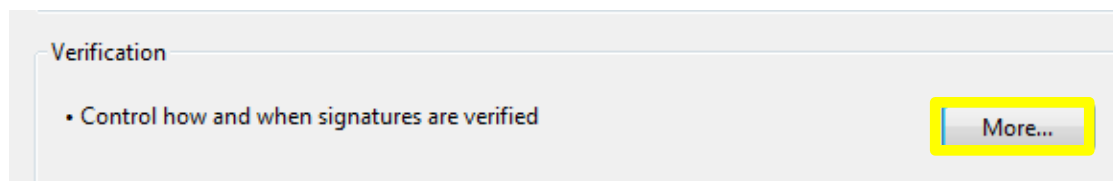


- Click on « Trust Manager »
- Click on the «Uppdate Now» button on the right side underneath of “Automatic European Union Trusted Lists (EUTL)”
- Wait for the confirmation and click « OK » to install the approved certificates.

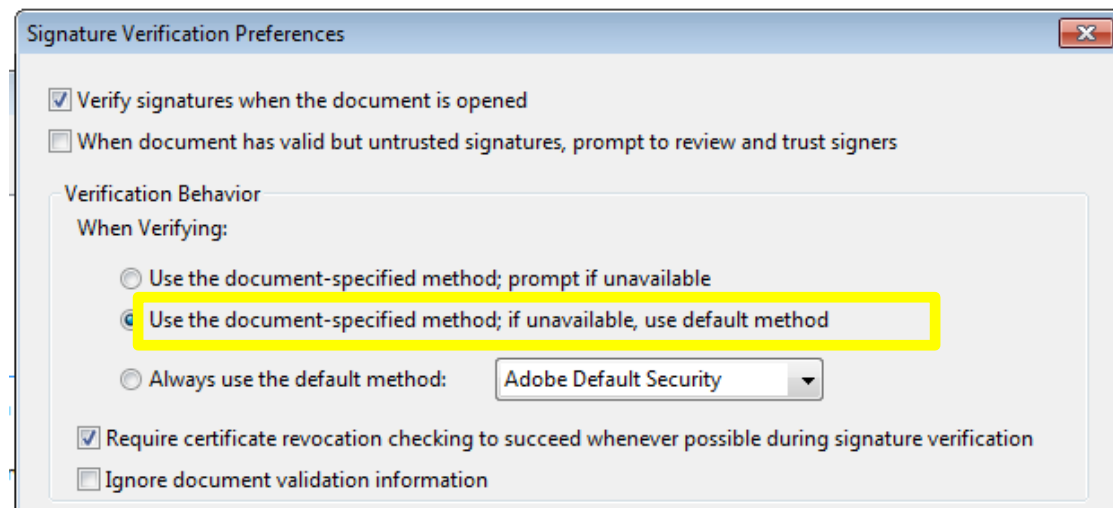


Verification Behaviour

Open the Edit Tab: → Preferences → Signatures → Digital Signature → Verification and click on “More...”

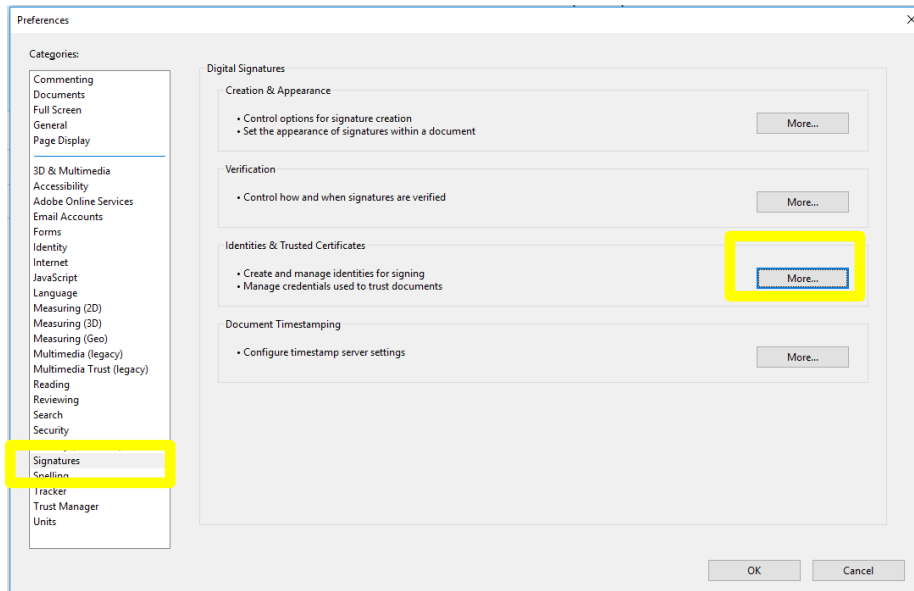


Set then the document specified method, if unavailable, use default method and validate with “Ok”.



