



AWP 5.2

How to

Version 1.0 – 03/01/2017

1 Table of contents

| | | |
|----------|---|-----------|
| 1 | TABLE OF CONTENTS..... | 2 |
| 2 | REVISION..... | 5 |
| 3 | INTRODUCTION | 6 |
| | 3.1 Purpose | 6 |
| | 3.2 References..... | 6 |
| | 3.3 Definitions..... | 6 |
| | 3.1 Software and Hardware requirements..... | 7 |
| | 3.1.1 Card Readers..... | 7 |
| | 3.1.1 Operating system | 7 |
| | 3.2 Change log..... | 8 |
| 4 | PACKAGES | 9 |
| | 4.1 [Windows] Packages list..... | 9 |
| | 4.1 [MAC] Packages list..... | 9 |
| | 4.1 [Linux] Packages list | 9 |
| 5 | INSTALL | 10 |
| | 5.1 [Windows] PKCS#11 & CSP | 10 |
| | 5.2 [Windows] Minidrivers..... | 10 |
| | 5.3 [Linux] PKCS#11 | 12 |
| | 5.4 [MAC] PKCS#11 & TokenD | 12 |
| 6 | UNINSTALL | 13 |
| | 6.1 [Windows] PKCS#11 & CSP | 13 |
| | 6.2 [Windows] Minidrivers..... | 13 |
| | 6.3 [Linux] PKCS#11 | 14 |
| | 6.4 [MAC] PKCS#11 & TokenD | 14 |
| 7 | LOG ACTIVATION | 15 |
| | 7.1 Context..... | 15 |
| | 7.2 How to activate logs? | 15 |
| | 7.2.1 [Windows] For Applications based on CSP, PKCS#11 or minidriver..... | 15 |
| | 7.2.2 [Linux & MAC] For applications based on PKCS#11 | 15 |
| | 7.3 FAQ..... | 16 |

| | | |
|-----------|---|-----------|
| 8 | IDENTITY MANAGER | 17 |
| 8.1 | Introduction..... | 17 |
| 8.2 | Launch Identity Manager..... | 17 |
| 8.2.1 | [Windows] Launch | 17 |
| 8.2.1 | [Linux & MAC] Launch | 17 |
| 8.3 | Information Panel | 18 |
| 8.4 | Change Password Panel..... | 19 |
| 8.5 | Unblock Password Panel | 19 |
| 8.6 | Erase Token Panel | 20 |
| 8.7 | Content Panel | 20 |
| 9 | BIOMETRICS..... | 21 |
| 9.1 | Bio readers | 21 |
| 9.2 | Zvetco P6500 reader | 21 |
| 9.3 | Enrollment tool..... | 22 |
| 10 | CONTACTLESS | 24 |
| 10.1 | Add contactless cards with CSP..... | 24 |
| 10.2 | Add contactless cards with minidriver | 24 |
| 11 | COMMERCIAL APPLICATIONS WITH AWP | 26 |
| 11.1 | Introduction..... | 26 |
| 11.1 | Certutil | 26 |
| 11.2 | Internet Explorer..... | 26 |
| 11.2.1 | Requirements | 26 |
| 11.2.2 | TLS authentication..... | 27 |
| 11.1 | Google Chrome | 28 |
| 11.1.1 | Requirements | 28 |
| 11.1.2 | TLS authentication..... | 29 |
| 11.2 | Firefox | 30 |
| 11.2.1 | Requirements | 30 |
| 11.2.2 | TLS authentication..... | 30 |
| 11.3 | Adobe Reader | 31 |
| 11.3.1 | Requirements | 31 |
| 11.3.2 | Digital Signature | 33 |
| 11.4 | Microsoft Word | 34 |
| 11.4.1 | Requirements | 34 |

11.4.1 Digital Signature 34

11.4.2 Word 2010 & 2013 35

2 Revision

| Version | Date | Modification |
|---------|------------|-------------------------------|
| 1.0 | 04/01/2017 | Creation Add packages list |
| | | |
| | | |

3 Introduction

3.1 Purpose

This document gathers information on how to use the AWP middleware from OT.

3.2 References

| | | |
|-----|--|---|
| [1] | PKCS #11 v2.20: Cryptographic Token Interface Standard | ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf |
| [2] | PKCS #15 v1.1: Cryptographic Token Information Syntax Standard | ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-15/pkcs-15v1-1tc2.pdf |
| [3] | IAS ECC Technical Specification – Revision 1.01 | http://www.acsiel.fr/iso_album/ias_ecc_v1_0_1_fr.pdf |
| [4] | PIV Standards | http://csrc.nist.gov/groups/SNS/piv/standards.html |
| [5] | Snooper, OT AWP diagnostic tool | Snooper v1.0 - User Guide.pdf |

3.3 Definitions

| | |
|------------------|---|
| AID | Applet IDentifier (byte string identifying an application on a smart card) |
| APDU | Application Protocol Data Units |
| API | Application Programming Interface |
| ATR | Answer To Reset (byte string sent by a smart card when it is initialized) |
| AWP | Authentic Web Pack |
| CNG | Crypto Next Generation |
| CSP | Cryptographic Service Provider (Microsoft standardized API to perform cryptographic operations) |
| DH | Diffie-Hellmann (public key encryption algorithm) |
| DLL | Dynamic-Link Library file |
| ELC | ELliptic Curves |
| EXE | EXE cutable file |
| GUID | Globally Unique Identifier |
| IAS - ECC | Identification-Authentication-Signature – European Citizen Card |
| MD | MiniDriver |
| MSIE | MicroSoft Internet Explorer |
| KSP | Key Storage Provider |
| OP | Operating System |

| | |
|--------------|---|
| PC/SC | Personal Computer / Smart Card (Standardized API to communicate with smart cards) |
| PDF | Portable Document Format |
| PIN | Personal Identifier Number |
| PIV | Personal Identification Verification |
| PUK | PIN Unlock Key |
| PKCS | Public-Key Cryptography Standards (RSA Laboratories standards) |
| PTC | Pin Try Counter |
| P11 | PKCS#11 Standard |
| P15 | PKCS#15 Standard |
| RSA | Rivest-Shamir-Adleman (asymmetric key encryption algorithm) |

3.1 Software and Hardware requirements

3.1.1 Card Readers

AWP supports any PCSC v1/PCSC v2 compliant card readers.

It supports any PIN pads compliant PCSC V2.

Only Omnikey 3821 has been validated with AWP.

Compatible readers are available on Windows Compatibility Center:

<http://www.microsoft.com/en-us/windows/compatibility/CompatCenter/ProductViewerWithDefaultFilters?TempOsid=Windows%208.1&Locale=en-us&Type=Hardware&ProductCategory=Mice%2C%20keyboards%20%26%20input%20devices>

3.1.1 Operating system

| Operating Systems | Releases |
|-------------------|--|
| Windows | 7, 8.1 and 10 (32 & 64 bits) |
| Linux | Ubuntu 12.04 LTS (32 & 64 bits) Ubuntu 14.04 LTS and 16.04 LTS (64 bits) RedHat 7.2 64bits CentOS 7.2 64 bits |
| MAC OSX | 10.7 (Lion), 10.8 (Mountain Lion), 10.9 (Maverick), 10.10 (Yosemite), 10.11 (El Capitan), 10.12 (Sierra) |

3.2 Change log

| Versioning | New features |
|-------------------------|--|
| From 5.0 SR1 to 5.0 SR2 | <ul style="list-style-type: none"> - Default certificate management (logon) - Event log under windows: <ul style="list-style-type: none"> ▪ PIN and PUK changes ▪ Wrong PIN and PUK entered ▪ PIN and PUK expired ▪ PIN and PUK locked |
| From 5.0 SR2 to 5.1 SR1 | <p>Major features:</p> <ul style="list-style-type: none"> - Biometry for Linux, - Support of PIV v2.3.5 applet - Support ID-One Cosmo V8 - Support MAC OX 10.9 <p>Minor features:</p> <ul style="list-style-type: none"> - AWP Manager : Manage the “P7” extension for the certificate import - XML file and registry : Add Sergas ATR - Support of ID-ONE MSFT - Support opacity on Cosmo V8 (this option is activated by default) - AWP Manager : DLL versions are dynamically retrieved and displayed in the “about” dialog box - Set the last generated key pair as default container - Credential provider for smart card login - Support multi ADF in IAS minidriver (read :all ADF, write only the default one) - AWP Manager optionally reads the PIN policy on AuthenticV3 (P11, CSP, minidriver) - UAC management during install under Windows - It's not possible anymore to import the same certificate twice - PKCS#11 : Proprietary API has been developed to retrieve the remaining tries (PIN / PUK) - Support new return for get version on AuthenticV3 (3 bytes instead of 2 bytes) |
| From 5.1 SR1 to 5.2 SR1 | <ul style="list-style-type: none"> - Support of PIV 2.4.0 - Support of AuthenticV3.2.5 - Support of Cosmo V8.1 - RSA_PSS padding support on AuthenticV3 and PIV (P11 / Minidriver, off card version only) - Support of new bio CHV manager - Support Opacity V2.0 for PIV 2.4 - Support Widows 10 - Support MAC OSX until 10.12 - Support of certificate online and compressed certificates on PIV - Support of pairing code on PIV - Elliptic curves on IAS - Include Italian translation - Enforced PIN Policy rules |

