

# AWP 5.2

How to

Version 1.0 – 03/01/2017

WWW.OBERTHUR.COM



# 1 Table of contents

1	TABL	E OF CONTENTS2
2	REVI	SION
3	INTR	ODUCTION6
	3.1	Purpose6
	3.2	References
	3.3	Definitions
	3.1	Software and Hardware requirements7
	3.2	1.1 Card Readers
	3.3	1.1 Operating system7
	3.2	Change log
4	PAC	(AGES9
	4.1	[Windows] Packages list9
	4.1	[MAC] Packages list9
	4.1	[Linux] Packages list9
5	INST	ALL10
	5.1	[Windows] PKCS#11 & CSP10
	5.2	[Windows] Minidrivers10
	5.3	[Linux] PKCS#11
	5.4	[MAC] PKCS#11 & TokenD
6	UNIN	ISTALL13
	6.1	[Windows] PKCS#11 & CSP13
	6.2	[Windows] Minidrivers13
	6.3	[Linux] PKCS#11
	6.4	[MAC] PKCS#11 & TokenD14
7	LOG	ACTIVATION15
	7.1	Context15
	7.2	How to activate logs?15
	7.2	2.1 [Windows] For Applications based on CSP, PKCS#11 or minidriver15
	7.2	2.2 [Linux & MAC] For applications based on PKCS#1115
	7.3	FAQ



8	IDEN	ITITY MANAGER17
	8.1	Introduction17
	8.2	Launch Identity Manager17
	8.	2.1 [Windows] Launch
	8.	2.1 [Linux & MAC] Launch17
	8.3	Information Panel18
	8.4	Change Password Panel19
	8.5	Unblock Password Panel19
	8.6	Erase Token Panel
	8.7	Content Panel
9	BIO	/IETRICS
	9.1	Bio readers21
	9.2	Zvetco P6500 reader21
	9.3	Enrollment tool
10	CON	TACTLESS
	10.1	Add contactless cards with CSP
	10.2	Add contactless cards with minidriver
	-	
11	CON	IMERCIAL APPLICATIONS WITH AWP26
11	CON 11.1	IMERCIAL APPLICATIONS WITH AWP
11	CON 11.1 11.1	IMERCIAL APPLICATIONS WITH AWP
11	CON 11.1 11.1 11.2	IMERCIAL APPLICATIONS WITH AWP
11	CON 11.1 11.1 11.2	IMERCIAL APPLICATIONS WITH AWP26Introduction.26Certutil26Internet Explorer.261.2.1 Requirements26
11	CON 11.1 11.1 11.2 11 11	IMERCIAL APPLICATIONS WITH AWP26Introduction26Certutil26Internet Explorer26I.2.1 Requirements26I.2.2 TLS authentication27
11	CON 11.1 11.1 11.2 11 11.1	IMERCIAL APPLICATIONS WITH AWP       26         Introduction       26         Certutil       26         Internet Explorer       26         I.2.1 Requirements       26         I.2.2 TLS authentication       27         Google Chrome       28
11	CON 11.1 11.1 11.2 12 12 11.1	IMERCIAL APPLICATIONS WITH AWP26Introduction26Certutil26Internet Explorer26I.2.1 Requirements26I.2.2 TLS authentication27Google Chrome28I.11 Requirements28
11	CON 11.1 11.1 11.2 11 11.1 11.1 11.1	IMERCIAL APPLICATIONS WITH AWP26Introduction26Certutil26Internet Explorer26I.2.1 Requirements26I.2.2 TLS authentication27Google Chrome28I.11 Requirements28I.12 TLS authentication29
11	CON 11.1 11.1 11.2 13 11.1 13 11.1 13 11.2	IMERCIAL APPLICATIONS WITH AWP26Introduction.26Certutil26Internet Explorer.261.2.1 Requirements261.2.2 TLS authentication27Google Chrome281.11 Requirements281.12 TLS authentication29Firefox30
11	CON 11.1 11.1 11.2 11 11.1 11 11 11 11 11 11 11 11 11 11 1	IMERCIAL APPLICATIONS WITH AWP26Introduction26Certutil26Internet Explorer26I.2.1 Requirements26I.2.2 TLS authentication27Google Chrome28I.11 Requirements28I.12 TLS authentication29Firefox30I.2.1 Requirements30
11	CON 11.1 11.1 11.2 13 11.1 13 11.1 13 11.2 13 11.2	IMERCIAL APPLICATIONS WITH AWP26Introduction.26Certutil26Internet Explorer261.2.1 Requirements261.2.2 TLS authentication27Google Chrome281.1 Requirements281.1 Requirements281.2 TLS authentication29Firefox301.2.1 Requirements301.2.2 TLS authentication30
11	CON 11.1 11.1 11.2 13 11.1 13 11.2 13 11.2 13 11.3	IMERCIAL APPLICATIONS WITH AWP26Introduction26Certutil26Internet Explorer261.2.1 Requirements261.2.2 TLS authentication27Google Chrome281.1 Requirements281.1.1 Requirements281.1.2 TLS authentication29Firefox301.2.1 Requirements301.2.1 Requirements301.2.1 Requirements301.2.2 TLS authentication301.2.1 Requirements301.2.2 TLS authentication301.2.3 TLS authentication301.2.4 Requirements301.2.5 TLS authentication301.2.6 TLS authentication301.2.7 TLS authentication303030Adobe Reader31
11	CON 11.1 11.1 11.2 13 11.1 13 11.1 13 11.2 13 11.3 13	IMERCIAL APPLICATIONS WITH AWP26Introduction26Certutil26Internet Explorer261.2.1 Requirements261.2.2 TLS authentication27Google Chrome281.1 Requirements281.1.1 Requirements281.1.2 TLS authentication29Firefox301.2.1 Requirements301.2.2 TLS authentication301.3.1 Requirements31
11	CON 11.1 11.1 11.2 13 11.1 13 11.2 13 11.2 13 11.2 13 11.3 13 13 14 15 15 15 15 15 15 15 15 15 15	IMERCIAL APPLICATIONS WITH AWP26Introduction.26Certutil26Internet Explorer.261.2.1 Requirements261.2.2 TLS authentication27Google Chrome281.1.1 Requirements281.1.2 TLS authentication29Firefox301.2.1 Requirements301.2.2 TLS authentication301.2.1 Requirements301.2.2 TLS authentication301.2.1 Requirements301.2.2 TLS authentication301.2.1 Requirements301.2.2 TLS authentication301.3.1 Requirements311.3.1 Requirements311.3.2 Digital Signature33
11	CON 11.1 11.1 11.2 13 11.1 13 11.1 13 11.3 13 11.3	IMERCIAL APPLICATIONS WITH AWP26Introduction26Certutil26Internet Explorer261.2.1 Requirements261.2.2 TLS authentication27Google Chrome281.1 Requirements281.1 Requirements29Firefox301.2 TLS authentication301.2.1 Requirements301.2.2 TLS authentication311.3.1 Requirements311.3.1 Requirements311.3.2 Digital Signature33Microsoft Word34



