

Aruba Key

V2

ARUBA PEC

ACTALIS

1 Index

1 Index 2
2 Information on document 3
2.1 Object of document 3
3 Device features 3
3.1 Prerequisites 3
4 Installation of smart card 4
5 Startup of Aruba Key 5
6 Sign a file in CAdES format (p7m) 6
6.1 Sign multiple files in CAdES format (P7M) 8
6.2 Enveloped Signature and Multiple Signature feature 11
7 Sign a PDF file digitally 13
7.1 Sign multiple PDF files digitally 16
8 Adding timestamps 19
9 Verification of signed files 21
10 Verification of timestamps 24
11 Verification of Timestamps in .TSD format 27
12 Management of smart card 28
12.1 Change pin code 28
12.2 Unlock PIN 29
12.3 Change PUK code 30
12.4 Smart card information 31
12.5 Smart card management error codes 32
13 Auto-diagnosis of the Aruba Key device 33
14 "Import" certificate 35
15 File encryption 37
16 File decryption 40
17 Options 42
17.1 Proxy settings 42
17.2 Language settings 44
18 Display of certificates on FireFox Portable. 46
19 Uploading process of ACTALIS certificate 48

Copyright © Aruba Pec S.p.A. - All Rights Reserved

2 Information on document

2.1 Object of document

This document is a quick guide for owners of the Aruba Key in performing the following:

1. Adding Digital Signatures in .P7M format
2. Adding Digital Signatures in .PDF format
3. Adding Timestamps
4. Verification of Digital Signatures in .P7M and .PDF format
5. Verification of Timestamps
6. Pin and Puk management of the smart card found in the Aruba Key

3 Device features

The Aruba Key is an advanced USB device which allows users to always have their Digital Signature and Timestamp at hand. The Aruba Key does not require any Hardware or Software installation, and is always ready to digitally sign and/or timestamp e-documents.

The device, furthermore, can also be used for secure authentication in websites.

3.1 Prerequisites

Here below are the Hardware and Software prerequisites that the workstation to which the Aruba Key will be connected needs to have.

3.1.1 Software

Operating Systems:

- MS Windows XP, Vista, Seven, Server 2003, Server 2008, Win 8, Win 8 PRO, Win 8.1, Win 8.1 PRO (32 and 64 bit)
- Mac Os X Tiger (10.4 - Intel), Leopard (10.5 - Intel), Snow Leopard (10.6 - Intel), Lion (10.7 - Intel), Mountain Lion (10.8 – Intel), Mavericks (10.9 – Intel) (32 and 64 bit)
- Linux Ubuntu 12.0.4 e 12.10, Debian 6.0, Mint 13 e 14 (32 bit)

3.1.2 Network

Here below are the network parameters that the workstation to which the Aruba Key will be connected needs to have:

1. Internet connection.
2. Possibility to setup HTTP, HTTPS and LDAP connections.

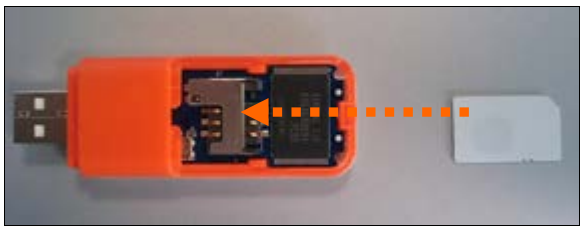
Copyright © Aruba Pec S.p.A. - All Rights Reserved

4 Installation of smart card

If the smart card is not already inserted remove the protective cover, on the back of the device, and slide it off. Once you have opened the smart card reader, insert the Digital Signature SIM, as shown below.

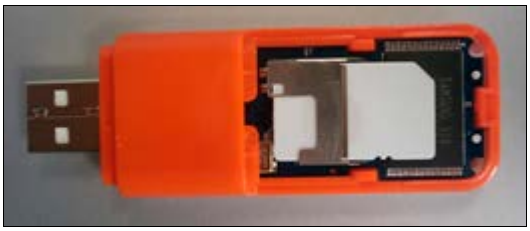
Step 1:

Insert the SIM card with the chip faced down as shown in the image.



Step 2:

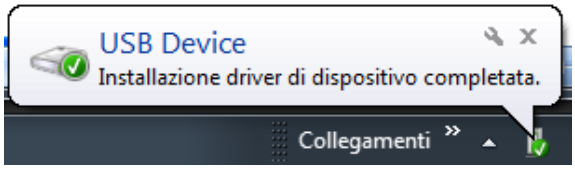
After inserting the SIM card, put the cover back.



Copyright © Aruba Pec S.p.A. - All Rights Reserved

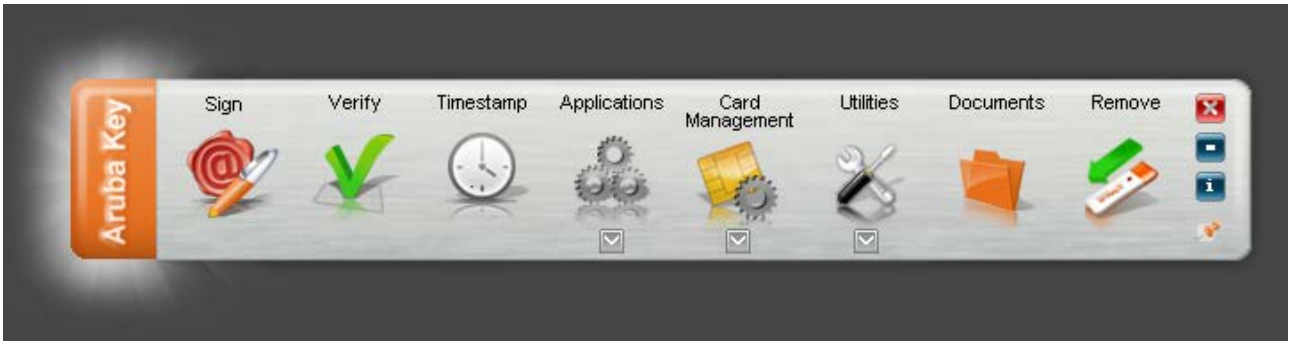
5 Startup of Aruba Key

Connect the Aruba Key to a USB port of the PC and wait for the message indicated here in the image.



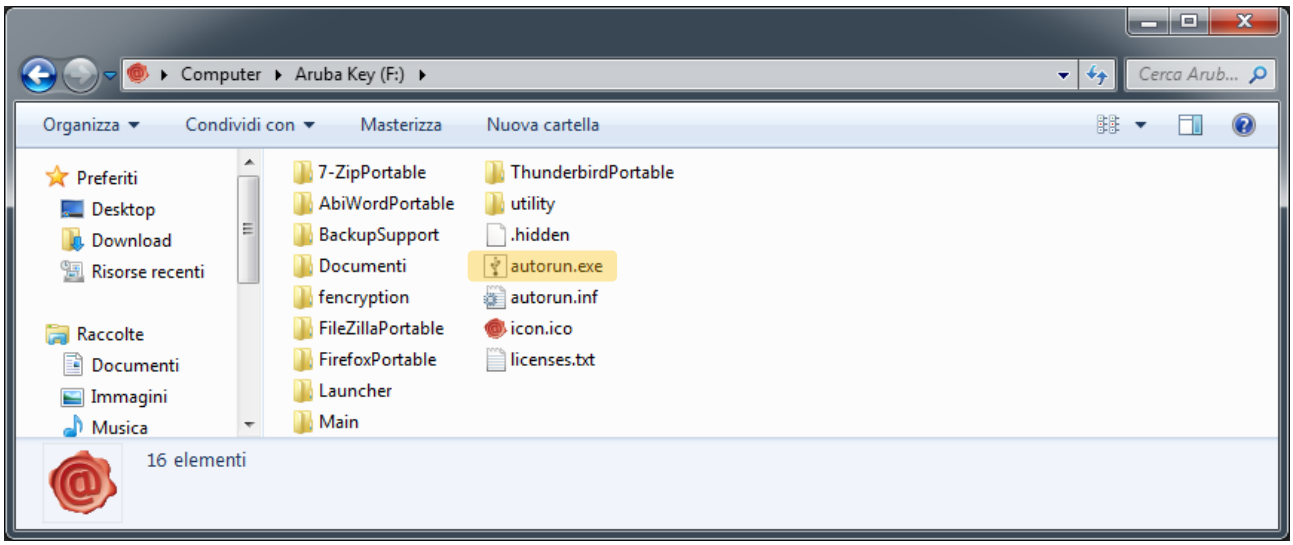
The Aruba Key is identified by the PC as a HID (Human Interface Device), therefore the drivers are found in the device itself for it to be recognized correctly.

If the PC has the Auto-run function active when connecting the Aruba Key the toolbar will automatically come up as shown below.



If, however, when the device is inserted, the Aruba Key toolbar does not come up, it is likely that the Auto-run function is not active.

In this case, access to the content of the Aruba Key and run the *autorun.exe* file, as shown in the image below.