4 Packages

4.1 [Windows] Packages list

| | Package name | Windows | | Cryptographic API | | | Synchroniser | Identity Manager | |
|----------------------------|---|---------|--------|-------------------|-----|-----------------|--------------|------------------|------|
| | | 32-bit | 64-bit | PKCS11 | CSP | Minidriver | | ADMIN | USER |
| With PKCS11 | AWP 5.2.0 SR2 64-bit.msi | | X | X | | All | X | | X |
| | AWP 5.2.0 SR2.msi | X | | X | | All | X | | X |
| | AWP 5.2.0 SR2 Admin 64-bit.msi | | X | X | | All | X | X | |
| | AWP 5.2.0 SR2 Admin.msi | X | | X | | All | X | X | |
| | AWP 5.2.0 SR2 CSP 64-bit.msi | | X | X | X | | X | | X |
| | AWP 5.2.0 SR2 CSP Admin 64-bit.msi | | X | X | X | | X | X | |
| | AWP 5.2.0 SR2 CSP Admin.msi | X | | X | X | | X | X | |
| | AWP 5.2.0 SR2 CSP.msi | X | | X | X | | X | | X |
| | AWP 5.2.0 SR2 P11 Only 64-bit.msi | | X | X | | | | | X |
| | AWP 5.2.0 SR2 P11 Only Admin 64-bit.msi | | X | X | | | | | X |
| | AWP 5.2.0 SR2 P11 Only Admin.msi | X | | X | | | | | X |
| AWP 5.2.0 SR2 P11 Only.msi | X | | X | | | | X | | |
| Minidriver only | AuthenticV3Minidriver-1.4.4 64-bit.msi | | X | | | AuthenticV3 | | | |
| | AuthenticV3Minidriver-1.4.4.msi | X | | | | AuthenticV3 | | | |
| | IasEccMinidriver-2.4.3 64-bit.msi | | X | | | IAS-ECC v1 & v2 | | | |
| | IasEccMinidriver-2.4.3.msi | X | | | | IAS-ECC v1 & v2 | | | |
| | PivMinidriver-1.3.4 64-bit.msi | | X | | | PIV <= 2.3.5 | | | |
| | PivMinidriver-1.3.4.msi | X | | | | PIV <= 2.3.5 | | | |
| | PivCivMinidriver-1.0.4 64-bit.msi | | X | | | PIV >= 2.4.0 | | | |
| | PivCivMinidriver-1.0.4.msi | X | | | | PIV >= 2.4.0 | | | |

4.1[MAC] Packages list

| Package name | Cryptographic API | | Identity Manager | |
|-------------------------|-------------------|---------|------------------|------|
| | PKCS11 | Token D | ADMIN | USER |
| AWP_5.2.0_SR2.dmg | X | X | | X |
| AWP_5.2.0_SR2_Admin.dmg | X | X | X | |

4.1[Linux] Packages list

The packages depend on the Linux distribution and version. Thus the list is not relevant.

5 INSTALL

Please uninstall all middleware from OT or any provider before installing a new one.

5.1 [Windows] PKCS#11 & CSP

Packages with 64-bit prefix will be installed on 64-bit OS only.

Packages with no 64-bit prefix will be installed on 32-bit OS only.

Double click on the .msi and follow instructions. A reboot is necessary.

5.2 [Windows] Minidrivers

Minidrivers can be installed on Microsoft OS starting from Windows 7. They have been certified by Microsoft.

Minidrivers shall never be installed together with CSP module to avoid any conflict.

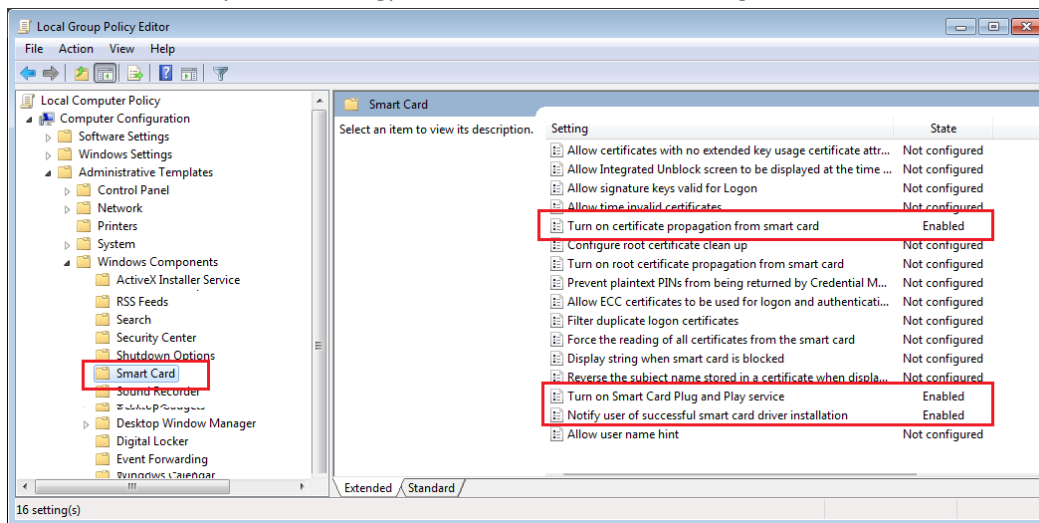
There are 3 ways to install them:

- Plug & play (default solution):

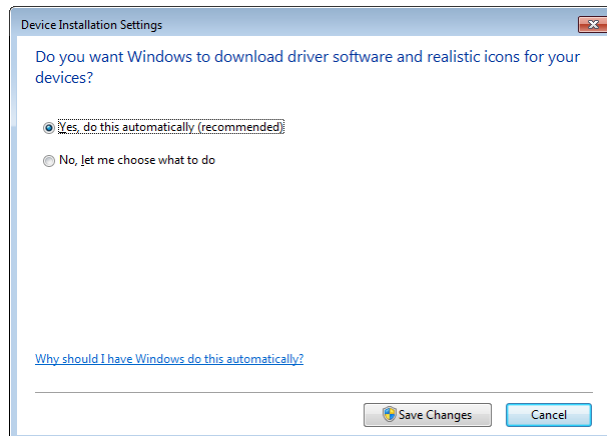
Activate plug & play in the Group Policy Object (GPO):

[http://technet.microsoft.com/fr-fr/library/ff404287\(v=ws.10\).aspx](http://technet.microsoft.com/fr-fr/library/ff404287(v=ws.10).aspx)

For example, execute gpedit.msc and select following services



Go in "Control Panel/All Control Items/System" (shortcut Win7 = "Win" + "Pause"). Select "Advanced system settings" then "Hardware", "Device Installation Settings" and "Yes, do this automatically'. Save Changes.



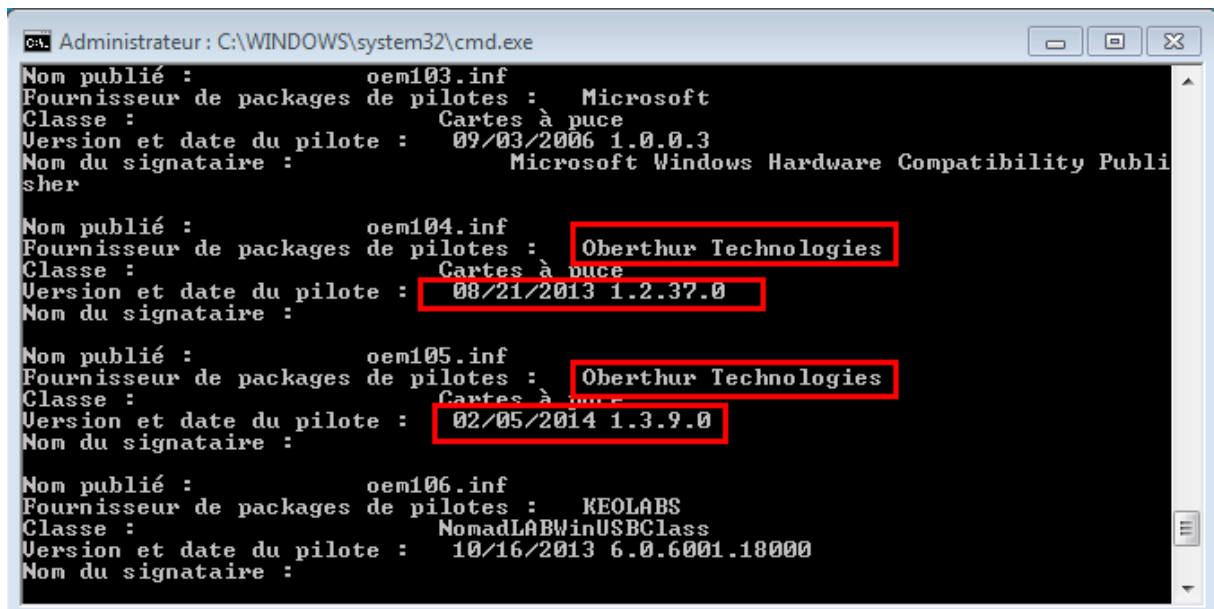
Insert the card in the reader.