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	ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-
	Token Interface Standard	<u>20/pkcs-11v2-20.pdf</u>
[2]	PKCS #15 v1.1: Cryptographic	ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-15/pkcs-15v1-
	Token Information Syntax	<u>1tc2.pdf</u>
	Standard	
[3]	IAS ECC Technical Specification –	http://www.acsiel.fr/iso_album/ias_ecc_v1_0_1_fr.pdf
	Revision 1.01	
[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	
ΑΡΙ	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	EXEcutable file	
GUID	Globally Unique Identifier	
IAS - ECC	Identification-Authentification-Signature – European Citizen Card	
MD	MiniDriver	
MSIE	MicroSoft Internet Explorer	
KSP	Key Storage Provider	
ОР	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%2 08.1&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> <li>Default certificate management (logon)</li> <li>Event log under windows: <ul> <li>PIN and PUK changes</li> <li>Wrong PIN and PUK entered</li> <li>PIN and PUK expired</li> <li>PIN and PUK locked</li> </ul> </li> </ul>
From 5.0 SR2 to 5.1 SR1	<ul> <li>Major features:</li> <li>Biometry for Linux,</li> <li>Support of PIV v2.3.5 applet</li> <li>Support ID-One Cosmo V8</li> <li>Support MAC OX 10.9</li> <li>Minor features:</li> <li>AWP Manager : Manage the "P7" extension for the certificate import</li> <li>XML file and registry : Add Sergas ATR</li> <li>Support of ID-ONE MSFT</li> <li>Support opacity on Cosmo V8 (this option is activated by default)</li> <li>AWP Manager : DLL versions are dynamically retrieved and displayed in the "about" dialog box</li> <li>Set the last generated key pair as default container</li> <li>Credential provider for smart card login</li> <li>Support multi ADF in IAS minidriver (read :all ADF, write only the default one)</li> <li>AWP Manager optionally reads the PIN policy on AuthenticV3 (P11, CSP, minidriver)</li> <li>UAC management during install under Windows</li> <li>It's not possible anymore to import the same certificate twice</li> <li>PKCS#11 : Proprietary API has been developed to retrieve the remaining tries (PIN / PUK)</li> <li>Support new return for get version on AuthentICV3 (3 bytes instead of 2 bytes)</li> </ul>
From 5.1 SR1 to 5.2 SR1	<ul> <li>Support of PIV 2.4.0</li> <li>Support of AuthenticV3.2.5</li> <li>Support of Cosmo V8.1</li> <li>RSA_PSS padding support on AuthentiV3 and PIV (P11 / Minidriver, off card version only)</li> <li>Support of new bio CHV manager</li> <li>Support Opacity V2.0 for PIV 2.4</li> <li>Support Widows 10</li> <li>Support MAC OSX until 10.12</li> <li>Support of certificate online and compressed certificates on PIV</li> <li>Support of pairing code on PIV</li> <li>Elliptic curves on IAS</li> <li>Include Italian translation</li> <li>Enforced PIN Policy rules</li> </ul>