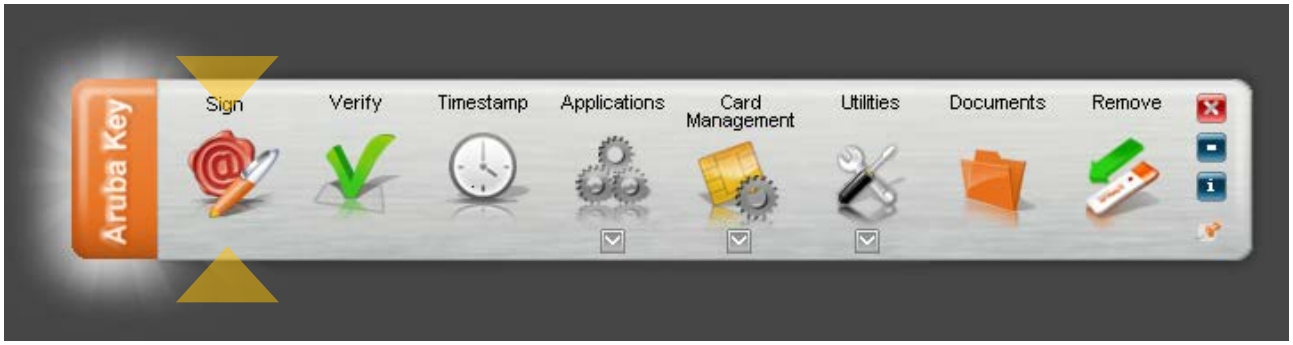


Copyright © Aruba Pec S.p.A. - All Rights Reserved

6 Sign a file in CAdES format (p7m)

Step 1

Drag the file over the **"Signature"** icon.



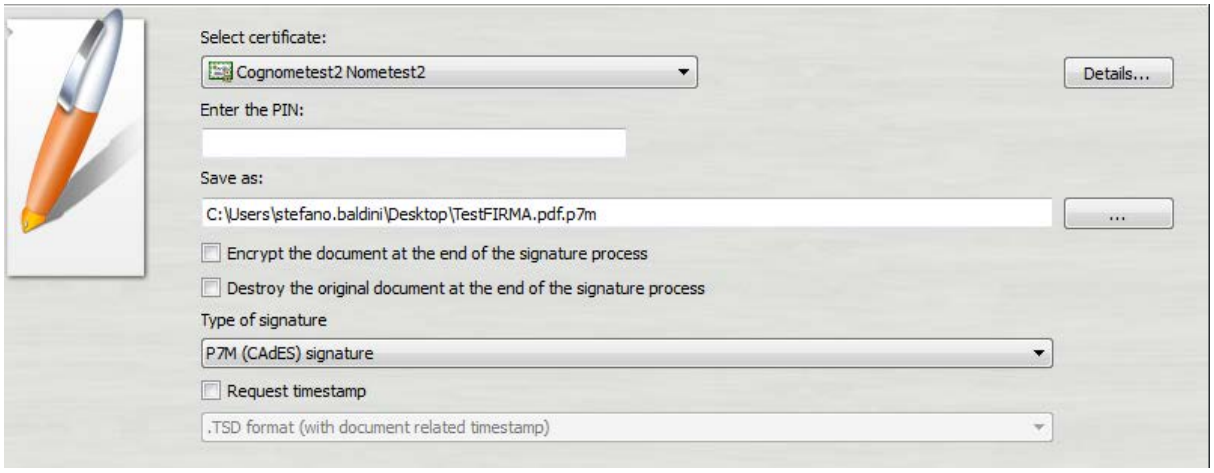
Step 2

Wait for the Aruba Key to fetch the information on the certificates found in the smart card.



Step 3

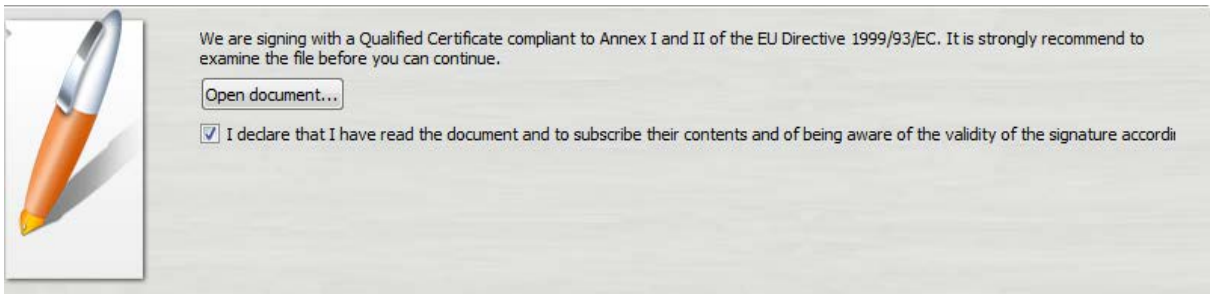
a. Make sure you have selected the certificate for the digital signature (Surname GivenName);
b. Enter the PIN code of the smart card;
c. Select the *"P7M (CAdES) signature";*
d. Verify that the path used to save the signed file is the one you want.
e. Click on **Next >**



Copyright © Aruba Pec S.p.A. - All Rights Reserved

Step 4

a. See the content of the document using the **"Open document"** button;
b. Select the box to confirm you have read the document;
c. Click on **Next >**



Step 5

Wait for the signature process to be completed.



Step 6

Verify that once completed, you see a message which confirms that the file has been signed correctly.

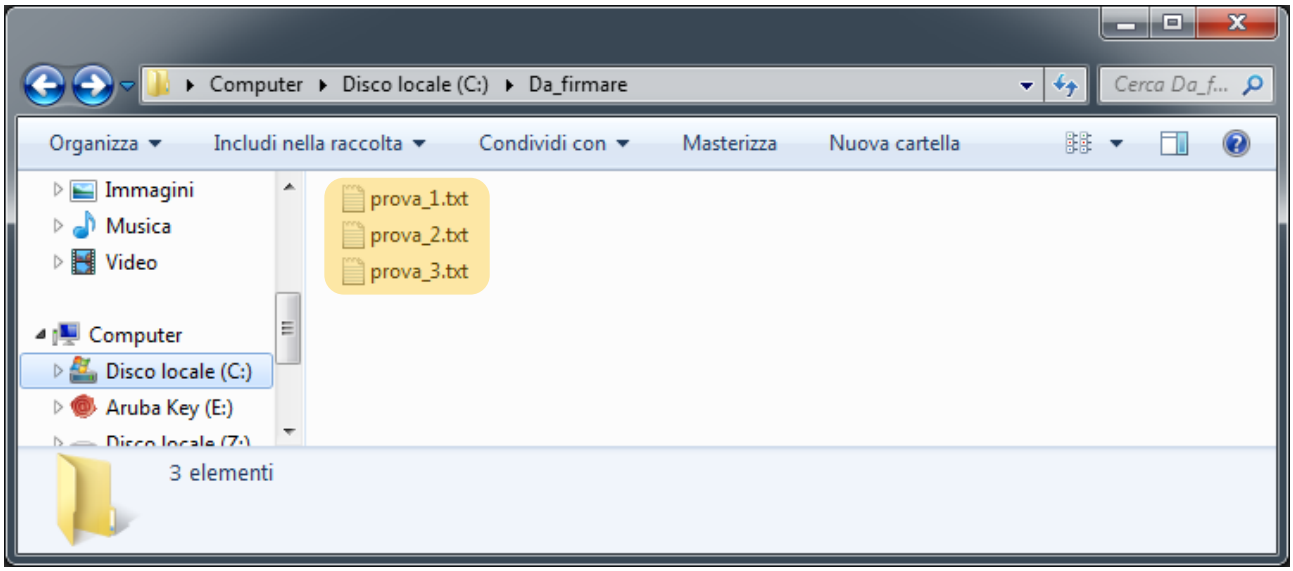


Copyright © Aruba Pec S.p.A. - All Rights Reserved

6.1 Sign multiple files in CAdES format (P7M)

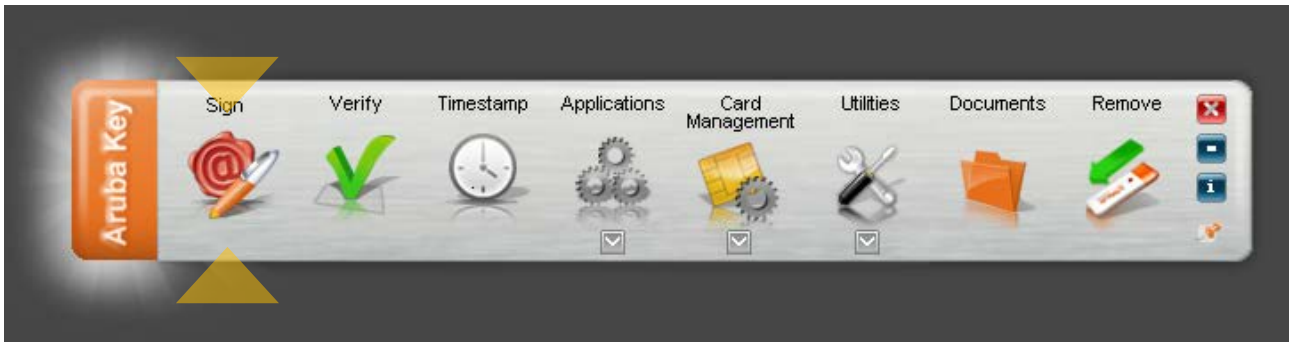
Step 1

Select all the documents which need to be signed.



Step 2

Drag the selected documents over the **"Signature"** icon and release the mouse..