The Minidrivers will be downloaded from Windows Update web site

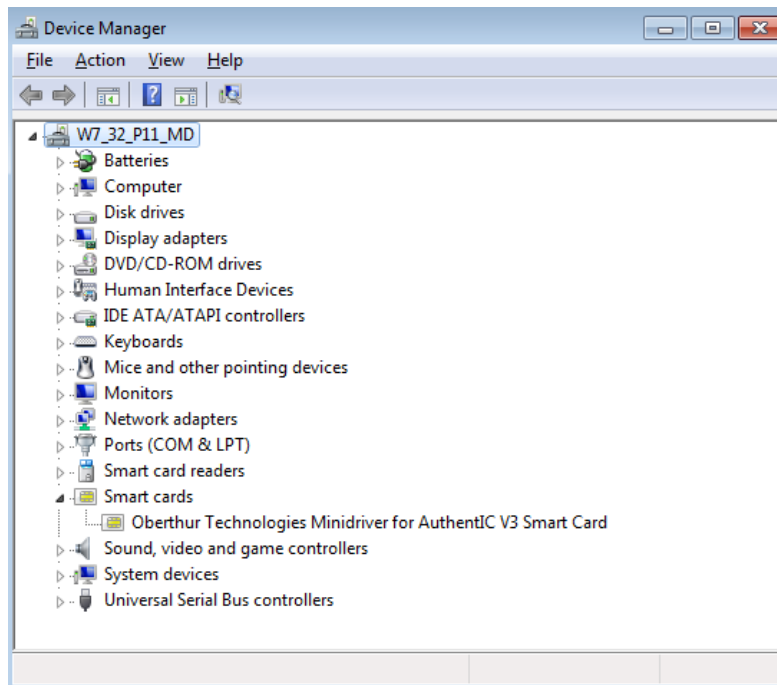
- Download Minidrivers from Microsoft Update Catalog:
<https://catalog.update.microsoft.com/v7/site/Search.aspx?q=oberthur>
 Choose the latest item for your device "Authentic", "IAS-ECC" or "PIV"
 Then, install the .cab fil. Example:

```
pkgmgr /ip /m:<path><file name>.cab /quiet
```
- Install the minidriver from the .msi provided by OT

In command line, execute "pnputil -e" to check that Oberthur Minidrivers are available.



The smart card must be detected and recognized in the device manager (devmgmt.msc).



After installation, it is not necessary to reboot Windows.

5.3 [Linux] PKCS#11

Packages with amd64 prefix will be installed on 64-bit OS only.

Packages with i386 prefix will be installed on 32-bit OS only.

Double click on the .deb and follow instructions

OR, for Debian based distribution,

```
# sudo apt-get install AWP_5.2.0_SR1_Admin_amd64.deb
```

And enter the admin password.

To install PKCS#11 module for applications (Example: Google Chrome) which requires a plugin, execute the following commands:

```
# sudo apt-get install libnss-tools
```

```
# modutil -dbdir sql:$HOME/.pki/nssdb -add "OT AWP" --libfile  
"/usr/local/AWP/lib/libOcsCryptoki.so" :$
```

5.4 [MAC] PKCS#11 & TokenD

Double click on the .pkg and follow instructions. Then reboot the laptop.

6 UNINSTALL

Cards must be removed from the readers prior starting the uninstall process.

6.1 [Windows] PKCS#11 & CSP

Go to control Panel, uninstall programs. Select AWP and right click to uninstall it.

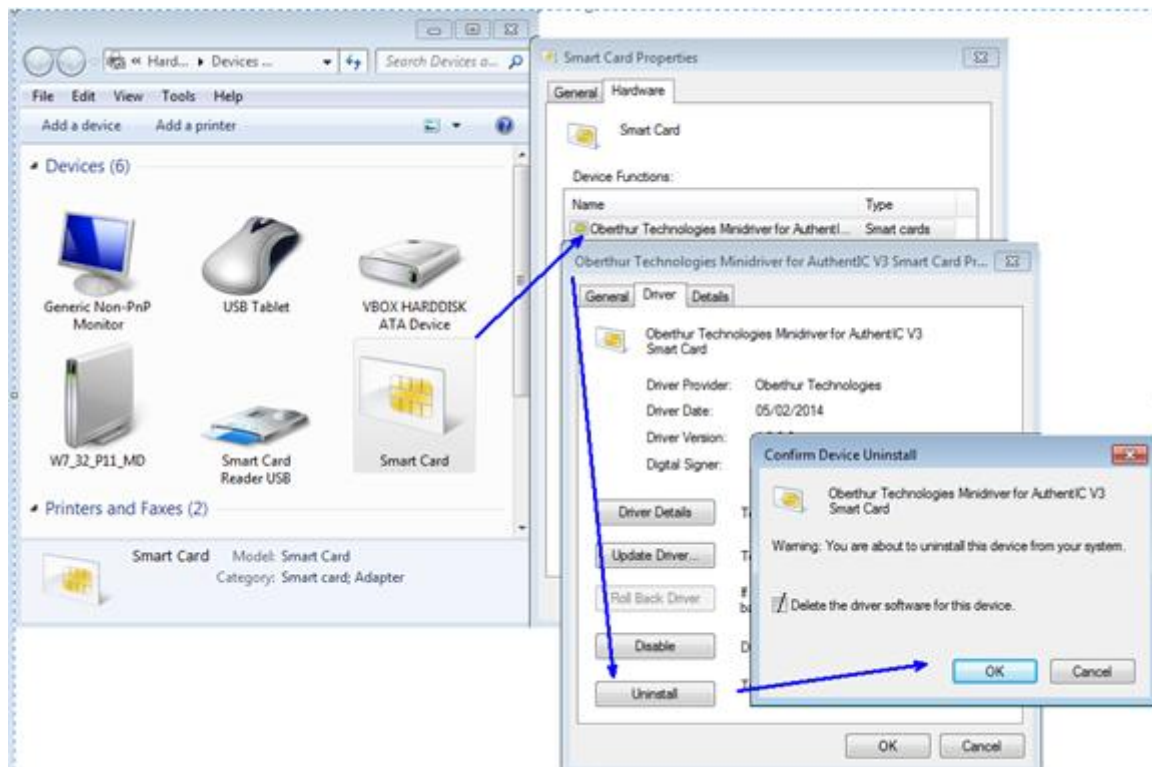
6.2 [Windows] Minidrivers

If Minidrivers were installed with .msi:

Go to control Panel, uninstall programs. Select OT Minidrivers (Authentic, IAS or PIV) and right click to uninstall it.

In all cases, uninstall the drivers:

1-Insert a smart card, go to the device manager and uninstall the drivers:



Next steps are required to have a clean installation only.

2- Remove card from reader

3- Reboot

4- Delete entries in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\Cache

5- In HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards

Delete the following folders:

PIV Device ATR Cache

AuthenticV3

IASECC

6- in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oberthur Technologies\MiniDriver

Delete folders: pivminidriver, authenticv3minidriver and laseccminidriver

7- in C:\Windows\System32\DriverStore\FileRepository

and in C:\Windows\SysWOW64\DriverStore\FileRepository

delete the following folders:

laseccminidriver.*

authenticv3minidriver.*

pivminidriver*

6.3 [Linux] PKCS#11

For Debian based distributions:

```
# sudo apt-get remove awp
```

For other distribution, use **rpm** command

6.4 [MAC] PKCS#11 & TokenD

Open Terminal

```
# cd /usr/local/AWP
```

```
# sudo ./awp_uninstall.sh
```

7 LOG ACTIVATION

7.1 Context

The middleware provides means to activate logs in order to analyze the behaviour of the middleware when an issue occurs.

7.2 How to activate logs?

Identity Manager allows enabling logs for PKCS11 module only. Simply go in “parameters > Settings” menu. Log activation depends from the OS and the middleware interface and the following chapters gives more details.

7.2.1 [Windows] For Applications based on CSP, PKCS#11 or minidriver

For this OS, it is highly recommended to use the user friendly diagnostic tool “Snooper” which enables logs and creates a detailed report. See [5] for more details.

7.2.2 [Linux & MAC] For applications based on PKCS#11

A single configuration file must be updated:

Edit the file

For Linux: # sudo gedit /usr/local/AWP/OCSMiddlewareConf.xml

For MAC: # sudo nano /usr/local/AWP/OCSMiddlewareConf.xml

And update the log tag:

```
<Log Activate="1" Path="/usr/OTLogs" DebugLevel="DEBUG"></Log>
```

Create the folder ‘OTLogs’:

```
# sudo mkdir /usr/OTLogs
```

Set access conditions for writing:

```
# sudo chown -R username OTLogs (use your username)
```

```
# sudo chgrp users OTLogs (set the rights to users group)
```

```
# chmod 775 OTLogs (set writing access)
```

```
# sudo adduser username users (add your user in the group)
```

7.3 FAQ

| Question | Answer |
|--|---|
| The xml configuration file has been updated to generate logs but no log has been generated | <ul style="list-style-type: none"> - For 64 bits OS, check that the 2 xml files have been updated - Check the consistency of the xml file with a parser, like Internet Explorer. - Restart the application that must be logged. Check that it is not running in background. If necessary, reboot the system. |
| Some logs are missing | <p>The log folder may be not available for writing, especially when the user session is not established. Change the log folder with this one:</p> <p>C:\Users\%username%\AppData\LocalLow\OTlogs\ Where %username% is the user login</p> |

8 Identity Manager

8.1 Introduction

“Identity manager” is a tool which performs cryptographic actions with the smart cards. It is part of the AWP packages and is available for Windows, Linux and MAC OS. It communicates with the cards through PKCS#11 module. **The AWP identity Manager is not part of the middleware but is only a tool.**

There is one configuration for administrators and another one for users with limited feature. Here are the main differences:

| | User | Admin |
|-----------------------|------|-------------------------------------|
| Unblock PIN | | <input checked="" type="checkbox"/> |
| Change PUK | | <input checked="" type="checkbox"/> |
| Init Token | | <input checked="" type="checkbox"/> |
| Generate Key | | <input checked="" type="checkbox"/> |
| Import Key | | <input checked="" type="checkbox"/> |
| Edit Label | | <input checked="" type="checkbox"/> |
| Delete Object | | <input checked="" type="checkbox"/> |
| Set Default Container | | <input checked="" type="checkbox"/> |

The Admin configuration is described in the following chapters.