# 4 Packages

# 4.1 [Windows] Packages list

	Package name		Windows		Cryptographic API		Synchroniser Identity M		Manager
		32-	64-	PKCS11	CSP	Minidrivers		ADMIN	USER
		bit	bit						
	AWP 5.2.0 SR2 64-bit.msi		Х	Х		All	Х		Х
	AWP 5.2.0 SR2.msi	Х		Х		All	Х		Х
	AWP 5.2.0 SR2 Admin 64-bit.msi		Х	Х		All	х	Х	
	AWP 5.2.0 SR2 Admin.msi	Х		Х		All	х	Х	
1	AWP 5.2.0 SR2 CSP 64-bit.msi		Х	Х	Х		х		Х
CS1	AWP 5.2.0 SR2 CSP Admin 64-bit.msi		Х	Х	Х		х	Х	
۱PK	AWP 5.2.0 SR2 CSP Admin.msi	Х		Х	Х		Х	Х	
Wit	AWP 5.2.0 SR2 CSP.msi	Х		Х	Х		Х		Х
-	AWP 5.2.0 SR2 P11 Only 64-bit.msi		Х	Х					Х
	AWP 5.2.0 SR2 P11 Only Admin 64- bit.msi		Х	Х					Х
	AWP 5.2.0 SR2 P11 Only Admin.msi	Х		Х					Х
	AWP 5.2.0 SR2 P11 Only.msi	Х		х				х	
	AuthentICV3Minidriver-1.4.4 64-bit.msi		Х			AuthenticV3			
	AuthentICV3Minidriver-1.4.4.msi	Х				AuthenticV3			
١						IAS-ECC v1 &			
uo :	lasEccMinidriver-2.4.3 64-bit.msi		Х			v2			
rivers	lasEccMinidriver-2.4.3.msi	х				IAS-ECC v1 & v2			
linid	PivMinidriver-1.3.4 64-bit.msi		Х			PIV <= 2.3.5			
Σ	PivMinidriver-1.3.4.msi	х				PIV <= 2.3.5			
	PivCivMinidriver-1.0.4 64-bit.msi		Х			PIV >= 2.4.0			
	PivCivMinidriver-1.0.4.msi	х				PIV >= 2.4.0			

# 4.1[MAC] Packages list

Package name	Cryptogr	aphic API	Identity Manager		
	PKCS11	Token D	ADMIN	USER	
AWP_5.2.0_SR2.dmg	Х	Х		Х	
AWP_5.2.0_SR2_Admin.dmg	Х	Х	Х		

# 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): <u>http://technet.microsoft.com/fr-fr/library/ff404287(v=ws.10).aspx</u> 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.