Step 3

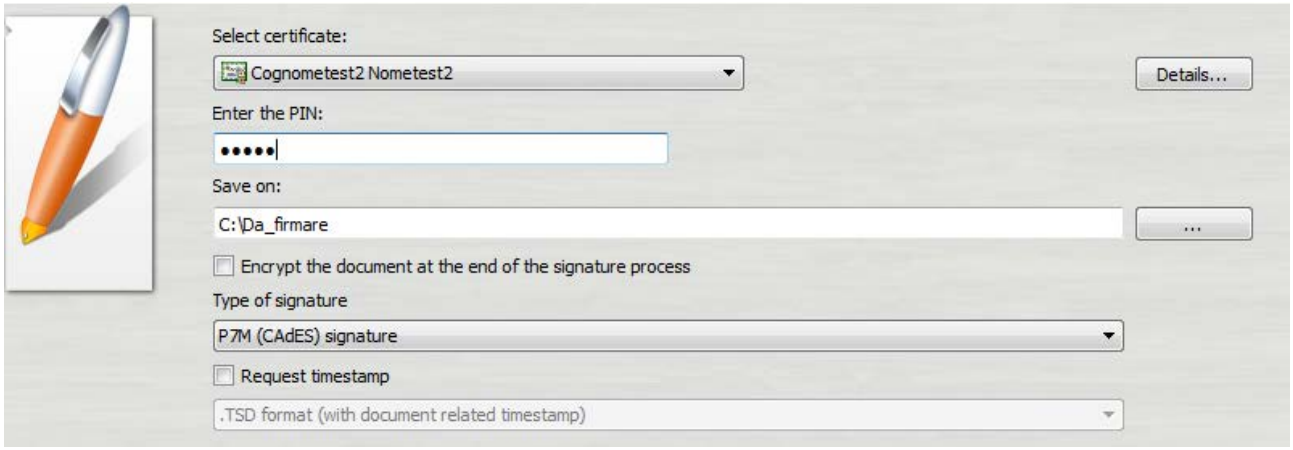
Wait for the Aruba Key to fetch the information on the certificates found in the smart card.



Copyright © Aruba Pec S.p.A. - All Rights Reserved

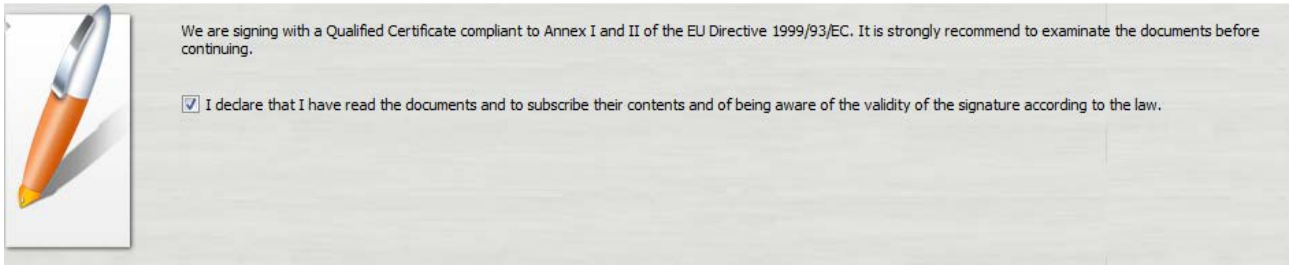
Step 4

a. Make sure you have selected the certificate for the digital signature (Surname GivenName);
b. Enter the PIN code of the smart card;
c. Select the *"P7M (CAdES) signature";*
d. Verify that the path used to save the signed file is the one you want.
e. Click on **Next >**



Step 5

a. Select the box to confirm you have read the documents;
b. Click on **Next >**



Step 6

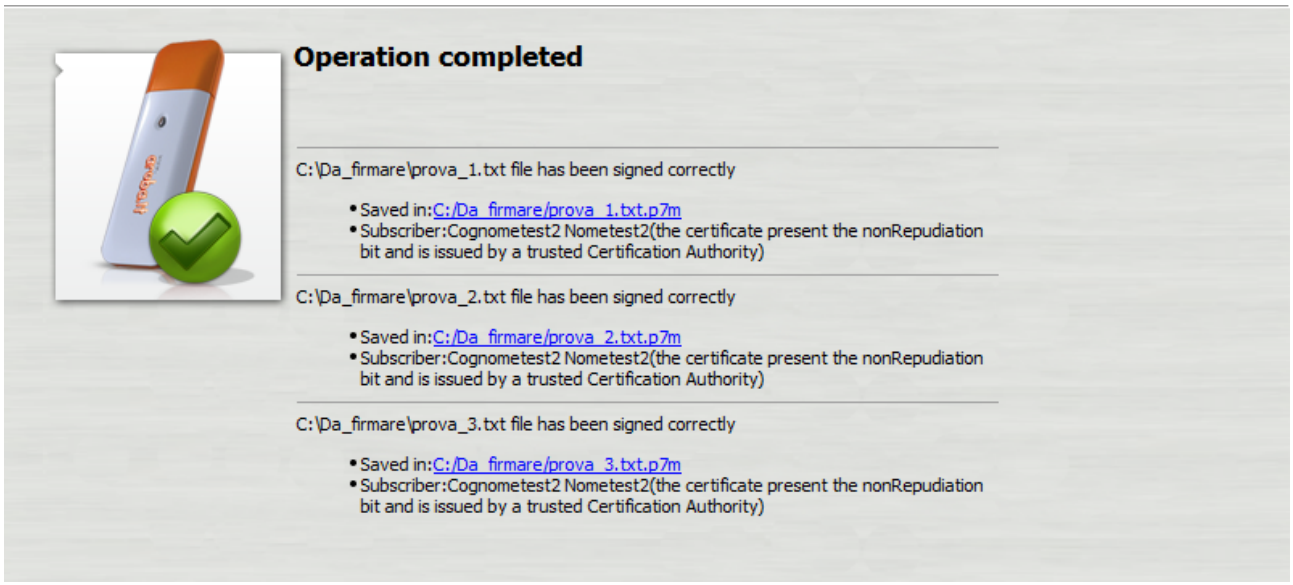
Wait for the signature process to be completed.



Step 7

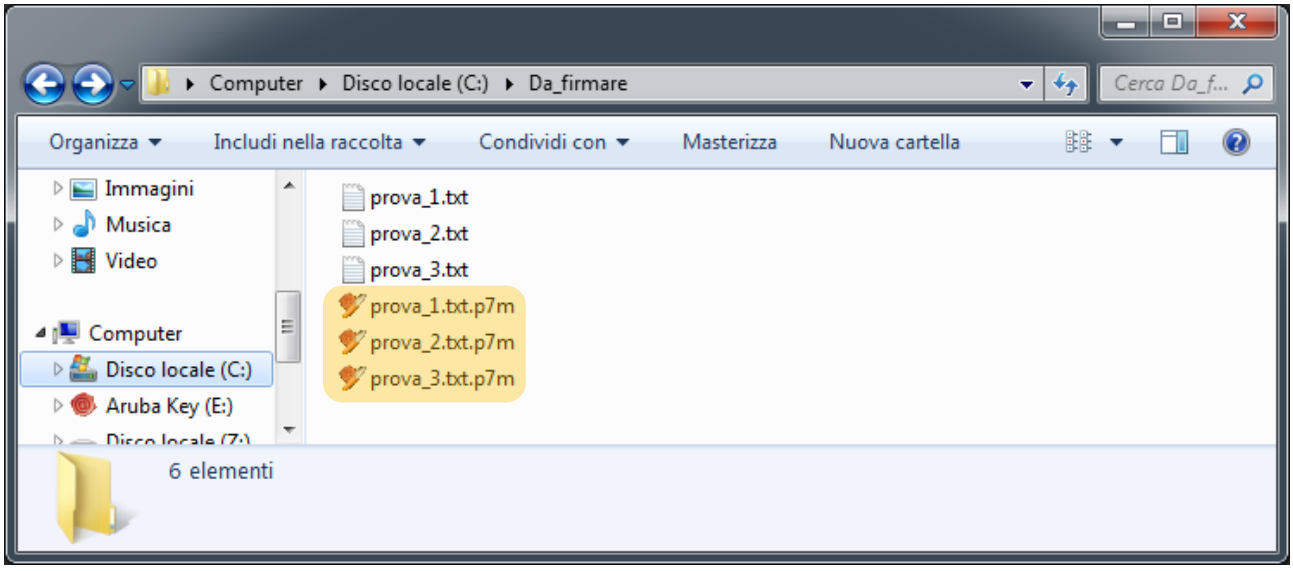
Verify that once completed, you see a message which confirms that each single document has been signed correctly.

Copyright © Aruba Pec S.p.A. - All Rights Reserved



Step 8

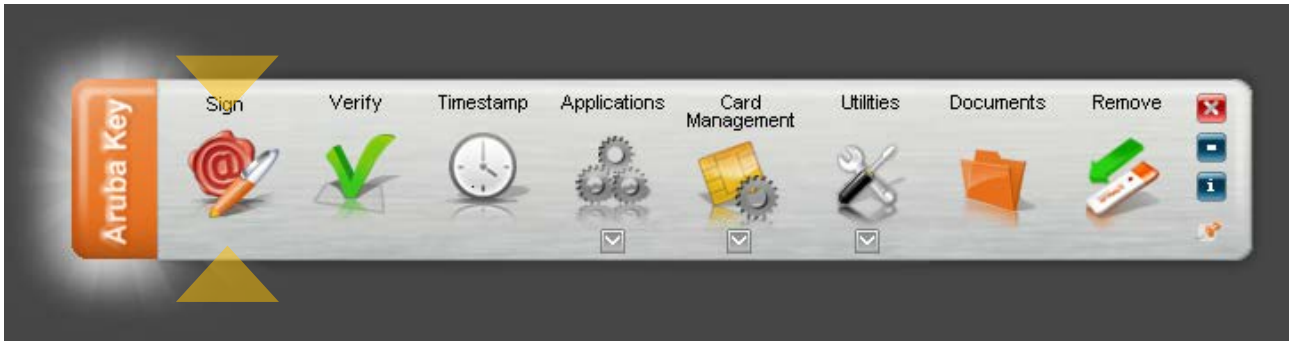
The signed documents will be saved in the folder with the original documents by adding the extension .p7m to the name.