8.2 Launch Identity Manager

8.2.1 [Windows] Launch

The tool can be launched from the start menu in the “AWP” folder or by selecting the .exe file.

| OS | Configuration file location |
|---------|--|
| 32 bits | C:\Program Files\Oberthur Technologies\AWP\IdentityManager.exe |
| 64 bits | C:\Program Files (x86)\Oberthur Technologies\AWP\IdentityManager.exe |

8.2.1 [Linux & MAC] Launch

Look for the application “Identity Manager”

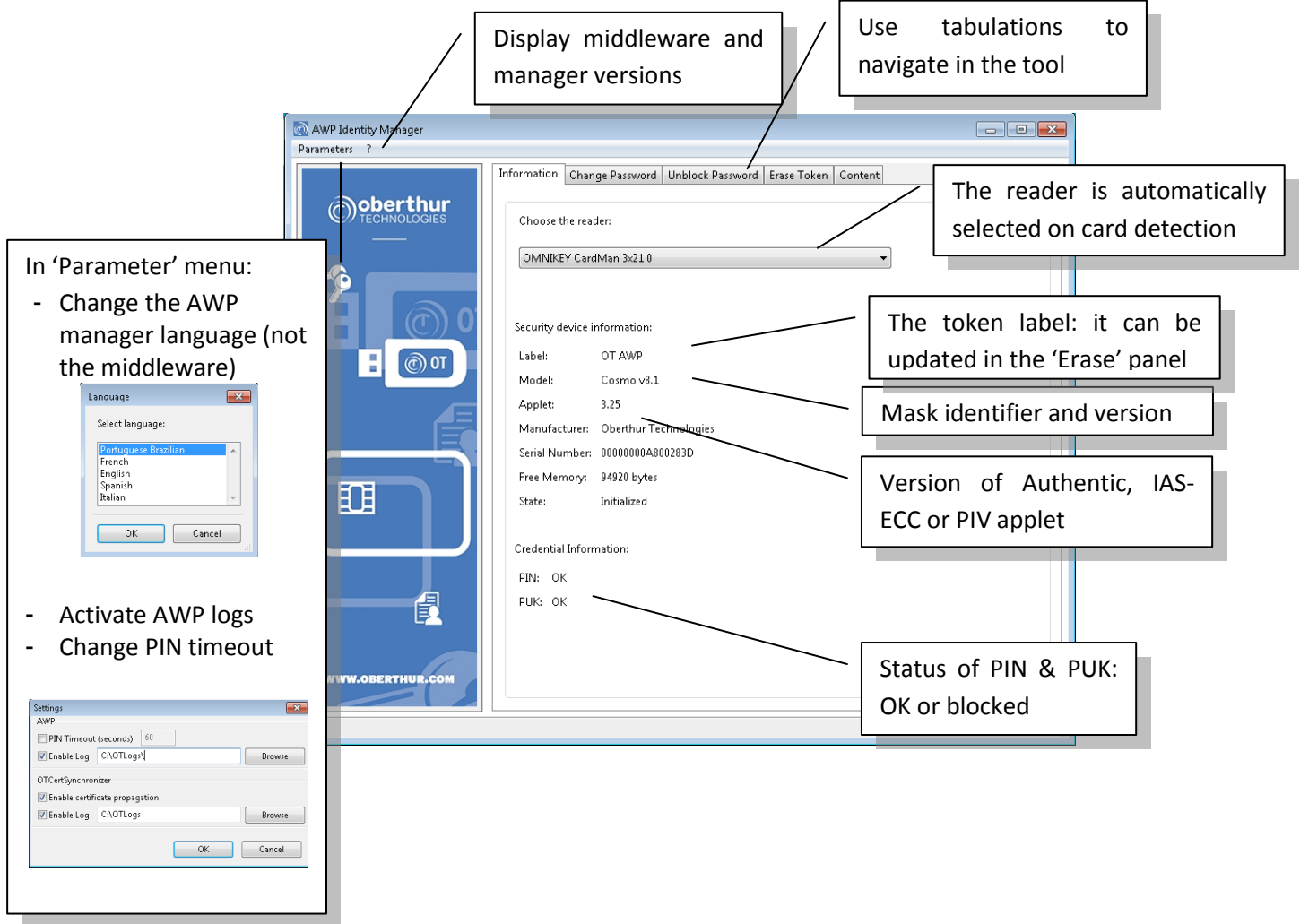


or use terminal:

```
#./usr/local/AWP/IdentityManager
```

8.3 Information Panel

This panel allows selecting a smartcard reader and displays the main card information and versions.



Display middleware and manager versions

Use tabulations to navigate in the tool

The reader is automatically selected on card detection

The token label: it can be updated in the 'Erase' panel

Mask identifier and version

Version of Authentic, IAS-ECC or PIV applet

Status of PIN & PUK: OK or blocked

In 'Parameter' menu:

- Change the AWP manager language (not the middleware)
- Activate AWP logs
- Change PIN timeout

Information Panel Data:

Choose the reader: OMNIKEY CardMan 3x21.0

Security device information:

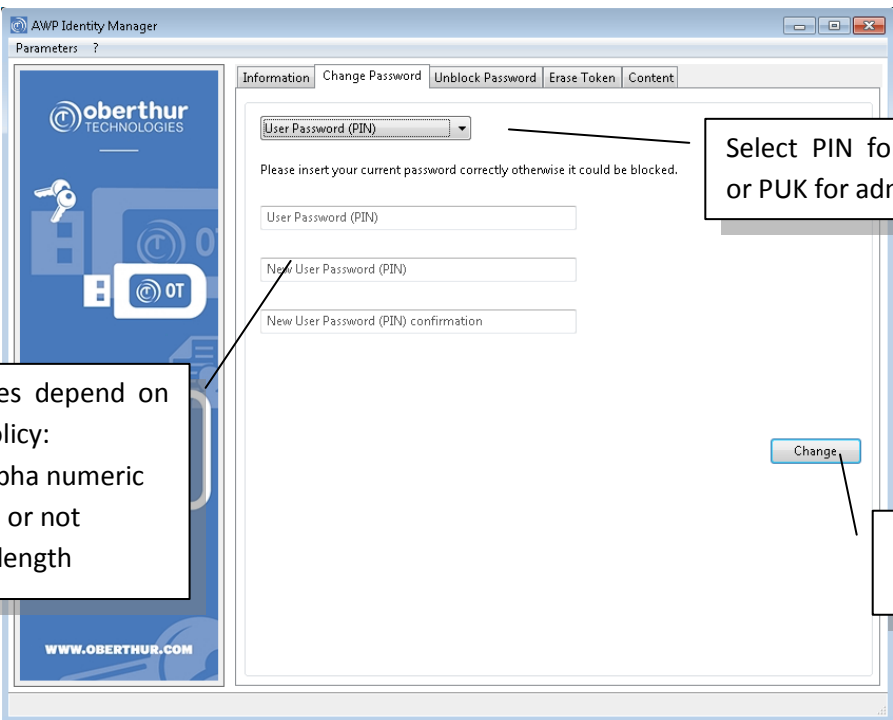
| | |
|----------------|-----------------------|
| Label: | OT AWP |
| Model: | Cosmo v8.1 |
| Applet: | 3.25 |
| Manufacturer: | Oberthur Technologies |
| Serial Number: | 0000000A800283D |
| Free Memory: | 94920 bytes |
| State: | Initialized |

Credential Information:

| | |
|------|----|
| PIN: | OK |
| PUK: | OK |

8.4 Change Password Panel

This panel allows changing the User (PIN) and administrator (PUK) passwords.



AWP Identity Manager
Parameters ?

Information | **Change Password** | Unlock Password | Erase Token | Content

User Password (PIN)

Please insert your current password correctly otherwise it could be blocked.

User Password (PIN)

New User Password (PIN)

New User Password (PIN) confirmation

Change

Select PIN for user or PUK for admin

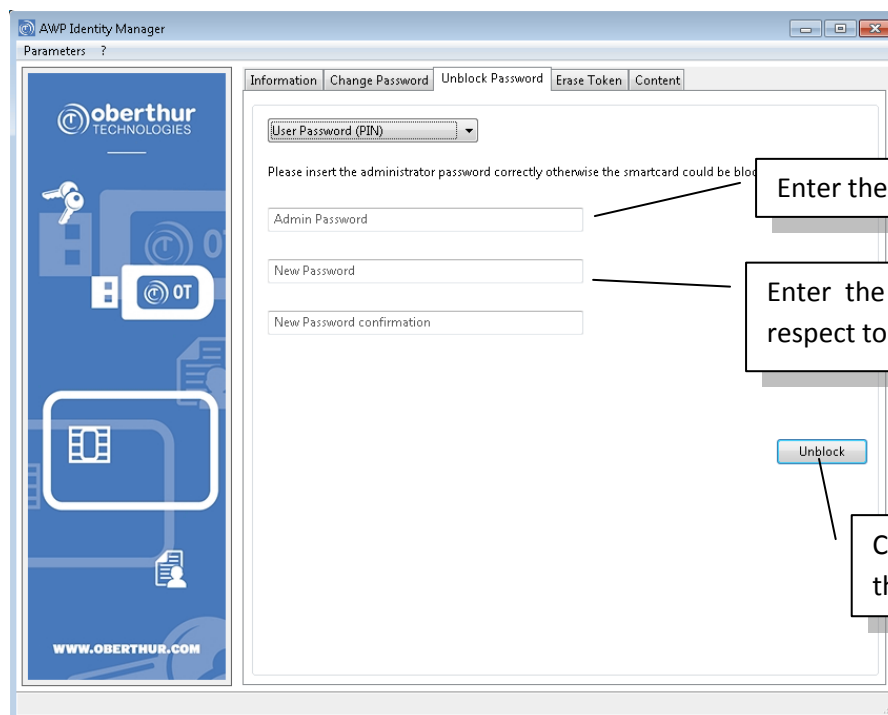
Password values depend on the card PIN policy:

- Numeric of alpha numeric
- Case sensitive or not
- Min and max length

Click to change the password

8.5 Unblock Password Panel

This panel allows unblocking the PIN thanks to the PUK.