Device Installation Settings
Do you want Windows to download driver software and realistic icons for your devices?
Yes, do this automatically (recommended)
No, let me choose what to do
Why should I have Windows do this automatically?
Save Changes Cancel

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.

Administrateur : C:\WINDOWS\system32\cmd.exe	- • ×
Nom publié : oem103.inf Fournisseur de packages de pilotes : Microsoft Classe : Cartes à puce Version et date du pilote : 09/03/2006 1.0.0.3 Nom du signataire : Microsoft Windows Hardware Compatibi sher	ility Publi
Nom publié : oem104.inf Fournisseur de packages de pilotes : Oberthur Technologies Classe : Cartes à puce Version et date du pilote : 08/21/2013 1.2.37.0 Nom du signataire :	
Nom publié : oem105.inf Fournisseur de packages de pilotes : Oberthur Technologies Classe : Cartes à purc Version et date du pilote : 02/05/2014 1.3.9.0 Nom du signataire :	
Nom publié : oem106.inf Fournisseur de packages de pilotes : KEOLABS Classe : NomadLABWinUSBClass Version et date du pilote : 10/16/2013 6.0.6001.18000 Nom du signataire :	THE STREET



🝰 Device Manager File Action View Help 🦛 🔿 | 🔐 | 🚺 🔜 🐼 🖌 📇 W7\_32\_P11\_MD Batteries b 🜉 Computer Disk drives Display adapters DVD/CD-ROM drives Human Interface Devices DE ATA/ATAPI controllers Keyboards Mice and other pointing devices Monitors Network adapters Ports (COM & LPT) 📲 Smart card readers Sound, video and game controllers System devices 🏺 Universal Serial Bus controllers

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.\*

# 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

Te 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>

Ceate the folder 'OTLogs': # sudo mkdir /usr/OTLogs

Set access conditions for writing: # sudo chown –R *username* OTLogs (use # sudo chgrp users OTLogs (set # chmod 775 OTLogs (set # sudo adduser *username* users (add

(use your username)(set the rights to users group)(set writing access)(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> <li>For 64 bits OS, check that the 2 xml files have been updated</li> </ul>
	<ul> <li>Check the consistency of the xml file with a parser, like Internet Explorer.</li> </ul>
	<ul> <li>Restart the application that must be logged.</li> <li>Check that it is not running in background. If necessary, reboot the system.</li> </ul>
Some logs are missing	The log folder may be not available for writing, especially when the user session is not established. Change the log folder with this one:
	C:\Users\%username%\AppData\LocalLow\OTlogs\
	Where %usename% is the user login



# 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		$\mathbf{\nabla}$
Change PUK		$\mathbf{N}$
Init Token		$\mathbf{\overline{A}}$
Generate Key		$\mathbf{N}$
Import Key		$\mathbf{N}$
Edit Label		$\mathbf{N}$
Delete Object		$\mathbf{N}$
Set Default Container		$\checkmark$

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"

0 ·	Q Search	
	iii Recent Apps	
	1	6
9		
	Identity	Adobe Reader

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
In 'Parameter' menu: - Change the AWP manager language (not the middleware)	WP Identity Mrager meters ? Coberthur TECHNOLOGIES CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODER CODE	Information Change Password Unblock Password Erase Token Choose the reader: OMNIKEY CardMan 3x21 0 Security device information: Label: OT AWP Model: Cosmo v8.1 Applet: 3.25 Manufacture: Oberthur Technologies Serial Number: 00000000A800283D Free Memory: 94920 bytes State: Initialized Credential Information: PIN: OK PUK: OK	Content 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
- Change PIN timeout	TVW.OBERTHUR.COM		Status of PIN & PUK: OK or blocked



# 8.4 Change Password Panel

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

AWP Identity Manager Parameters ?	Information Change Password Unblock 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	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.

arameters ?	Information Change Password Unblock Password Erase Token Content	
Oberthur     TECHNOLOGIES	User Password (PIN)	
	Please insert the administrator password correctly otherwise the smartcard could be bi	<sup>°°</sup> Enter the PUK
0	Admin Password	
E © 0T	New Password	Enter the new PIN with
	New Password confirmation	respect to the PIN policy
		Unblock
		Click to unblock
		the PIN
www.oberthur.com		