Copyright © Aruba Pec S.p.A. - All Rights Reserved

6.2 Enveloped Signature and Multiple Signature feature

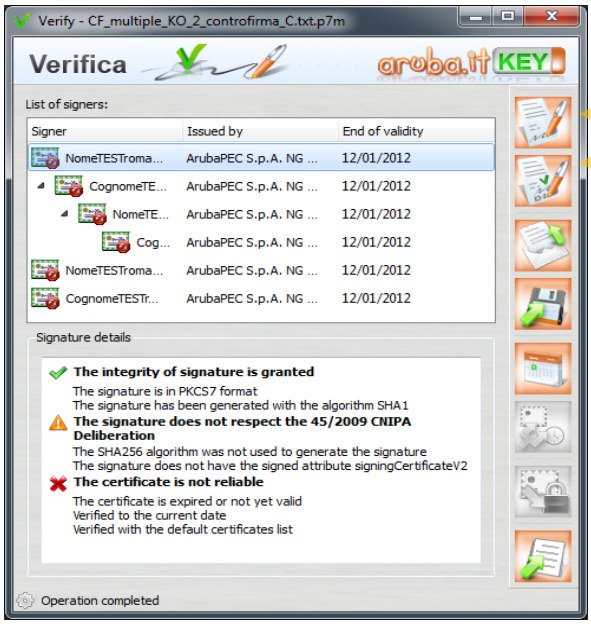
By dragging a pre-signed p7m file over the signature icon it is possible to access the **Multiple Signature** or **Enveloped Signature** features, see images below:



NOTE: To activate the above functions the name of the file must have the .p7m extension.



By selecting **Multiple Signature** the verification window of the signed file will open in which it is then possible to select the signature to which you wish to add a **Parallel Signature** (first button from the top in the right column) or **Countersignature** (second button from the top).



Parallel Signature: Is a type of signature which is added next to an existing signature. This signature is placed in the same content of the previous signature and is normally used to add signatures to a document that has already been signed in cases where this is required.

Countersignature: Is a type of signature which is placed below an existing signature and in fact undersigns the latter. This signature is more nested compared to the signature it is related to and this aspect is shown through a signature tree representation.

Copyright © Aruba Pec S.p.A. - All Rights Reserved

By selecting **Enveloped Signature** you run the wizard for the signature of the entire document and the operations that you need to perform are those indicated in paragraph 6 (step 2 onwards)



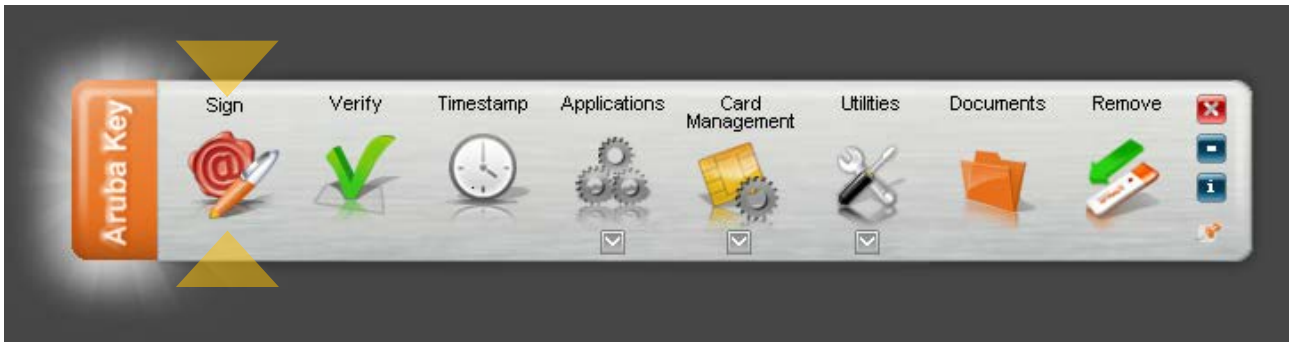
Copyright © Aruba Pec S.p.A. - All Rights Reserved

7 Sign a PDF file digitally

The PDF signing process can only be applied to .PDF files.
It is therefore not possible, using the Aruba Key, to sign in PDF file which has not been previously converted into this format.

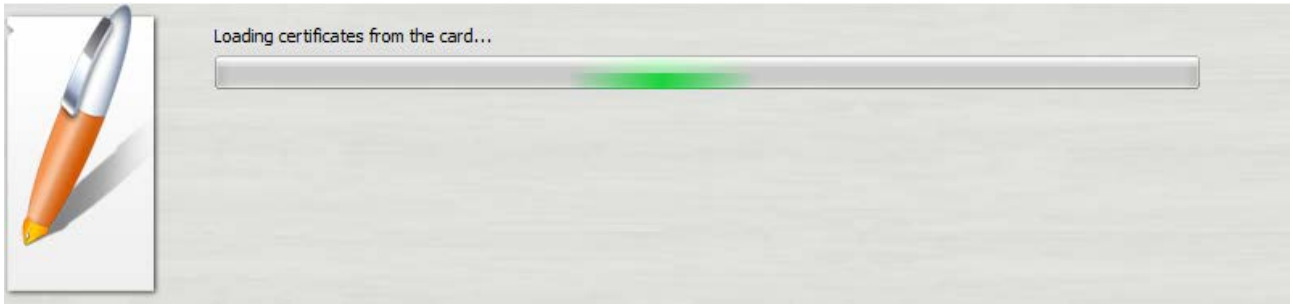
Step 1

Drag the PDF file over the **"Signature"** icon.



Step 2

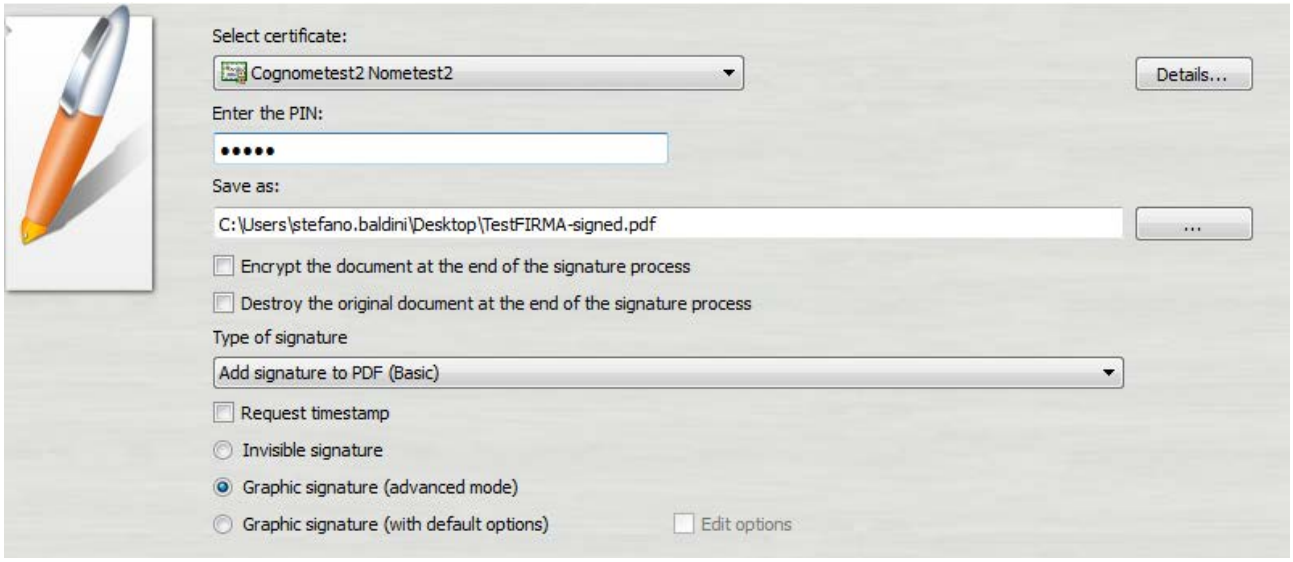
Wait for the Aruba Key to fetch the information on the certificates found in the smart card.



Step 3

a. Make sure you have selected the certificate for the digital signature (Surname GivenName);
b. Enter the PIN code of the smart card;
c. Select *"Add signature to PDF(Basic) or (BES)"* and activate the *"Graphic signature (advanced mode)"* option;
d. Click on **Next >**

Copyright © Aruba Pec S.p.A. - All Rights Reserved

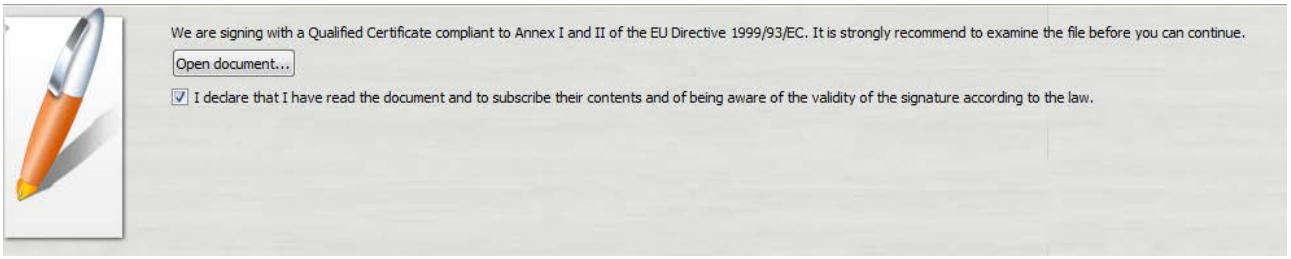


Step 4

a. See the content of the document using the **"Open document"** button;

b. Select the box to confirm you have read the document;