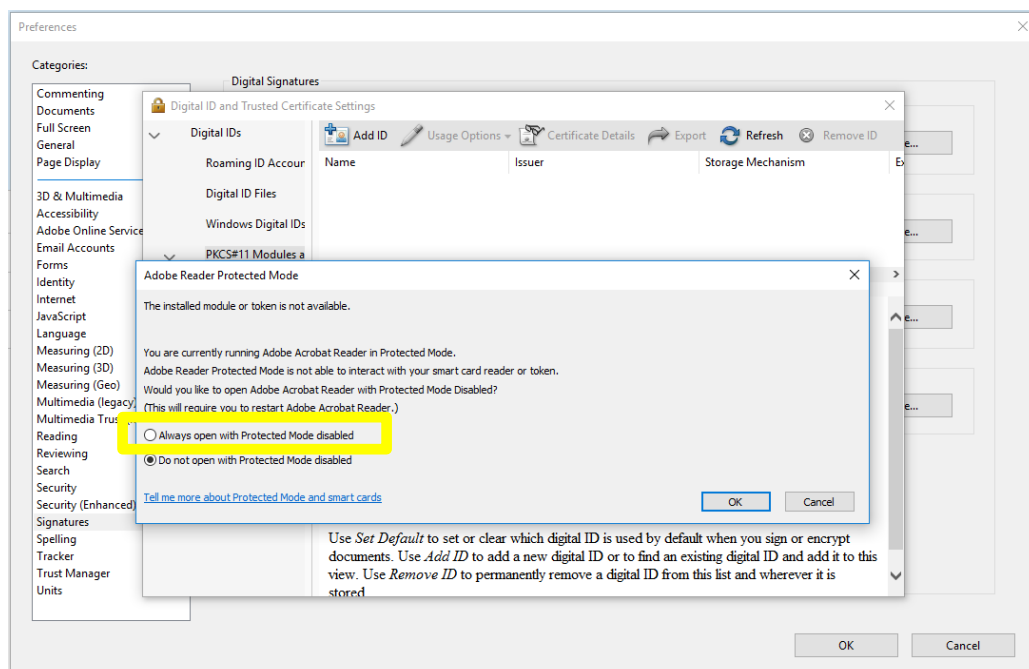
Steps to add the PKCS#11 module in Adobe DC:

- 1) Insert your LuxTrust SmartCard in your reader or plug in your Signing Stick in the USB port of your PC.
- 2) Choose the option « Signatures » in the categories and click on the “More...” button in the « Identities & Trusted Certificates » section.



- 3) Click on « **PKCS#11 Modules and Tokens** »
Attention: If Adobe shows the following message

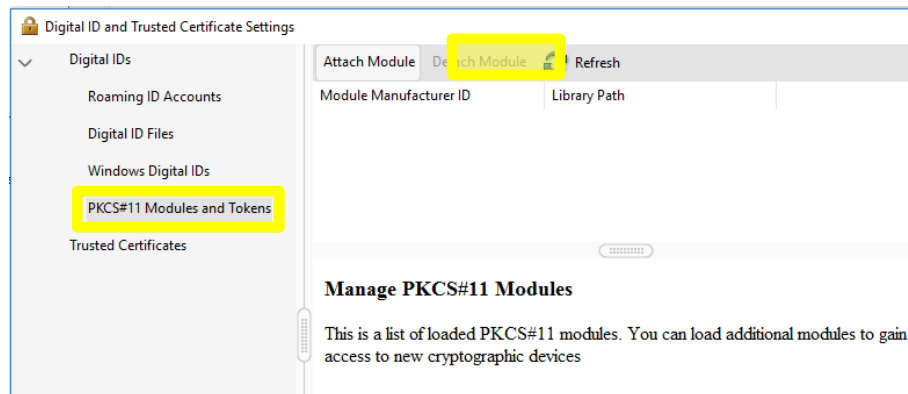
- Choose the first option « Always open with Protected Mode disabled » and confirm with « OK »



IMPORTANT

The changes will only take effect after you restart Adobe.