## 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.

AWP Identity Manager		
Parameters ?	Information Change Password Linblock Password Frase Token Content	
<b>Oberthur</b>	Please insert the administrator password correctly otherwise the smartcard could be block	ked.
—	Admin Password	Enter the PUK
<b>~</b>	New smartcard information	
0 (	Token Label	Enter the new
💼 💿 от	New Password	token label
	New Password confirmation	
		Enter and confirm
		the new PIN
WWW.OBERTHUR.COM		Erase Click to erase
		the token

## 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, Biothentic	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> <li>Intelligent readers based on the following chipsets: TCD21 (TFM), TCD41, TCD42, TCD50A, TCD50D. This includes EIKON, EIKON II and EIKON-To-Go external readers.</li> <li>Sensor-only readers based on the following sensors: TCS4B, TCS4C, TCS5B, TCS4K</li> <li>Area sensor readers: TCRU (using ST9 controller), TCEFB module (using Cypress controller CY764215), EIKON Touch (using STM32 controller)</li> </ul>	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"



Propriétés de : TouchChip Fingerprint Coprocessor	Propriétés de : SCR3310 USB Smart Card Reader
Général Pilote Détails Gestion de l'alimentation	Général Pilote Détails
TouchChip Fingerprint Coprocessor	SCR3310 USB Smart Card Reader
Fournisseur du pilote : UPEK	Fournisseur du pilote : SCM Microsystems Inc.
Date du pilote : 24/07/2009	Date du pilote : 21/06/2012
Version du pilote : 1.9.2.155	Version du pilote : 4.58.0.0
Signataire numérique : Non signé numériquement	Signataire numérique : Microsoft Windows Hardware Compatibility Publisher
Détails du pilote Afficher les détails concernant les fichiers du pilote.	Détails du pilote Afficher les détails concernant les fichiers du pilote.
Mettre à jour le pilote Mettre à jour le pilote de ce périphérique.	Mettre à jour le pilote Mettre à jour le pilote de ce périphérique.
Version précédente Si le périphérique ne fonctionne pas après mise à jour du pilote, réinstaller le pilote précédent.	Version précédente         Si le périphérique ne fonctionne pas après mise à jour du pilote, réinstaller le pilote précédent.
Désagtiver Désactiver le périphérique sélectionné.	Désactiver Désactiver le périphérique sélectionné.
Désinstaller Désinstaller le pilote (utilisateur expérimenté).	Désinstaller le pilote (utilisateur expérimenté).
OK Annuler	OK Annuler

## 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.









# 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	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Oberth ur Technologies CTL]
	"ATR"=hex:3b,00,00,00,00,00,31,80,71,8e,64,77,e3,00,00,00,90,00
	"ATRMask"=hex:ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,
	"Crypto Provider"="Oberthur Card Systems Cryptographic Provider"
64 bits	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Oberth ur Technologies CTL]
	"ATR"=hex:3b,00,00,00,00,00,31,80,71,8e,64,77,e3,00,00,00,90,00
	"ATRMask"=hex: ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,
	"Crypto Provider"="Oberthur Card Systems Cryptographic Provider"
	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\Sm artCards\Oberthur Technologies CTL]
	"ATR"=hex:3b,00,00,00,00,00,31,80,71,8e,64,77,e3,00,00,00,90,00
	"ATRMask"=hex: ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,
	"Crypto Provider"="Oberthur Card Systems Cryptographic Provider"