AWP Identity Manager
Parameters ?

Information | Change Password | **Unlock Password** | Erase Token | Content

User Password (PIN)

Please insert the administrator password correctly otherwise the smartcard could be blocked.

Admin Password

New Password

New Password confirmation

Unlock

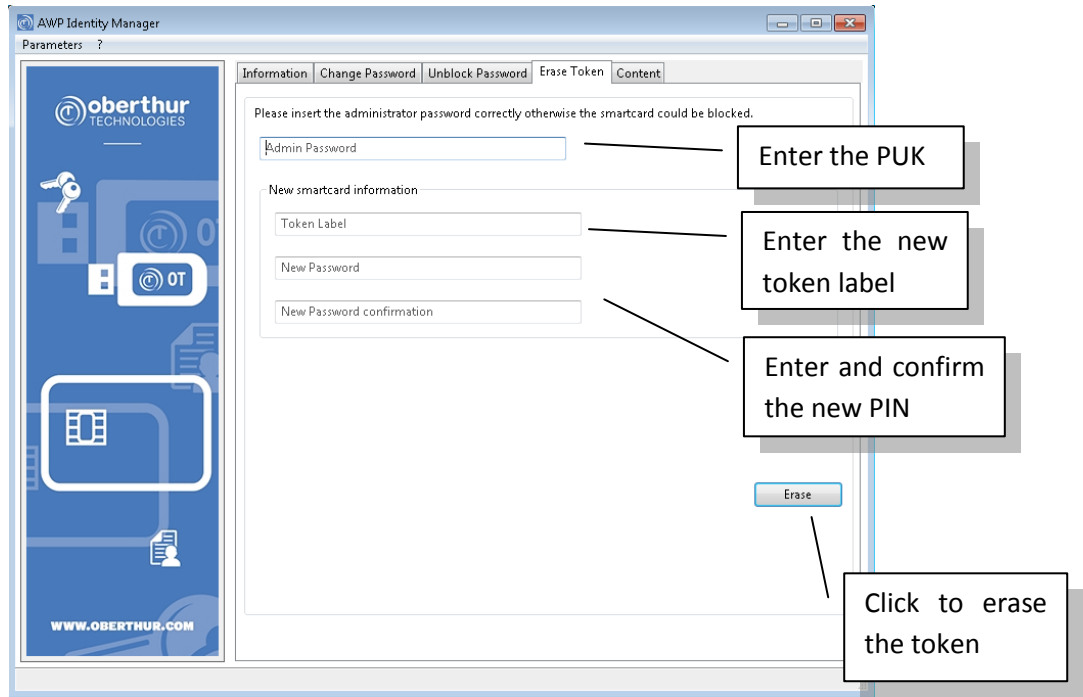
Enter the PUK

Enter the new PIN with respect to the PIN policy

Click to unblock the PIN

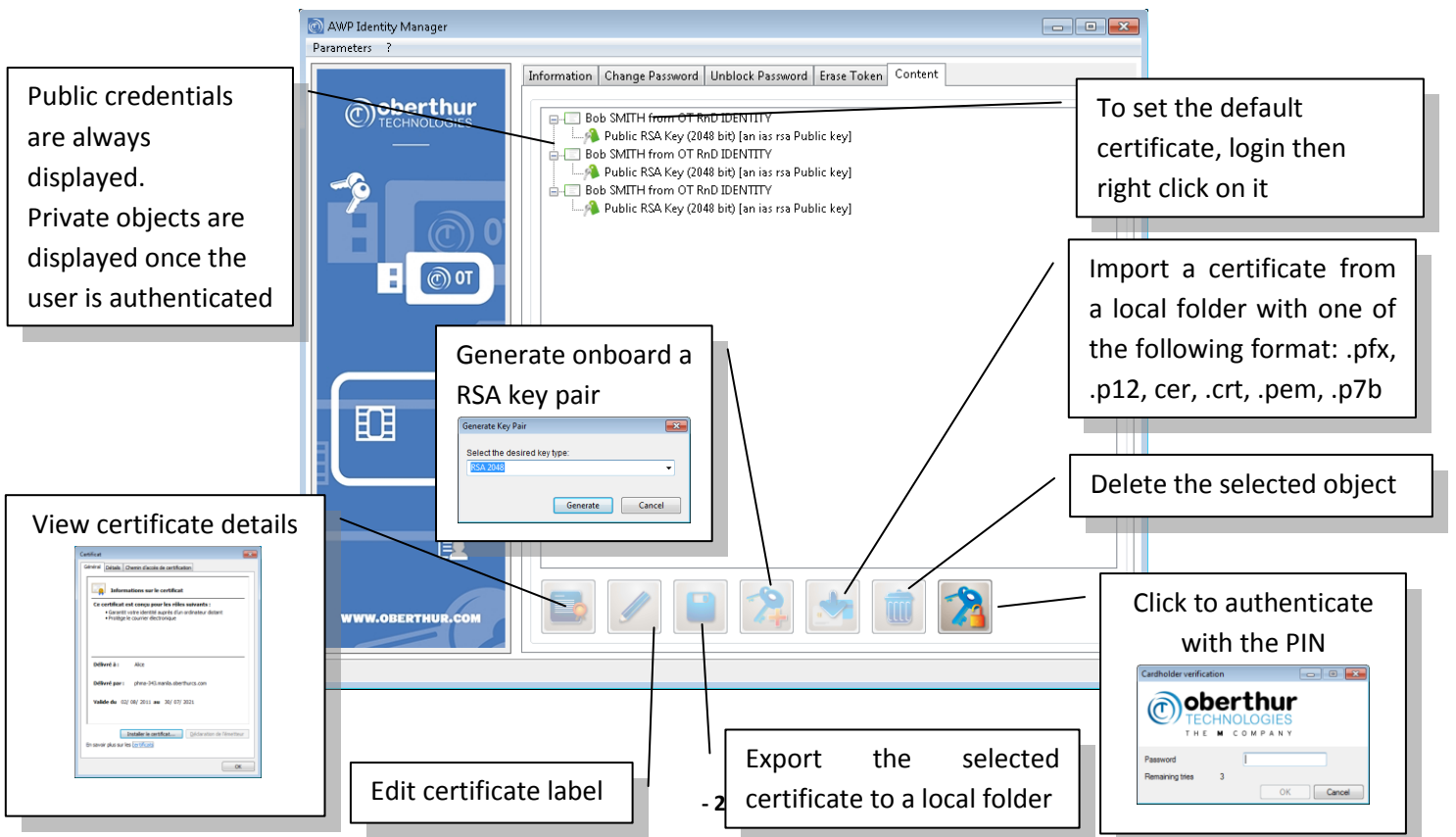
8.6 Erase Token Panel

This panel allows erasing the content of the token (private keys and certificates). At the same time, it is possible to change the token label. This feature requires the PUK.



8.7 Content Panel

This panel allows erasing the content of the token (private keys and certificates). At the same time, it is possible to change the token label.



9 Biometrics

9.1 Bio readers

The following fingerprint scanners are currently supported

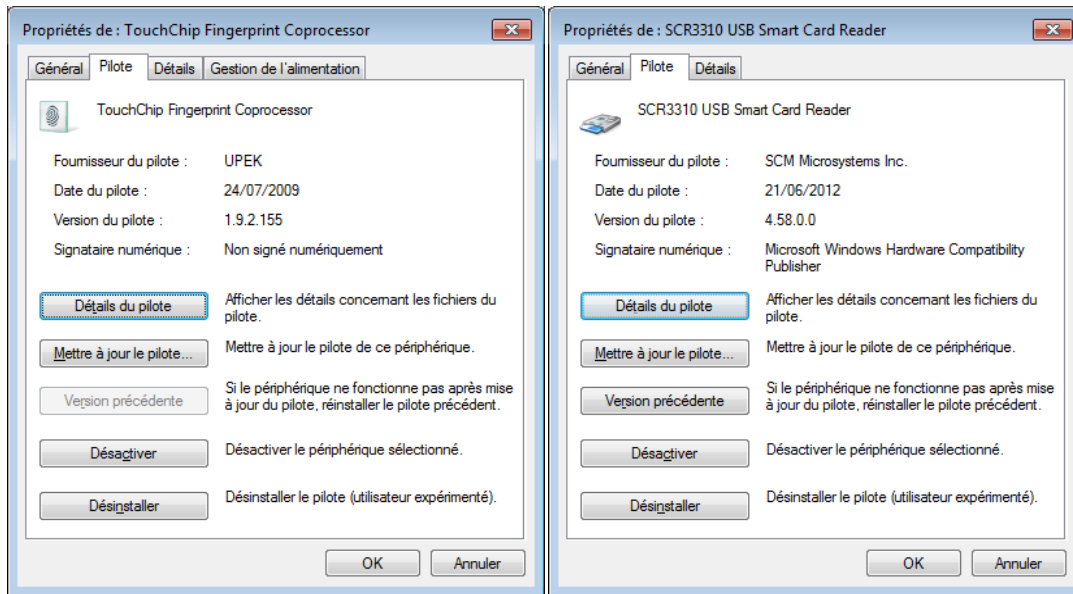
| Vendors | Models | Technology |
|--------------------|---|---------------|
| CrossMatch | Verifier 300 LC, 300 LC 2.0, 310, 310 LC Optical | Optical |
| Dakty | Naos-1 | Optical |
| DigitalPersona | U.are.U 4000B, U.are.U 4500 | Optical |
| Futronic | FS50, FS80, FS88, FS90 | Optical |
| Orcanthus | Certis Image, Certis Bio, Biothetic | Thermal swipe |
| Precise Biometrics | Precise 200 Series | Capacitive |
| Sagem | MorphoSmart MSO200, MSO201, MSO300, MSO301, MSO350, MSO351 | Optical |
| SecuGen | Hamster series (All SecuGen USB readers based on FDU02, FDU03, FDU04 and SDU03 sensors) | Optical |
| Suprema | SFR200, SFR300-S, SFR300-S (Ver.2), SFR400, BioMini | Optical |
| Upek | <ul style="list-style-type: none"> - Intelligent readers based on the following chipsets: TCD21 (TFM), TCD41, TCD42, TCD50A, TCD50D. This includes EIKON, EIKON II and EIKON-To-Go external readers. - Sensor-only readers based on the following sensors: TCS4B, TCS4C, TCS5B, TCS4K - Area sensor readers: TCRU (using ST9 controller), TCEFB module (using Cypress controller CY764215), EIKON Touch (using STM32 controller) | Capacitive |
| Zvetco | P5500, P6000, P6500 | Optical |