c. Click on **Next >**

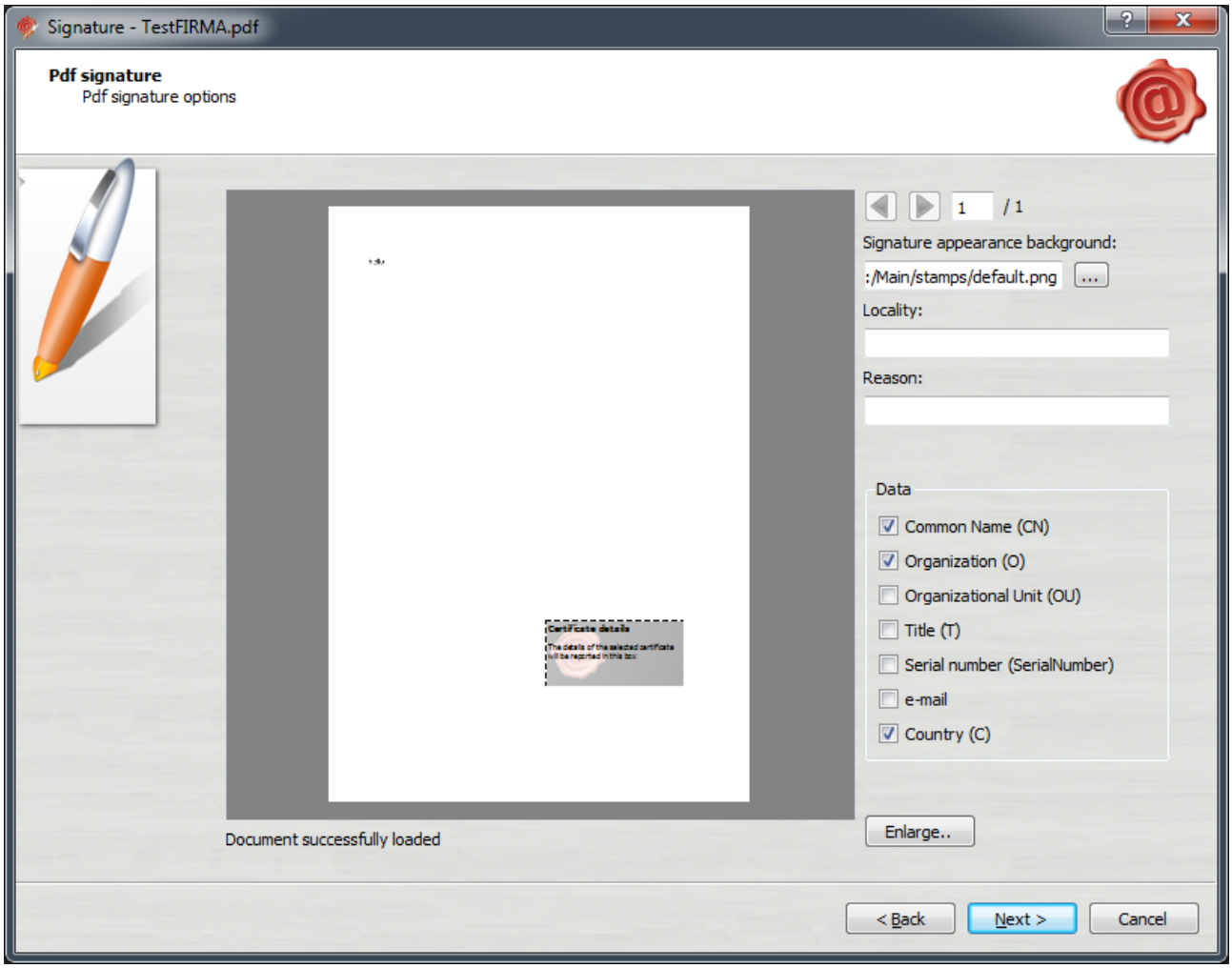


Step 5

a. Specify, using the preview window, the position, the size and the logo of the field where the digital signature will be placed;

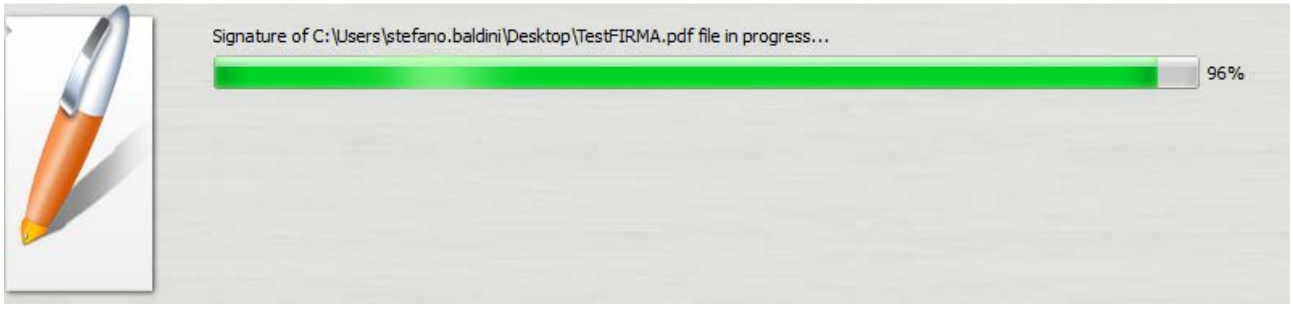
b. Click on **Next >**

Copyright © Aruba Pec S.p.A. - All Rights Reserved



Step 6

Wait for the signature process to be completed.



Step 7

Verify that once completed, you see a message which confirms that the file has been signed correctly.

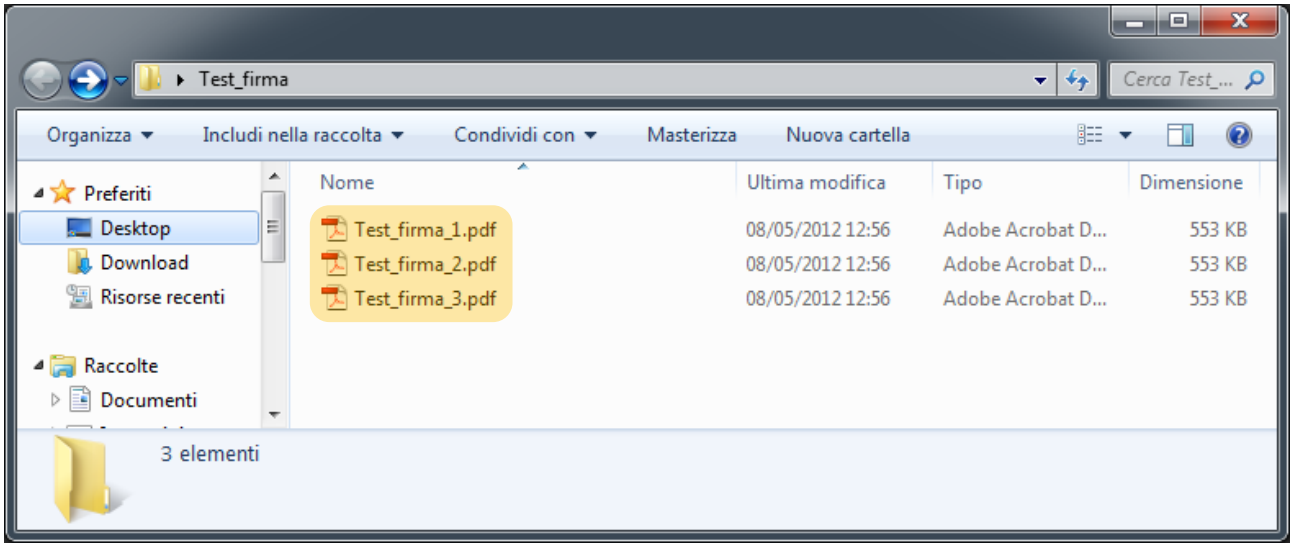
Copyright © Aruba Pec S.p.A. - All Rights Reserved



7.1 Sign multiple PDF files digitally

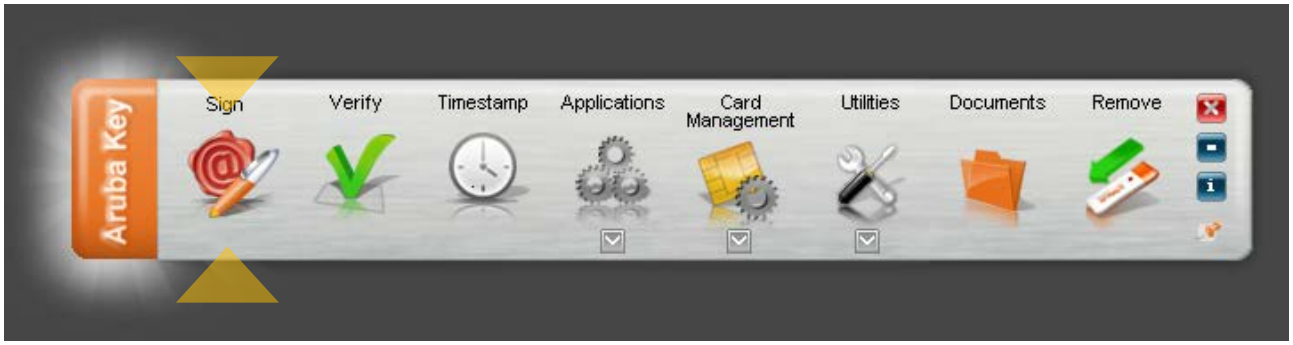
Step 1

Select all the PDF documents you wish to sign.



Step 2

Drag the selected files over the **"Signature"** icon and release the mouse.