## **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



OS	Configuration file location
32 bits	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Oberthur Technologies CTL]
	@=""
	"ATR"=hex:3b,00,00,00,81,31,fe,45,80,f9,a0,00,00,00,77,01,00,70,0a,90,00,00
	"ATRMask"=hex:ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,
	"Crypto Provider"="Microsoft Base Smart Card Crypto Provider"
	"Smart Card Key Storage Provider"="Microsoft Smart Card Key Storage Provider"
	"80000001"="AuthentICV3MiniDriver.dll"
	"AuthenticationMode"=dword:0000001
	"EnableBiometric"=dword:0000001
	"EnablePinPad"=dword:00000001
64 bits	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Oberthur Technologies CTL]
	@=""
	"ATR"=hex:3b,00,00,00,81,31,fe,45,80,f9,a0,00,00,00,77,01,00,70,0a,90,00,00
	"ATRMask"=hex:ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,
	"Crypto Provider"="Microsoft Base Smart Card Crypto Provider"
	"Smart Card Key Storage Provider"="Microsoft Smart Card Key Storage Provider"
	"80000001"="AuthentICV3MiniDriver64.dll"
	"AuthenticationMode"=dword:0000001
	"EnableBiometric"=dword:0000001
	"EnablePinPad"=dword:00000001
	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\Smart Cards\Oberthur Technologies CTL]
	@=""
	"ATR"=hex:3b,00,00,00,81,31,fe,45,80,f9,a0,00,00,00,77,01,00,70,0a,90,00,00
	"ATRMask"=hex:ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,
	"Crypto Provider"="Microsoft Base Smart Card Crypto Provider"
	"Smart Card Key Storage Provider"="Microsoft Smart Card Key Storage Provider"
	"80000001"="AuthentICV3MiniDriver.dll"
	"AuthenticationMode"=dword:0000001
	"EnableBiometric"=dword:0000001
	"EnablePinPad"=dword:00000001



# **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 Minidrivers 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:

Internet Properties				? 🔰
General Security Privacy	Content	Connectio	ns Progra	ms Advanced
Content Advisor				
Ratings help you viewed on this co	control th mputer.	e Internet o	ontent that	t can be
	Ena	ble	Se	ttings
Cortificator				
Use certificates f	or encryp	ed connect:	ions and ide	entification.
Clear SSL state	Certi	ficates	Pub	olishers
AutoComplete sto on webpages and for you.	ores previ d suggest:	ous entries ; matches	Se	ttings
Feeds and Web Slices				
Feeds and Web S content from wet read in Internet for programs	5lices prov bsites that Explorer a	ide updatec : can be nd other	Se	ttings
	0		Cancel	Apply
rtificates				3
tended purpose: <ai></ai>				
Personal Other People Intermedia	ite Certifica	tion Authoritie	rs Trusted P	Root Certification
Irond To Irond	D.	Evel	atio Erie	and Hame
Alce phma-	oy 343.manila.	obe 30/	07/2021 <	Augun>
CHAMBLAIN Xavier Oberth Patricia E. Thomas PIV Ter	st CA	gCA 31/ 31/	03/2015 < 01/2010 <	Aucun> Aucun>
Import Export	Remove			Advanced
Certificate intended purposes				
Server Authentication, Client Autheni Stamping, Encrypting File System, Sm	tication, Co Nart Card Lo	de Signing, Se gon	cure Email, T	jime Vjew
				Chris

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

← → Ø https://prod.idrix.eu:8443/secure/						
@ IDRIX SSL Client Authentica ×						
<u>Fichier</u> <u>Edition</u> Affic <u>h</u> age Fa <u>v</u> oris O <u>u</u> tils <u>?</u>						
SSL Authentication OK!						
Technical information follows :						
7						
Array						
[ss]-unclean-shutdown] => 1						
[HTTPS] => on						
[SSL TLS SNI] => prod.idrix.eu						
[SSL_SERVER_CERT] =>BEGIN CERTIFICATE						
MIIFijCCBHKgAwIBAgIHS2ZeSukayTANBgkqhkiG9w0BAQUFADCB3DELMAkGA1UE						
BhMCVVMxEDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTC1Njb3R0c2RhbGUxJTAj						
BgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIE1uYy4xOTA3BgNVBAsTMGh0						
dHA6Ly9jZXJ0aWZpY2F0ZXMuc3RhcmZpZWxkdGVjaC5jb20vcmVwb3NpdG9yeTEx						
MC8GA1UEAxMoU3RhcmZpZWxkIFN1Y3VyZSBDZXJ0aWZpY2F0aW9uIEF1dGhvcm10						
eTERMA8GA1UEBRMIMTA2ODg0MzUwHhcNMTIwODAyMjExMzIwWhcNMTUwODE3MDIw						
MjMyWjBTMRYwFAYDVQQKEw1wcm9kLm1kcm14LmV1MSEwHwYDVQQLExhEb21haW4g						
Q29udHJvbCBWYWxpZGF0ZWQxFjAUBgNVBAMTDXByb2QuaWRyaXguZXUwggEiMA0G						
CSQGSIDSUQEBAQUAA4IBUWAWggEKAOIBAQCSFZSZOTQSn/Op0KZU+r6CCJ5VYYDX						
Cheraoteneogioan//hughaobg/cbbbbhbgM0QMXErKDAIIW4KKQ2yW6f46C0QKL						