9.2 Zvetco P6500 reader

The drivers shall be installed manually to be supported by the middleware and the bio module. It means that the automatic driver windows update shall be deactivated to avoid installing the wrong drivers.

Go to Start menu > right click on computer > select "properties" > select "system protection" > Hardware > Peripheric Installation Parameters > Select "never install drivers from Windows Update"

Then, install reader drivers "SCR3xxx_V8.52.exe"
 And the fingerprint coprocessor driver "2.20B_package"



9.3 Enrollment tool

This tool is used for demo to enroll fingers with a simple user interface on Windows.

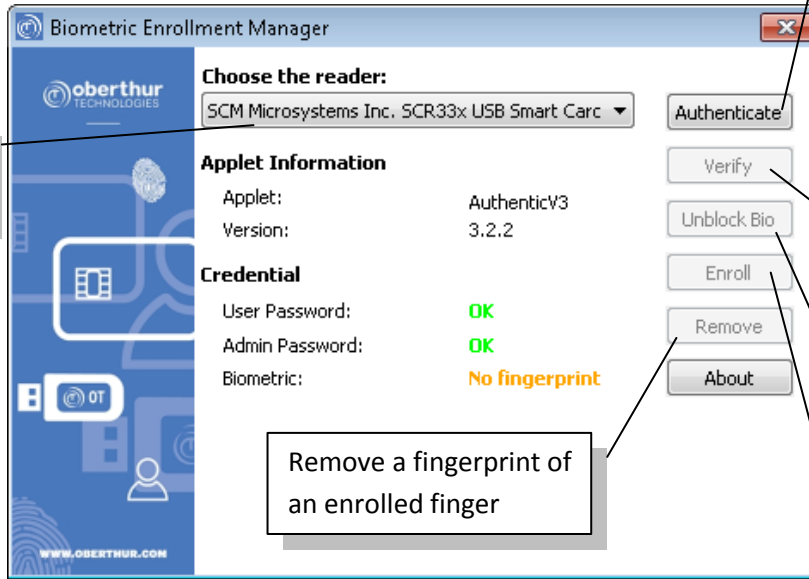
The bio module and the bio reader driver shall be installed before using this tool

Launch the tool from the menu

Start menu > Oberthur Technologies > AWP enrollment tool

It allows to:

- Authenticate to the card prior to any enrollment operations
- Enroll finger(s)
- Verify fingerprint(s)
- Remove fingerprint(s)
- Unblock a bio PIN.



Insert card and select card reader.

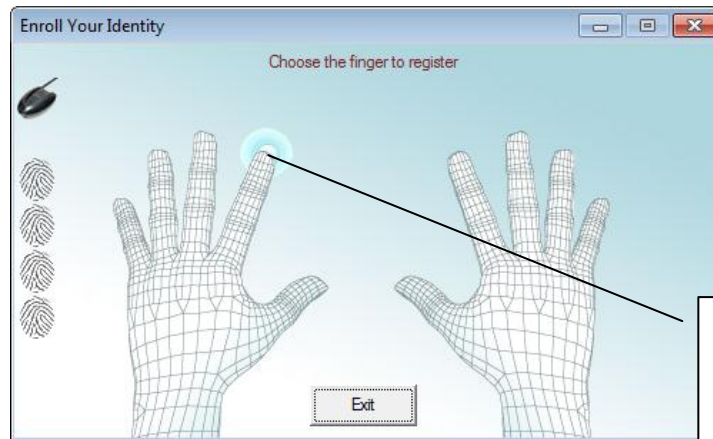
Click to authenticate to the card. A password will be requested. when successful, "verify" button will be enabled

Click to verify the enrolled finger(s)

Click to unblock a blocked bio PIN.

Click to enrol finger(s) with the bio reader.

Remove a fingerprint of an enrolled finger



Enrolment:

- select a finger
- Present it on the reader.

10 Contactless

CSP and minidriver use the windows registry to identify a contact and contactless card.

In contact, the reader returns the card ATR. But in contactless, the reader uses the card ATS to build and return his own ATS. As a consequence, the value may change depending on the reader model and drivers.

To support contactless cards with CSP and minidriver, the windows registry shall be updated manually, case by case.

The ATR value (the ATS actually) can be retrieved with this command “certutil –scinfo”

The ATR mask shall have the same length than the ATR value.

Data in red shall be customised depending on the CSP/minidriver and ATR values

10.1 Add contactless cards with CSP

| OS | Configuration file location |
|---------|---|
| 32 bits | <p>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Oberthur Technologies CTL]</p> <p>"ATR"=hex:3b,00,00,00,00,00,31,80,71,8e,64,77,e3,00,00,00,90,00</p> <p>"ATRMask"=hex:ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff</p> <p>"Crypto Provider"="Oberthur Card Systems Cryptographic Provider"</p> |
| 64 bits | <p>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Oberthur Technologies CTL]</p> <p>"ATR"=hex:3b,00,00,00,00,00,31,80,71,8e,64,77,e3,00,00,00,90,00</p> <p>"ATRMask"=hex: ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff</p> <p>"Crypto Provider"="Oberthur Card Systems Cryptographic Provider"</p> <p>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards\Oberthur Technologies CTL]</p> <p>"ATR"=hex:3b,00,00,00,00,00,31,80,71,8e,64,77,e3,00,00,00,90,00</p> <p>"ATRMask"=hex: ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff</p> <p>"Crypto Provider"="Oberthur Card Systems Cryptographic Provider"</p> |

10.2 Add contactless cards with minidriver

The dll depends on the applet type: laseccminidriver, authenticv3minidriver or pivminidriver

Note that the dll name for 64 bits has the suffix '64'.

Example: laseccminidriver.dll for 32 bits, laseccminidriver64.dll for 64 bits

11 Commercial applications with AWP

11.1 Introduction

There are plenty of commercial tools which can use cryptographic tokens through the AWP middleware.

The following chapters describe some scenario to setup these tools with AWP and to test some cryptographic features.

11.1 Certutil

This tool manages certificates with the CAPI module.

Here is how keys can be loaded:

1) Update windows registry

The windows registry shall be updated to allow keys import

```
HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Base
Smart Card Crypto
Provider\AllowPrivateExchangeKeyImport=DWORD:0x1
HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Base Smart
Card Crypto
Provider\AllowPrivateSignatureKeyImport=DWORD:0x1
```

2) Use .pfx file

A pfx file is required with certutil.

“certmgr.msc” can be used to export certificates. Make sure private keys are exported.

3) Import keys with certutil

```
certutil -csp "Microsoft Base Smart Card Crypto Provider" -
importpfx {PFXfile}
```

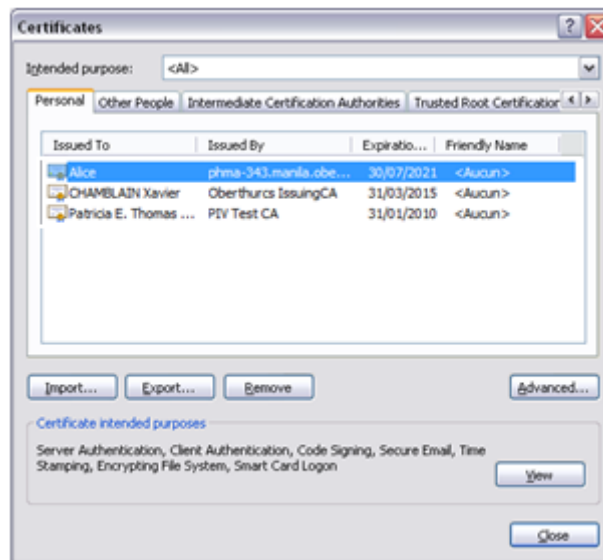
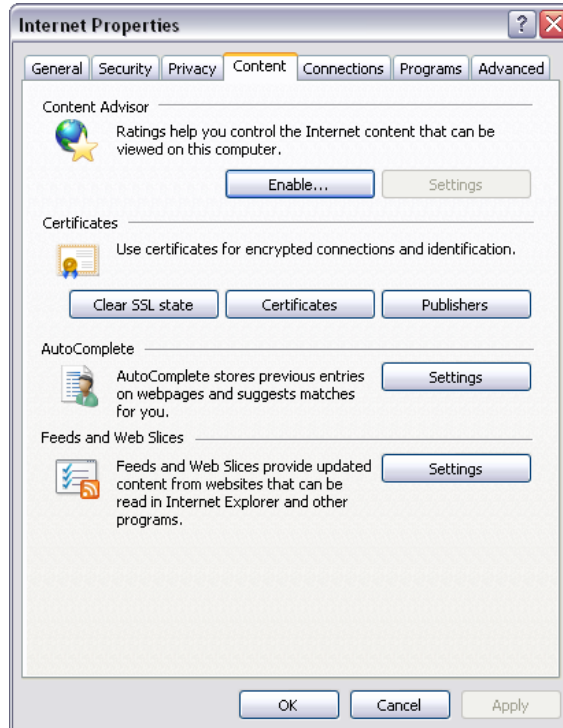
11.2 Internet Explorer