- Restart at the step II.3 .1 to continue:
- 4) Click on « PKCS#11 Modules and Tokens » and then on « Attach Module »



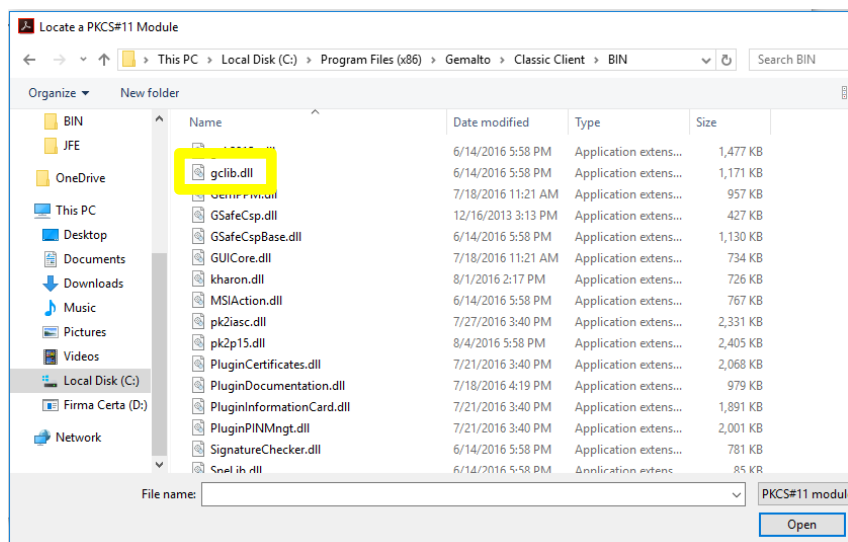
The standard installation directory of the Gemalto software depends on the Windows ¹ version that is used:

For a 64 bit version of Windows: C:\Program Files (x86)\Gemalto

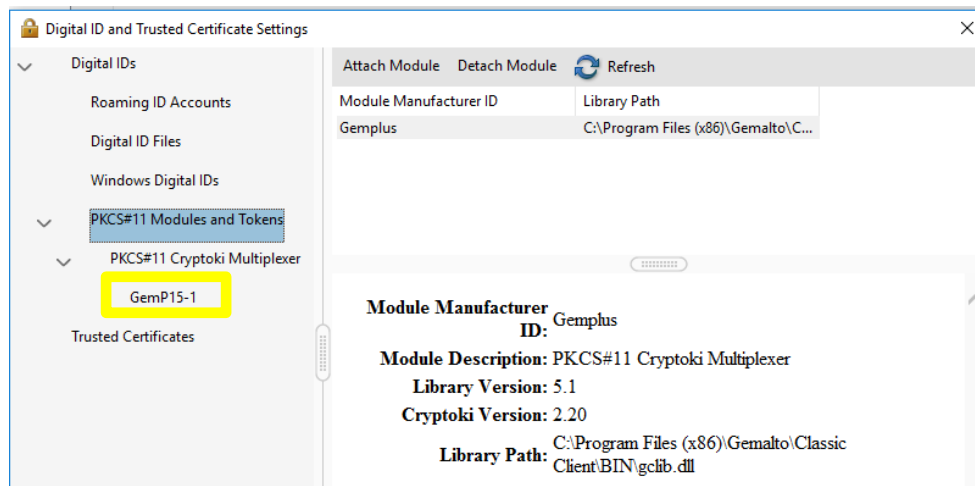
For a 32 bit version of Windows : C:\Program Files\Gemalto

Note: If you have a "C:\Program Files (x86)\\" directory, you are using Windows 64 bits.