Copyright © Aruba Pec S.p.A. - All Rights Reserved

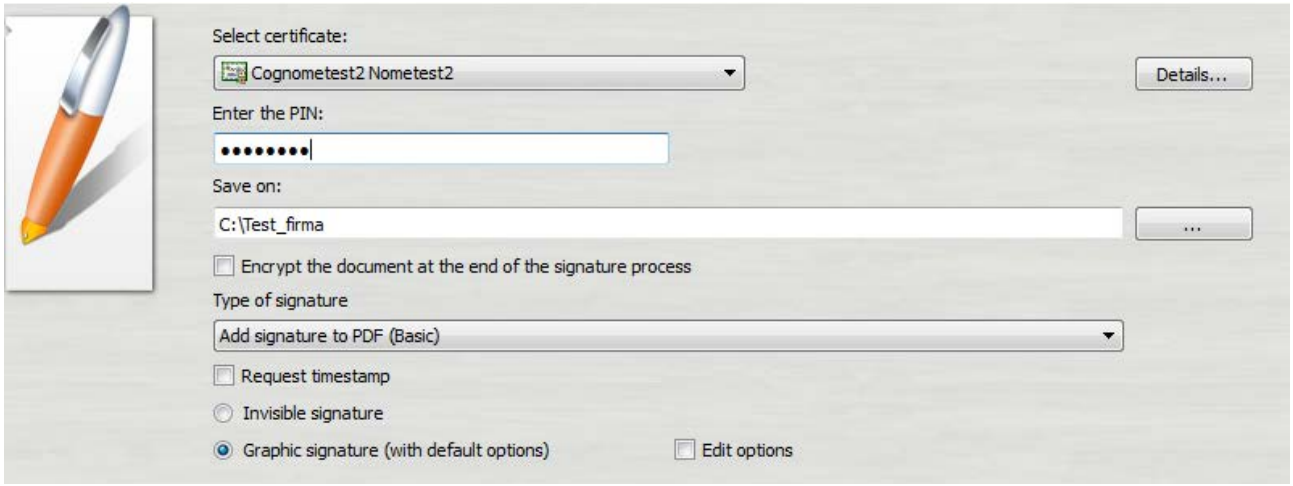
Step 3

Wait for the Aruba Key to fetch the information on the certificates found in the smart card.



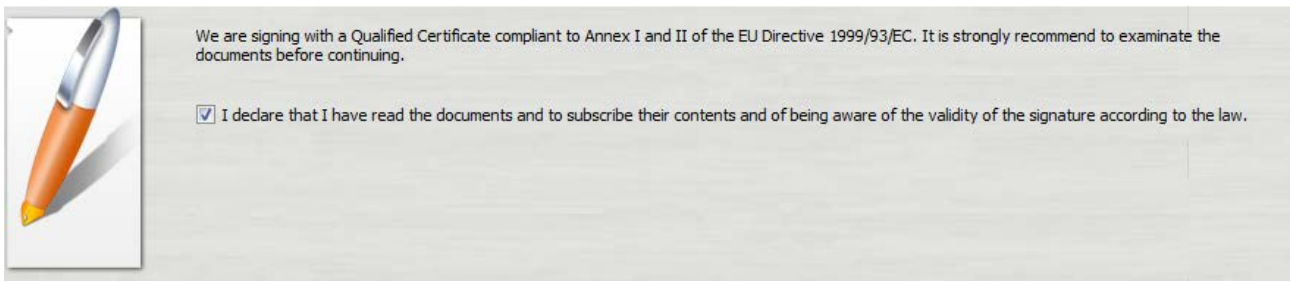
Step 4

a. Make sure you have selected the certificate for the digital signature (Surname GivenName);
b. Enter the PIN code of the smart card;
c. Select the *"Add signature to PDF"* option;
d. Click on **Next >**



Step 5

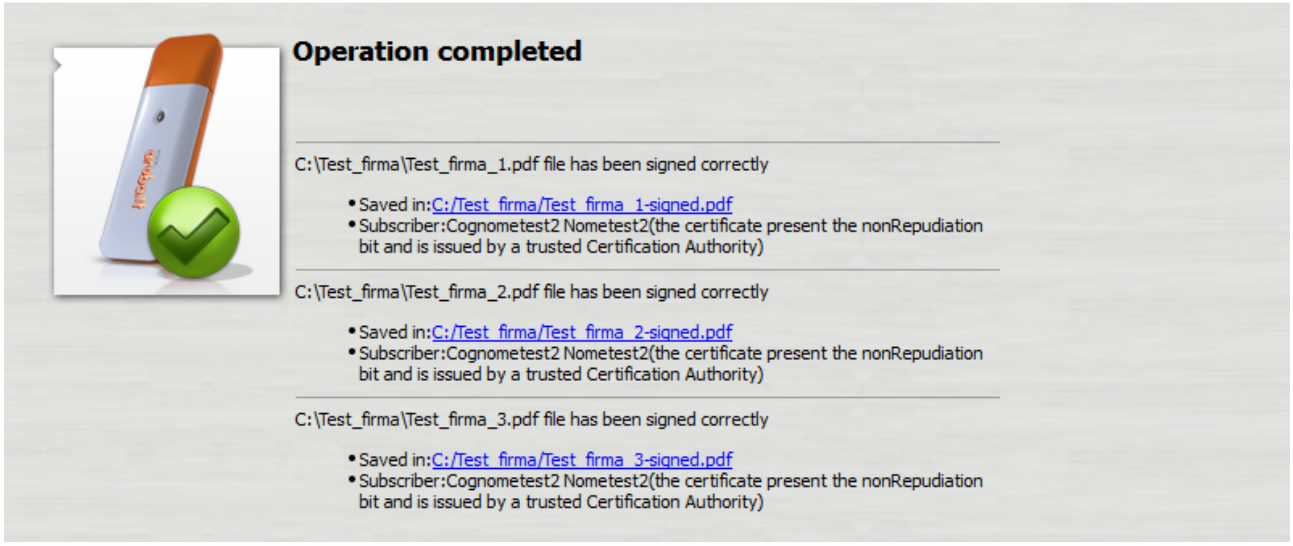
c. Select the box to confirm you have read the documents;
d. Click on **Next >**



Copyright © Aruba Pec S.p.A. - All Rights Reserved

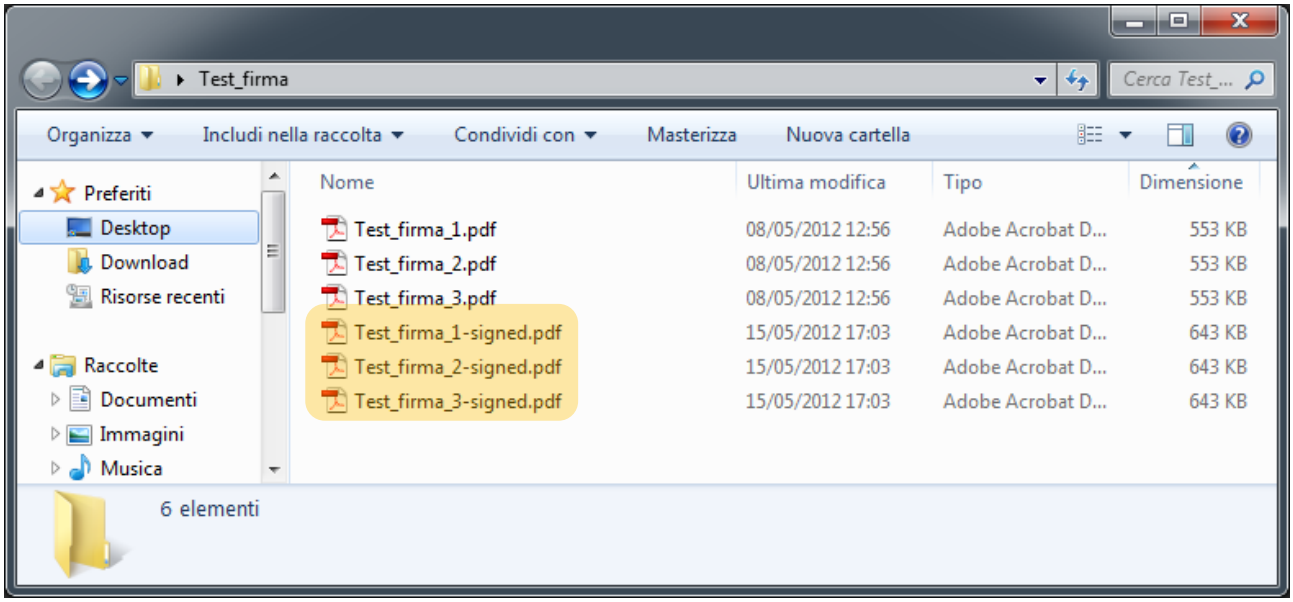
Step 6

Verify that once completed, you see a message which confirms that each single document has been signed correctly.



Step 7

The signed documents will be saved in the folder with the original documents by adding the suffix “signed” to the name.