11.2.1 Requirements

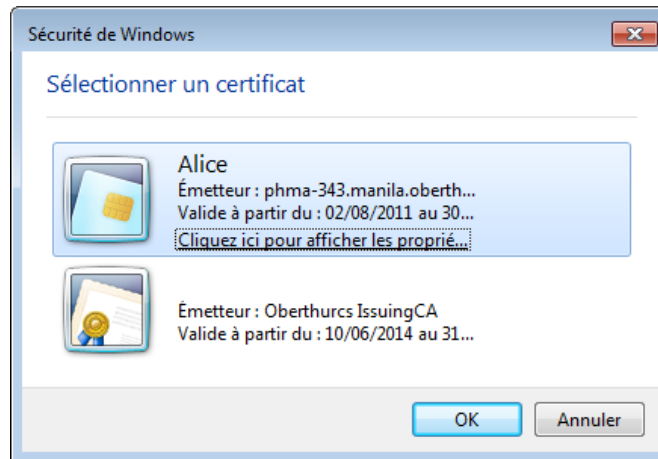
| Description | Version and environment |
|--|--|
| CSP module or Minidriver must be installed | Windows only |
| Latest Internet Explorer must be installed | Window only |
| OT token must be available | Authentic, IAS-ECC or PIV |
| SSL Certificate on the token | Certificate Key Usage should be Key encipherment but Digital Signature is commonly requested |

11.2.2 TLS authentication

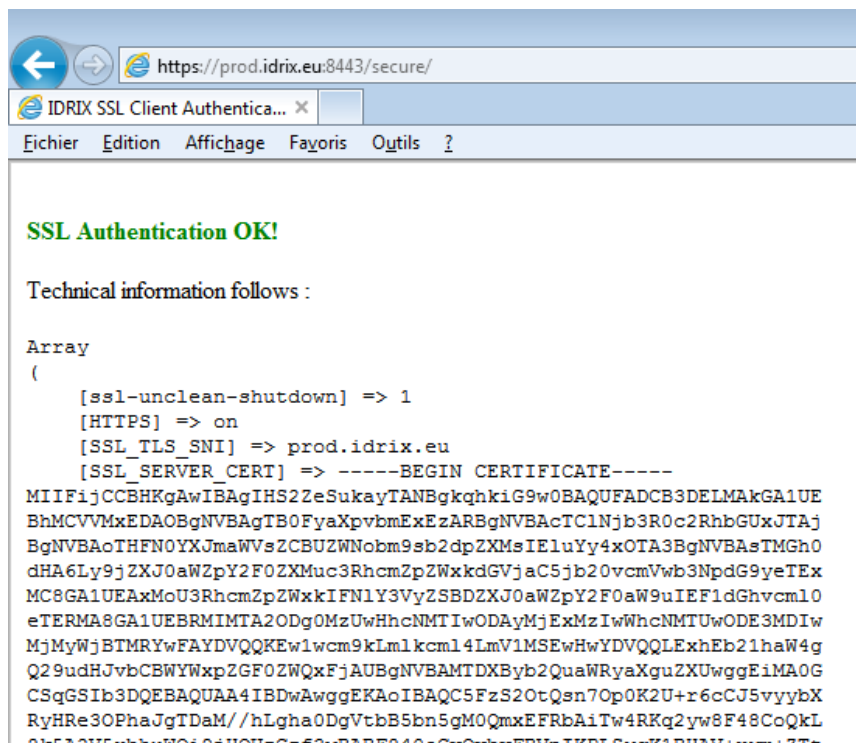
Check that the authentication certificates are loaded in the certificate store:
Internet Options > Content > Certificates:



Start IE and connect to the following website: <https://prod.idrix.eu:8443/secure/>
It will prompt all valid certificates:



Click on OK then enter the password. The certificates will be parsed by the server but not the validity.



11.1 Google Chrome

11.1.1 Requirements

| Description | Version and environment |
|--|-------------------------|
| CSP module or Minidrivers must be installed | Windows |
| PKCS#11 module "libOcsCryptoki.so" must be installed | Linux |
| Latest Internet Explorer must be installed | Windows and Linux |

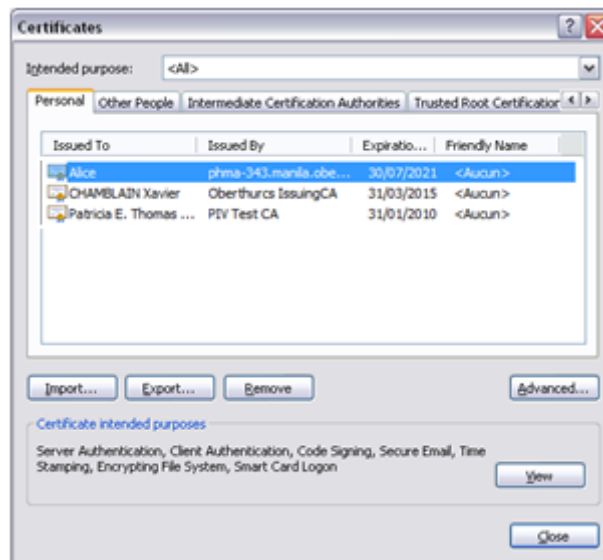
| | |
|------------------------------|--|
| OT token must be available | Authentic, IAS-ECC or PIV |
| SSL Certificate on the token | Certificate Key Usage should be Key encipherment but Digital Signature is commonly requested |

11.1.2 TLS authentication

Check that the authentication certificates are loaded in the certificate store:

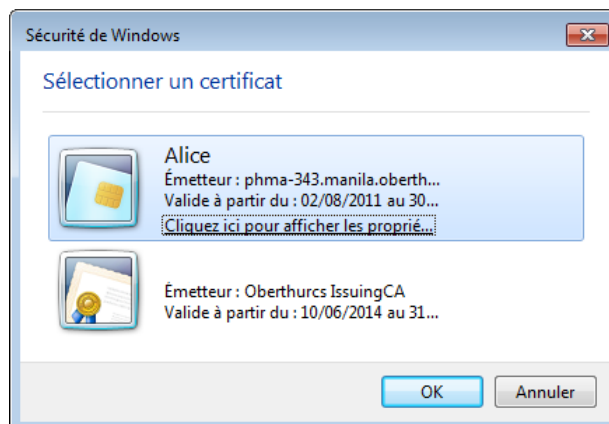
Settings > Advanced settings > HTTPS/SSL:

Select “manage certificates...”



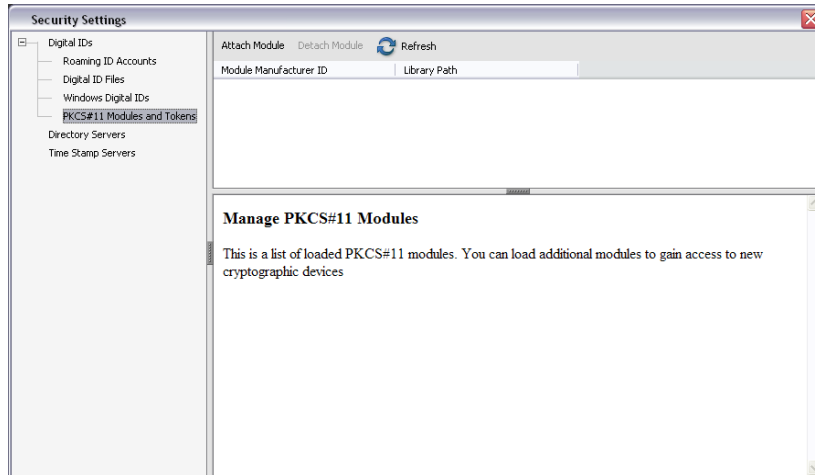
Start Google Chrome and connect to the following website: <https://prod.idrix.eu:8443/secure/>

It will prompt all valid SSL certificates:



Click on OK then enter the password. The certificates will be parsed by the server but not the validity.