# 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..."

ertificate	в						?
ntended p	urpose:	<ai></ai>					~
Personal	Other Peo	ple Int	ermediate Certification	Authorities	Trus	ted Root Certificatio	(4)
Issued	То		Issued By	Expirati	o	Friendly Name	
Alco			phma-343.manila.ob	e 30/07/	2021	<aucun></aucun>	
ПОЧ	MBLAIN X	wier	Oberthurcs IssuingC	A 31/03/	2015	<aucun></aucun>	-1
Patr	icia E. Tho	nas	PIV Test CA	31/01/	2010	<aucun></aucun>	
L							
Import	E	port	Remove			Advan	ced
Certificate	e intended	purposes					
Server Au Stamping,	thenticatio Encryptin	n, Client File Sys	Authentication, Code tem, Smart Card Logo	Signing, Secu n	re Em	al, Time	
							ice.

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

Sécurité de Windows			
Sélectionne	er un certificat		
	Alice Émetteur : phma-343.manila.oberth Valide à partir du : 02/08/2011 au 30 Cliquez ici pour afficher les proprié		
Émetteur : Oberthurcs IssuingCA Valide à partir du : 10/06/2014 au 31			
	OK	ler	

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





#### 11.2 Firefox

#### 11.2.1 Requirements

PKCS#11 module must be installed.

Latest Mozilla Firefox

Description	Version and environment	
PKCS#11 must be installed	Windows, Linux, MAC OS	
Latest Mozilla Firefox must be installed	Windows, Linux, MAC OS	
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

Add the PKCS#11 OT module from Firefox menu:

In Menu > module > extensions > "Install a module from a file"

Select the extension in AWP folder:

"C:\Program Files (x86)\Oberthur

Technologies\AWP\Firefox\Extension\PKCS11\_Firefox@oberthur.com.xpi" (64-bit) Restart the application then connect to <u>https://prod.idrix.eu:8443/secure/</u>



#### Enter the password:



The authentication must be successful:

IDRIX SSL Client Authentication × +				
A https://prod.idrix.eu:8443/secure/				
Les plus visités [] IDRIX SSL Client Authe				

SSL Authentication OK!

Technical information follows :
Array
(
[HTTPS] => on
[SSL TLS SNI] => prod.idrix.eu
[SSL SERVER CERT] =>BEGIN CERTIFICATE
MIIFijCCBHKgAwIBAgIHS2ZeSukayTANBgkghkiG9w0BAQUFADCB3DELMAkGA1UE
BhMCVVMxEDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTC1Njb3R0c2RhbGUxJTAj
BgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xOTA3BgNVBAsTMGh0
dHA6Ly9jZXJ0aWZpY2F0ZXMuc3RhcmZpZWxkdGVjaC5jb20vcmVwb3NpdG9yeTEx
MC8GA1UEAxMoU3RhcmZpZWxkIFN1Y3VyZSBDZXJ0aWZpY2F0aW9uIEF1dGhvcm10
eTERMA8GA1UEBRMIMTA2ODg0MzUwHhcNMTIwODAyMjExMzIwWhcNMTUwODE3MDIw
MjMyWjBTMRYwFAYDVQQKEw1wcm9kLm1kcm14LmV1MSEwHwYDVQQLExhEb21haW4g
Q29udHJvbCBWYWxpZGF0ZWQxFjAUBgNVBAMTDXByb2QuaWRyaXguZXUwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5FzS2OtQsn7Op0K2U+r6cCJ5vyybX
RyHRe3OPhaJgTDaM//hLgha0DgVtbB5bn5gM0QmxEFRbAiTw4RKq2yw8F48CoQkL
8k5A2V5xbhuWQi9jHQUzCzf3wBABF840oCvQvbvFBVnIKPLSygK1BHAV+xym+2Tt
OzAJQWRicnZcNcIEaj4lpJVr1wBlSZ3zvKHQALUOvwgHT1+3Sti4aaEoWD0SMjTg
pMM9chfL16MqFoL1/8Kk2L63+e6m2RdiwEDGZNCnKmkHCrJei3Wssak/aRqpaBdk
QWYLGdgCwwQe6Cz1jx47JIxC+1slQKR/oGMDg3fmQffYNnv8ekFuiEWhAgMBAAGj
ggHXMIIB0zAPBgNVHRMBAf8EBTADAQEAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggr
BgEFBQcDAjAOBgNVHQ8BAf8EBAMCBaAwOQYDVR0fBDIwMDAuoCygKoYoaHR0cDov
L2NvbC5zdGFvZml1bGR0ZWNoLmNvbS9zZnMxLTIvLmNvbDBZBgNVHSAEUjBQME4G
C2CGSAGG/W4BBxcBMD8wPQYIKwYBBQUHAqEWMWh0dHA6Ly9jZXJ0aWZpY2F0ZXMu
C3Bhcm2p2WxkdGViaC5ib20vcmVwb3NpdG9ve58wqY0GCCsGA0UFBwEBBIGAMH4w