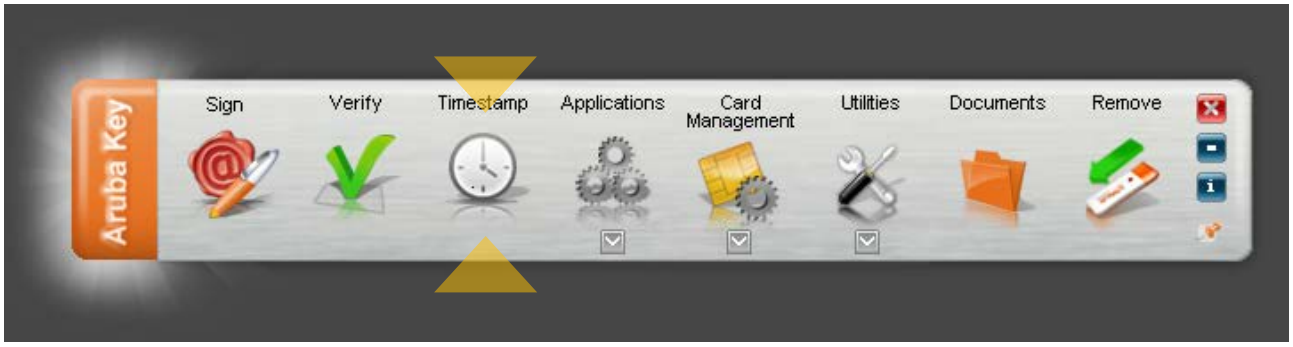


Copyright © Aruba Pec S.p.A. - All Rights Reserved

8 Adding timestamps

Step 1

Drag the file you wish to stamp over the **"Timestamp"** icon.



Step 2

a. Select the account to use for the timestamp request;

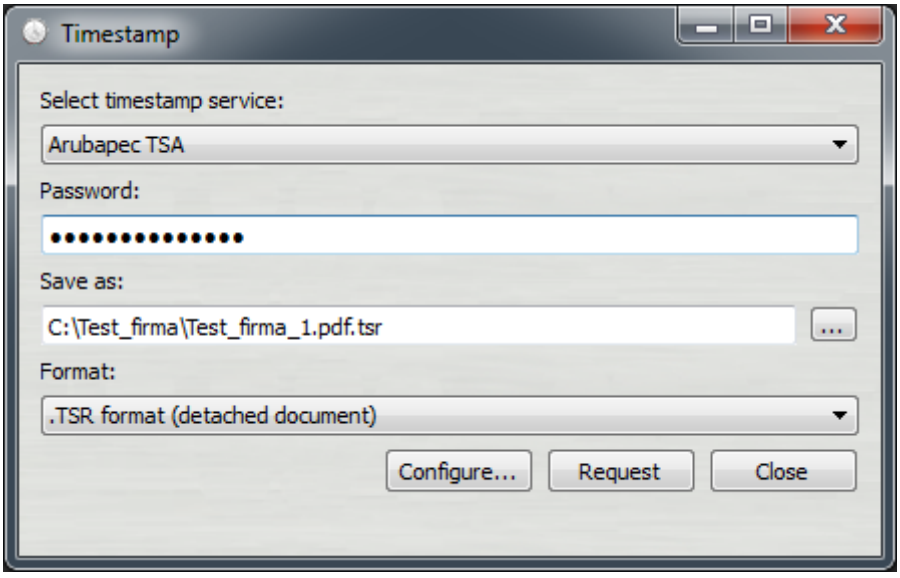
b. Enter the password of the timestamp service;

ATTENTION: The password that you need to enter in this step is that which you received after purchasing and activating a set of timestamps.

Therefore in this stage you should NOT enter any of the codes you received in the envelope with the smart card (e.g. PIN PUK or User Code);

c. Verify that the path used to save the stamped file is the correct one;

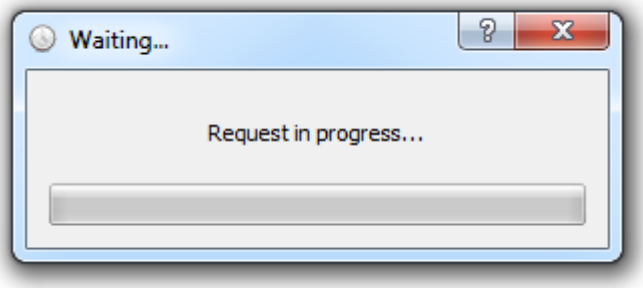
d. Select the format for saving the timestamp;



Copyright © Aruba Pec S.p.A. - All Rights Reserved

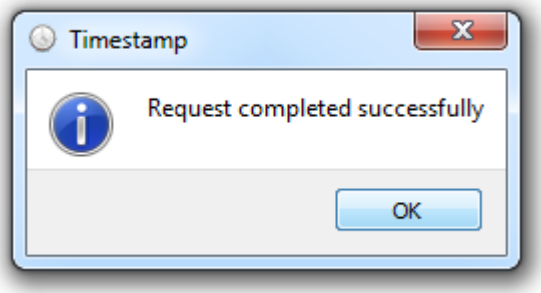
Step 3

Wait for the timestamp process to be completed.



Step 4

Click on OK for the message which notifies the correct timestamp of the file.



Step 5

Recuperate the stamped file saved in the path indicated in Step 2.

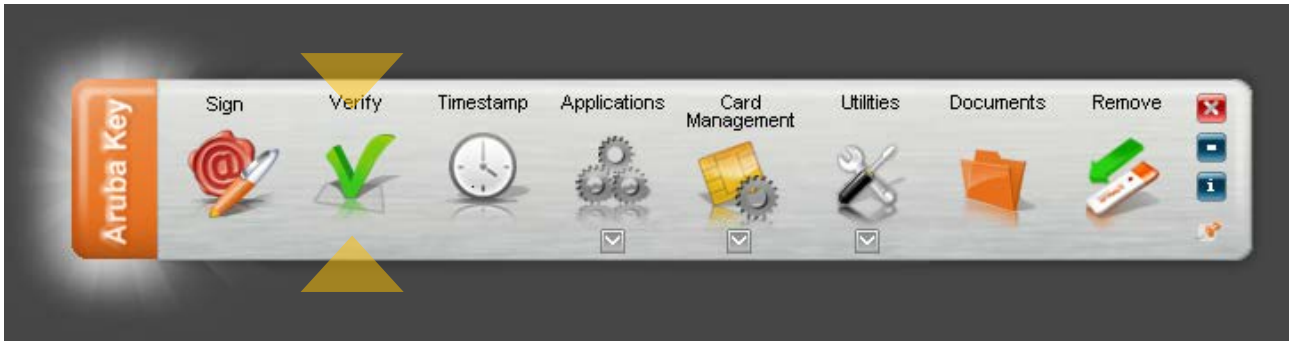
Copyright © Aruba Pec S.p.A. - All Rights Reserved

9 Verification of signed files

Step 1

Drag the file you wish to verify over the **"Verify"** icon.

NOTE: The details indicated below apply to files signed in p7m (CAdES) and pdf (PAdES) format.



Step 2

After completing the Aruba Key verifications you will see a summary window like the following:

The integrity of signature is granted.
The message indicates that the document has not been altered after it was signed.

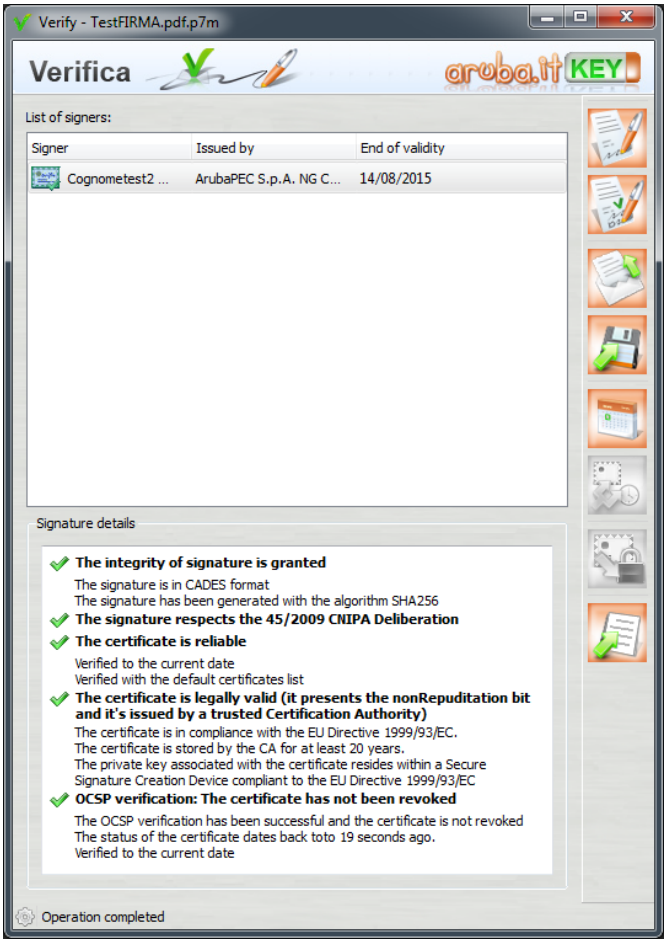
This section contains additional details on the algorithms that were used as well as indicating details on the standards used to generate the signature

The signature respects the 45/2009 CNIPA Deliberation.
Confirms the compliance with the provisions included in the latest law updates according the Italian Regulation.

The certificate is reliable.
This message indicates that the certificate of the signer is guaranteed by a Certificate Authority that is included in the Public List of Certifiers and that on the date of verification, it is not expired.

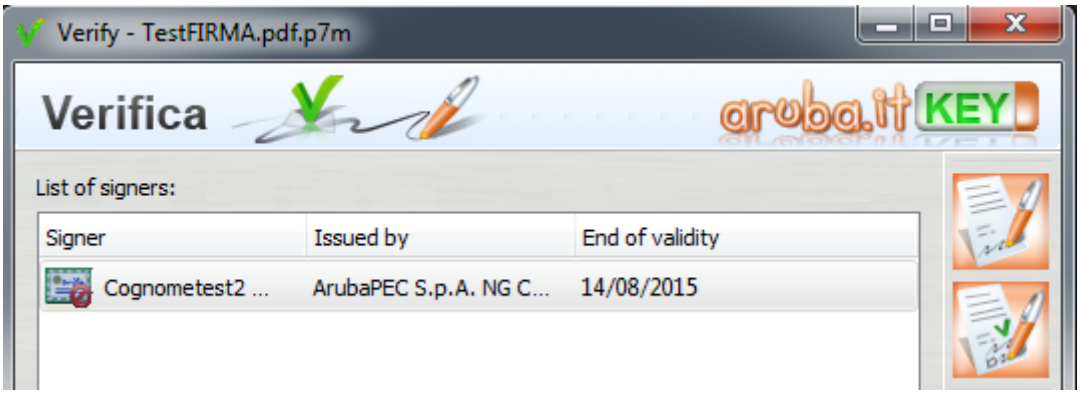
The certificate is legally valid...
This message indicates that the certificate of the signer is a qualified Digital Signature certificate.