In Edit > Protection > Security Settings > PKCS#11 Modules and Tokens



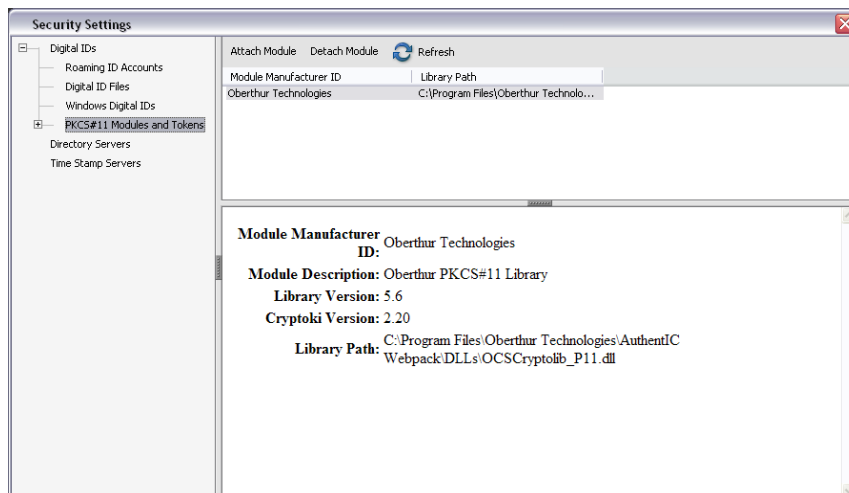
Select PKCS#11 Modules and tokens

Click on “Attach module” and select the PKCS#11 dll from OT which is located in different places according to the platform

| Platform | PKCS#11 Full path |
|----------------|---|
| Windows 32bits | C:\Program Files\Oberthur Technologies\AWP\DLLs\OcsCryptoki.dll |
| Windows 64bits | C:\Program Files (x86)\Oberthur Technologies\AWP\DLLs\OcsCryptoki.dll |
| Linux | /usr/local/AWP/lib/libOcsCryptoki.so |
| MAC OSX | /usr/local/AWP/lib/libOcsCryptok.dylib |

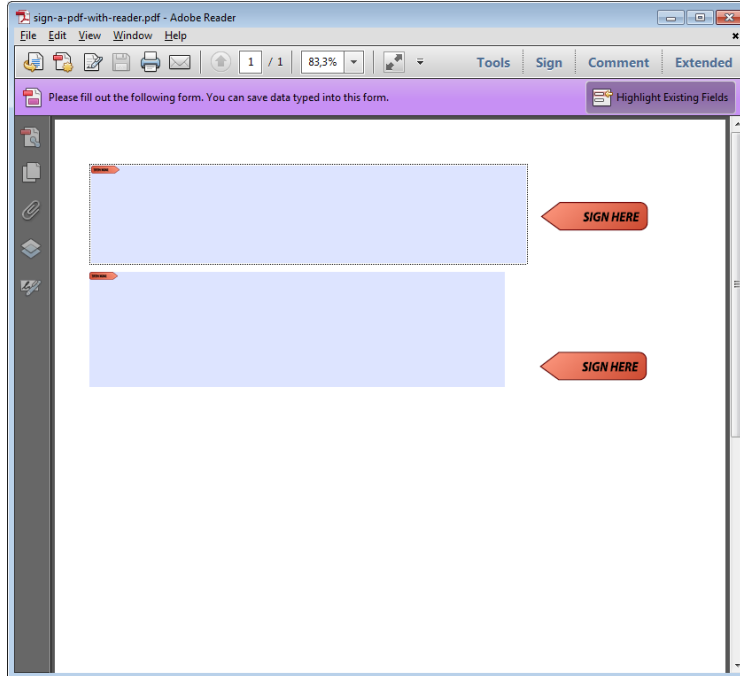
Note: OCSCryptolib_P11.dll is a former dll with the same content than OCSCryptolib.dll. It should not be used anymore.

The PKCS#11 module is now displayed:

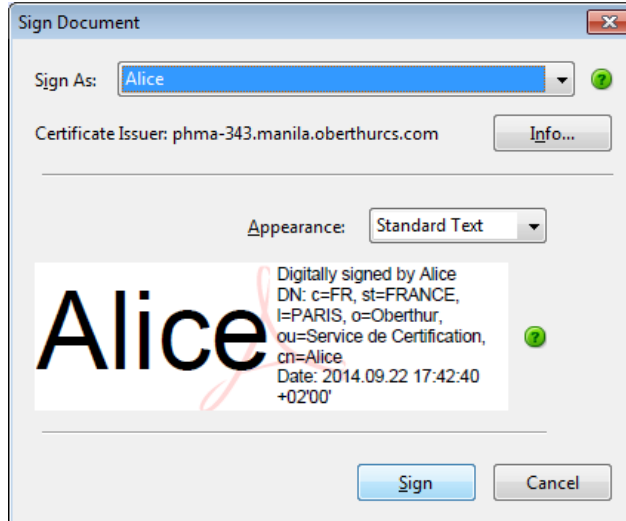


11.3.2 Digital Signature

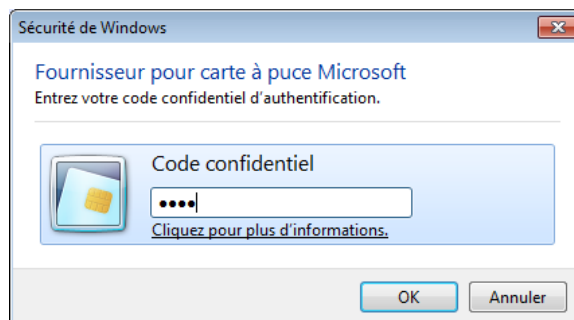
Open the pdf file with the signature field



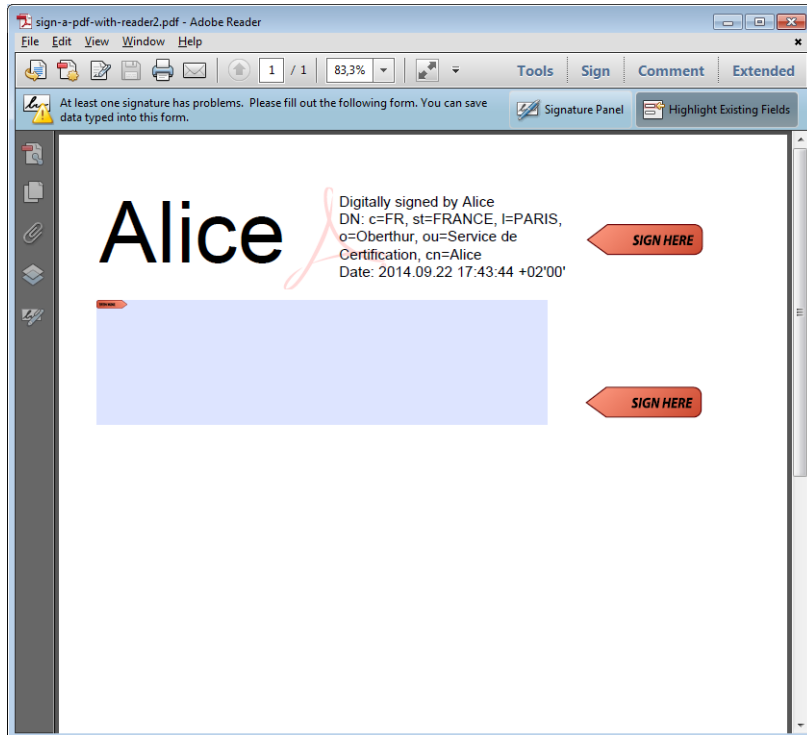
Select the certificate of the person that will sign the document:



Select the output file then enter the password:



The document is signed:



11.4 Microsoft Word

11.4.1 Requirements

| Description | Version and environment |
|--|---------------------------|
| CSP module or Minidivers must be installed | Windows only |
| Microsoft Word must be installed | Until version 2013 |
| OT token must be available | Authentic, IAS-ECC or PIV |
| Digital Signature Certificate on the token | |

11.4.1 Digital Signature

This example is based on Word 2007 only.

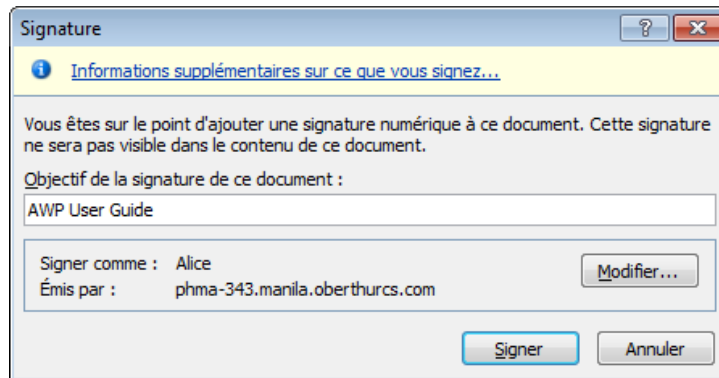
Open the word document to be signed



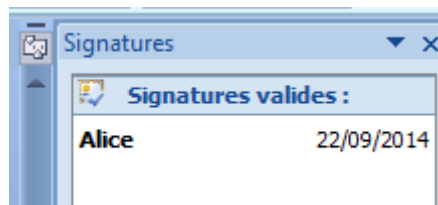
Select the Office button:

Select Prepare > "Add a digital Signature"

It is possible to select certificates from Windows Store. Select one of them and click on sign:



A confirmation pop up is displayed and the document cannot be modified anymore.



On one side, the signature validity can be checked:

11.4.2 Word 2010 & 2013

By default, Office 2010 will use SHA1 for the digital signature.

It is possible to select another hash algorithm by updating the Windows registry as follows

| OS | Configuration file location |
|-------------------|--|
| 32 bits & 64 bits | [HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Signatures] "SignatureHashAlg"="sha256" "sha1" (default for 2010) "sha256" "Sha384" "sha512" |





BE READY
TO ACTIVATE
THE OT EFFECT!

LEARN MORE ABOUT OT ON

WWW.OBERTHUR.COM

 TWITTER

 LINKEDIN

DISCOVER THE M WORLD

OUR MAGAZINE AVAILABLE ON

 ANDROID

 IOS TABLETS



All rights of Oberthur Technologies are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

SIEGE SOCIAL (HEADQUARTERS) : 420, rue d'Estienne d'Orves. 92705 COLOMBES Cedex - FRANCE
S.A. AU CAPITAL de 22 310 409,20€- RCS NANTERRE 340 709 534 - TEL. : +33(0)1 55 46 72 00 - FAX : +33(0)1 55 46 72 01