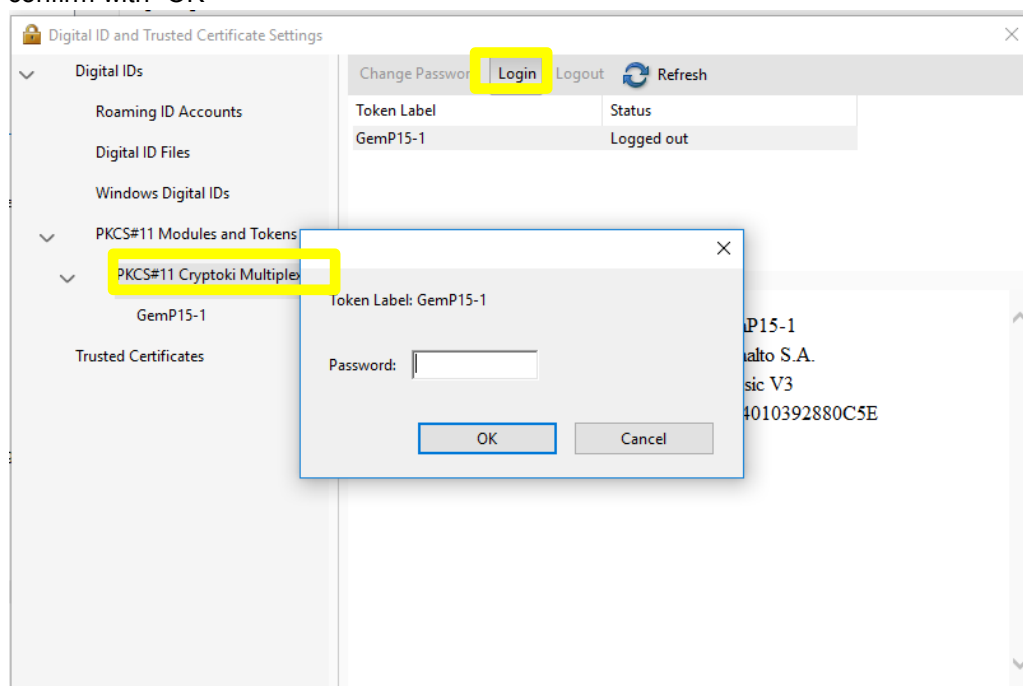
- In the window that opens, choose the directory in which the Gemalto software is installed and open the sub-folder **Classic Client\BIN** to select the « gclib.dll ».



- Validate your choice by clicking on «Open »
- 5) As soon as you added the PKCS#11 module you will see the following window. Click on “GemP15-1”.

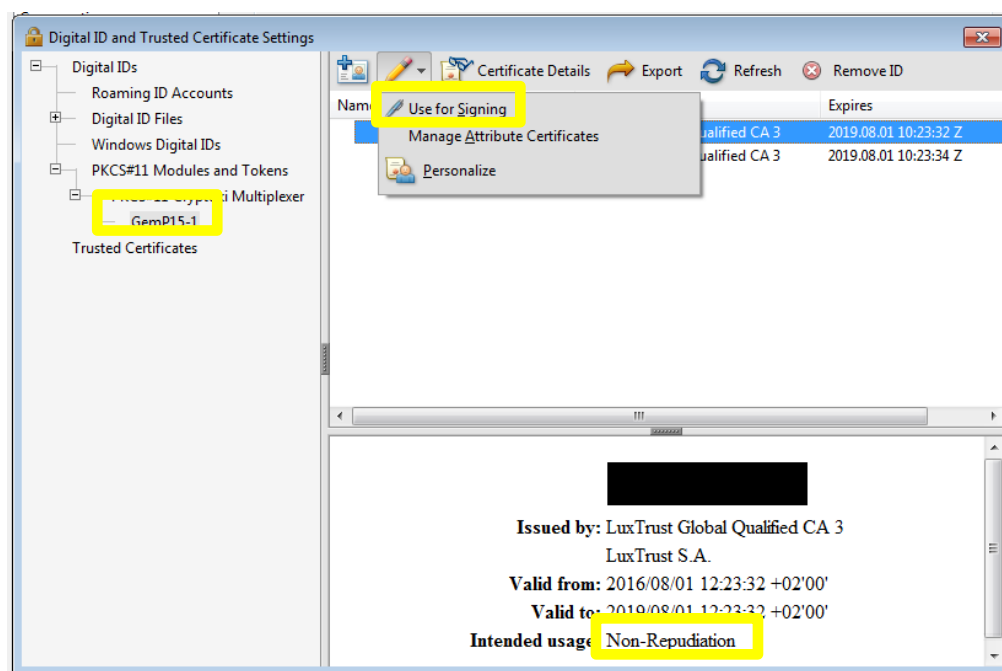


Note: To circumvent the need to enter your PIN code multiple times in this session, click on “PKCS#11 Cryptoki Multiplexer” and on “Login”. Now enter your PIN and confirm with “OK”



The status of the GemP15-1 token will now change to “Logged in”.