#### **11.3** Adobe Reader

#### 11.3.1 Requirements

Description	Version and environment
PKCS#11 or CSP or minidrivers must be installed	Windows, Linux, MAC OS
Install Adobe Reader	Version 9, 10 and 11
OT token must be available	Authentic, IAS-ECC or PIV
Digital signature Certificates	
Get a pdf file with a signature field	sign-a-pdf-with-read er.pdf

By default, Adobe Reader is configured to sign only using the CSP or minidriver interface. With the following settings, it is possible to use the PKCS#11 interface.



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

Security Settings		
Security Settings Digital IDs Reaming ID Accounts Digital ID Files Windows Digital IDs RKC\$#11 Modules and Tokens Directory Servers Time Stamp Servers	Attach Module Detach Module 😂 Refresh Module Manufacturer ID Ubrary Path	
	Manage PKCS#11 Modules This is a list of loaded PKCS#11 modules. You can load additional modules to gain access to new cryptographic devices	<

#### 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:

Security Settings		>
Digital IDs     Roaming ID Accounts     Digital ID Files     Windows Digital IDs     PKCS#11 Modules and Tokens     Directory Servers	Attach Module Detach Module Refresh Module Manufacturer ID Library Path Oberthur Technologies C:\Program Files\Oberthur Technolo	
Time Stamp Servers	Module Manufacturer D: Oberthur Technologies ID: Module Description: Oberthur PKCS#11 Library	4
	Library Version: 5.6 Cryptoki Version: 2.20 C:Program Files:Oberthur Technologies\AuthentIC Library Path: Webpack:DLLs:OCSCryptolib_P11.dll	



#### 11.3.2 Digital Signature

Open the pdf file with the signature field



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

Sign Document		X
Sign As: Alice	•	(?)
Certificate Issuer: phma-3	343.manila.oberthurcs.com	
	Appearance: Standard Text	
Alice	DN: c=FR, st=FRANCE, I=PARIS, o=Oberthur, ou=Service de Certification, cn=Alice Date: 2014.09.22 17:42:40 +02'00'	
	<u>Sign</u> Cance	I

Select the output file then enter the password:

Sécurité de Windows	
Fournisseur pour carte à puce Microsoft Entrez votre code confidentiel d'authentification.	
Code confidentiel  Code confidentiel  Cliquez pour plus d'informations.	
OK Annuler	



The document is signed:



## **11.4** Microsoft Word

#### **11.4.1 Requirements**

Description	Version and environment
CSP module or Minidrivers 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

<b>]</b> •) •
Accueil
X Coupe

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:



Signature	? 💌
Informations supplémentaires sur ce que vous si	ignez
Vous êtes sur le point d'ajouter une signature numériq ne sera pas visible dans le contenu de ce document.	ue à ce document. Cette signature
Objectif de la signature de ce document :	
AWP User Guide	
Signer comme : Alice Émis par : phma-343.manila.oberthurcs.com	Modifier
	Signer Annuler

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\Signatu res]
	"SignatureHashAlg"="sha256"
	"sha1" (default for 2010)
	"sha256"
	"Sha384"
	"sha512"







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