- 6) Open the GemP15-1 token, now choose the certificate with the intended usage “Non-Repudation”.
- Should you not see any elements in the list, push on the “Refresh” button
- Now click on the pencil on the top -> Use for Signing

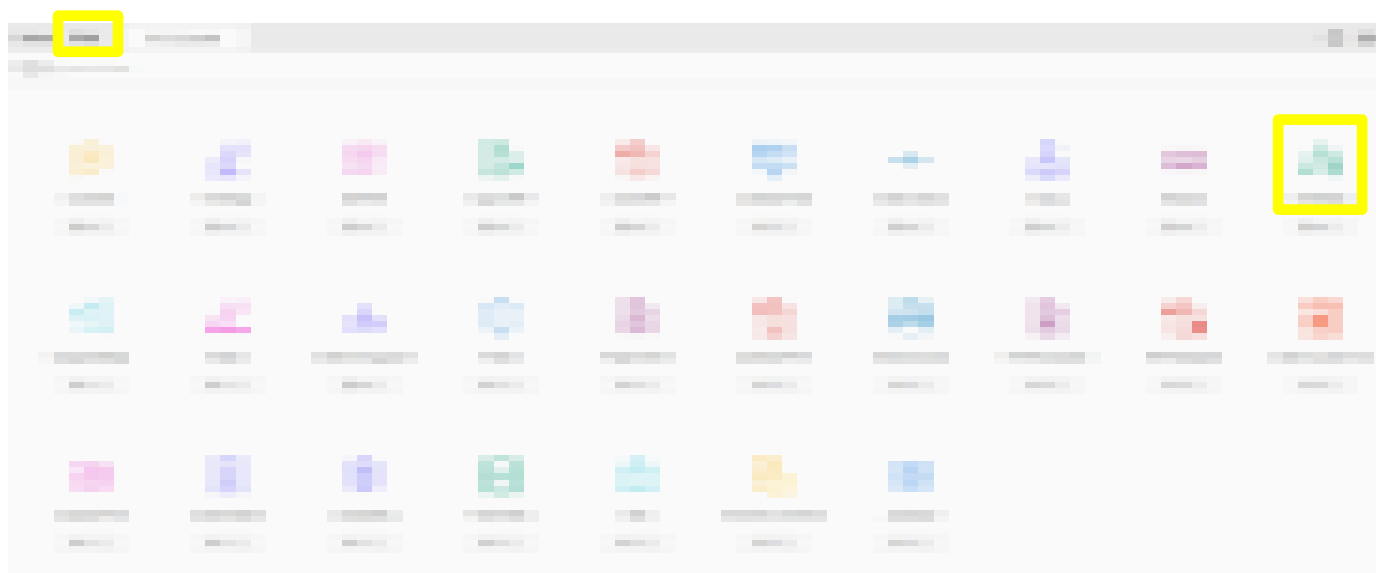


The pencil should now be shown in front of the PKCS#11 token ID (Non-Repudiation).

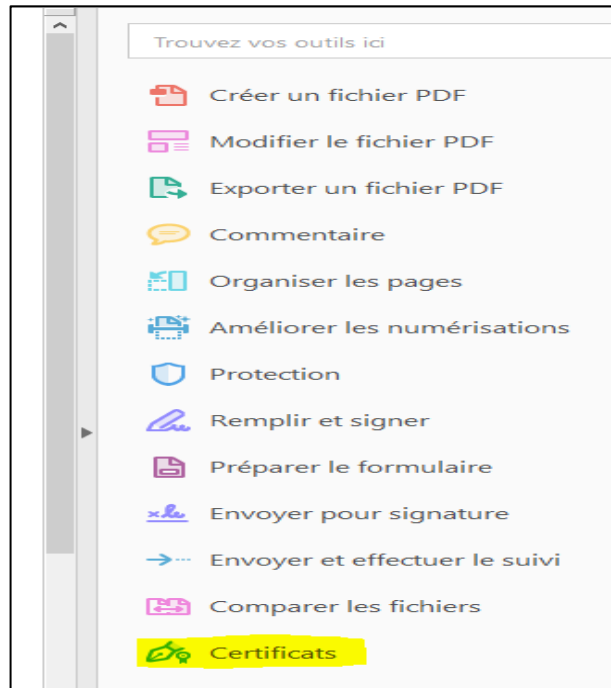
3. Signing a document

To sign documents follow these steps:

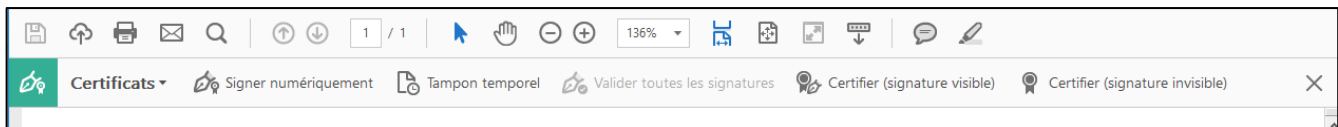
- For the standard Adobe (Reader) version click on “Tools” on the left side and then on “Certificates”.



- In the Adobe Pro version click on “Certificates” at the right.



A new toolbox will appear on top of the window. (the options might be different, depending on the Adobe version):



- 1) If you want to sign a document as a natural person choose the “Sign electronically” option, if you want to sign it with an eSeal certificate choose “Certify” (Pro version of Adobe required).
- 2) To visually put the signature on the document, push the left mouse button and drag a rectangle at the place you want the signature to appear. You will automatically be redirected to the next step
- 3) At this stage a list with certificates is shown.

Signer avec une identification numérique [X]

Choisissez l'identification numérique à utiliser pour la signature : [Actualiser]

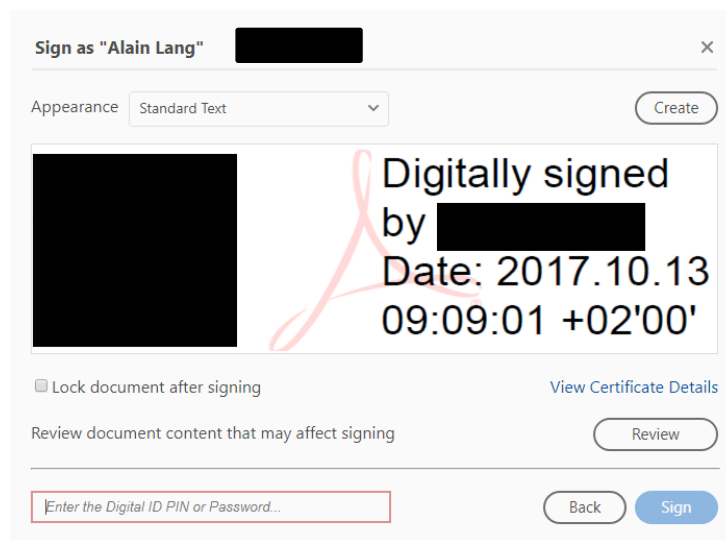
☒ [Icon] [Redacted] (Périphérique PKCS#11)
Délivré par : LuxTrust Global Qualified CA 3, Date d'expiration : 2019.08.03

☐ [Icon] [Redacted] (ID numérique Windows)
Délivré par : LuxTrust Global Qualified CA 3, Date d'expiration : 2019.08.03

[Afficher les détails] (next to Windows ID)

[?] [Configurer un nouvel ID numérique] [Annuler] [Continuer]

- By default the certificate that you chose at step II.6 is selected (PKCS#11 – Non-Repudiation) so you can click "Continue".
- 4) Enter your PIN in the field at the bottom left¹ (only shown if you didn't do the steps in II.3.4 and/or you did unplug your device)



Sign as "Alain Lang" [redacted]

Appearance: Standard Text [v] Create

Digitally signed by [redacted]
Date: 2017.10.13 09:09:01 +02'00'

☐ Lock document after signing View Certificate Details

Review document content that may affect signing Review

Enter the Digital ID PIN or Password... Back Sign

- 5) Click on "Sign".
- 6) Adobe will ask to save the signed document.

If the signature has been correctly inserted you will see the following information on top of your document and your signature will appear in the zone on which you placed it.