The certificate has not been revoked.
This message indicates that the certificate of the signer is not revoked nor suspended.



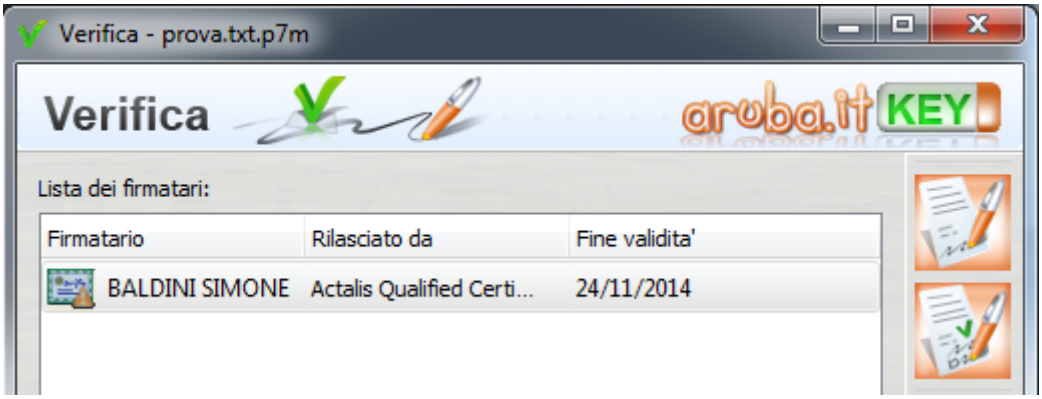
Copyright © Aruba Pec S.p.A. - All Rights Reserved

Should the summary window display a result like the following:



then this shows that all the verification checks on the validity of the signature have been completed, but some of these were not successful. To analyze the type of error that was detected simply see the messages provided by the application in the “Signature Details” section.

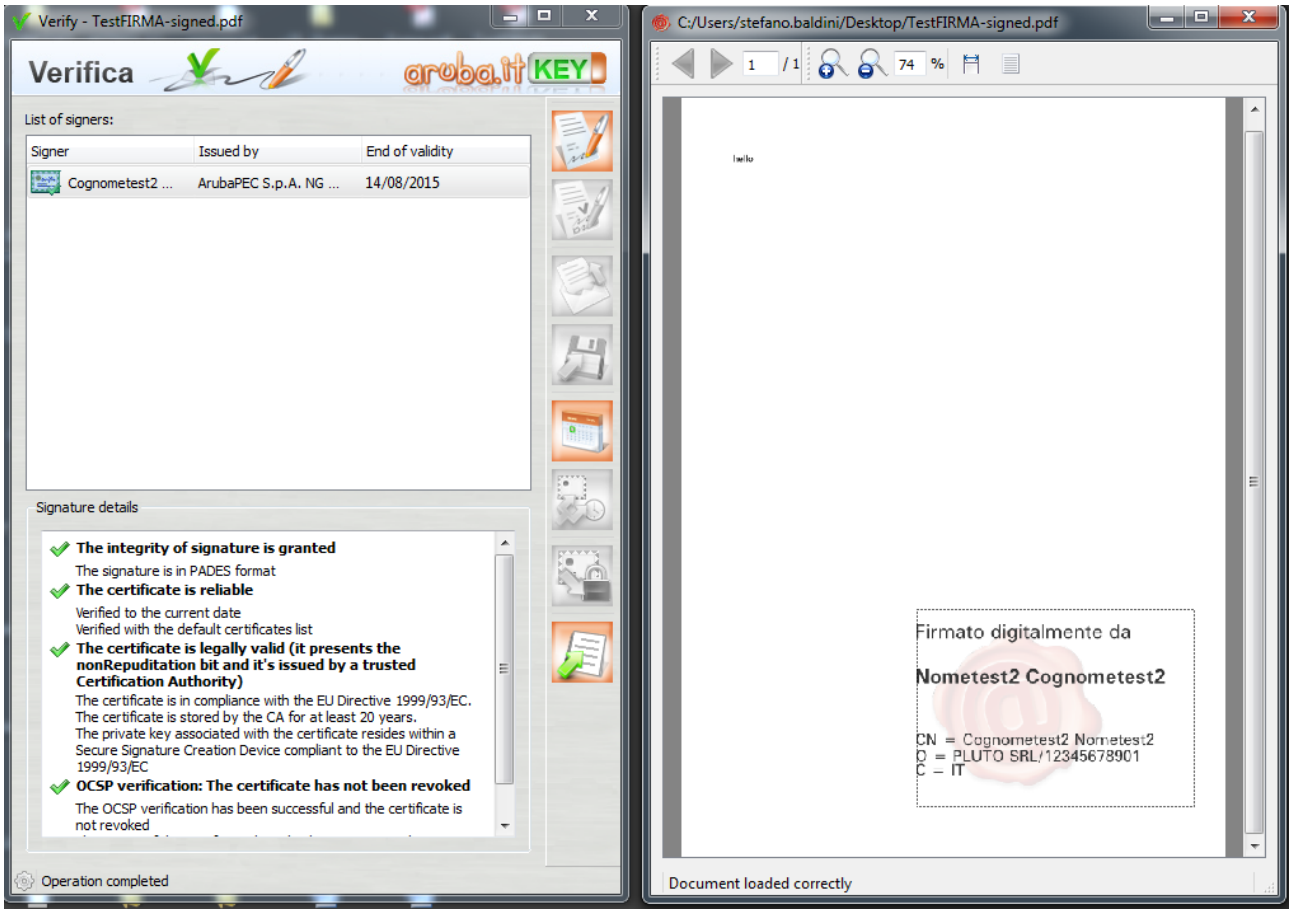
Should the summary window display a message like the following:



then this shows that it has not been possible to complete all the verification checks on the validity of the signature and you are required to analyze the type of error that has been detected by seeing the messages provided by the application in the “Signature Details” section.

Copyright © Aruba Pec S.p.A. - All Rights Reserved

If you are verifying a signed pdf file (identifiable by the type of signature being **PADES-Basic** or **PADES-BES**) it is possible to see the document by right-clicking on the specific signature and selecting **View Signature.**

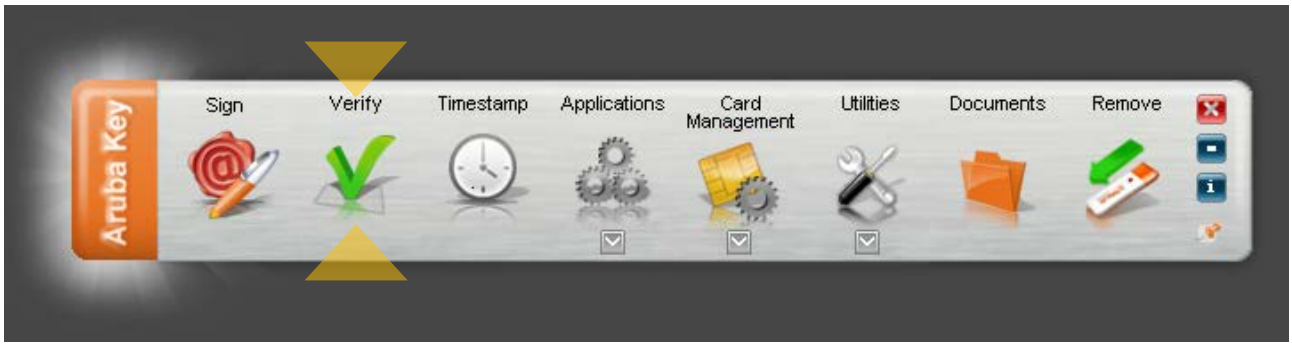


Copyright © Aruba Pec S.p.A. - All Rights Reserved

10 Verification of timestamps

Step 1

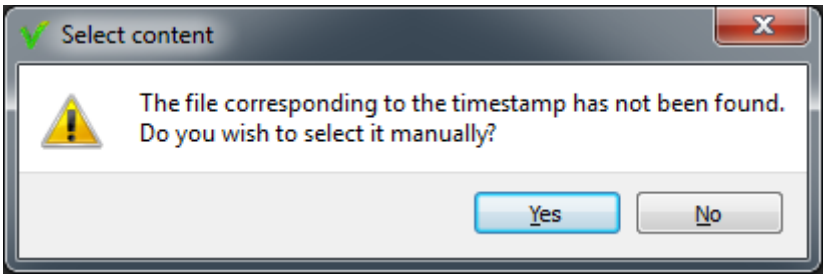
Drag the timestamp to be verified over the **"Verify"** icon.



Step 2

The software, first of all, makes the association Timestamp <-> Stamped File.

During this stage the system will automatically check that the file associated to the timestamp is in the same folder from which the timestamp was selected and, if the search is not successful, the user will be asked if he/she wishes to select the file associated to the timestamp that he/she is verifying manually (see image below).



Select the file and click on Open.

Copyright © Aruba Pec S.p.A. - All Rights Reserved

Step 3

The software activates the verification and, after completing the operations, shows a summary window like the following:

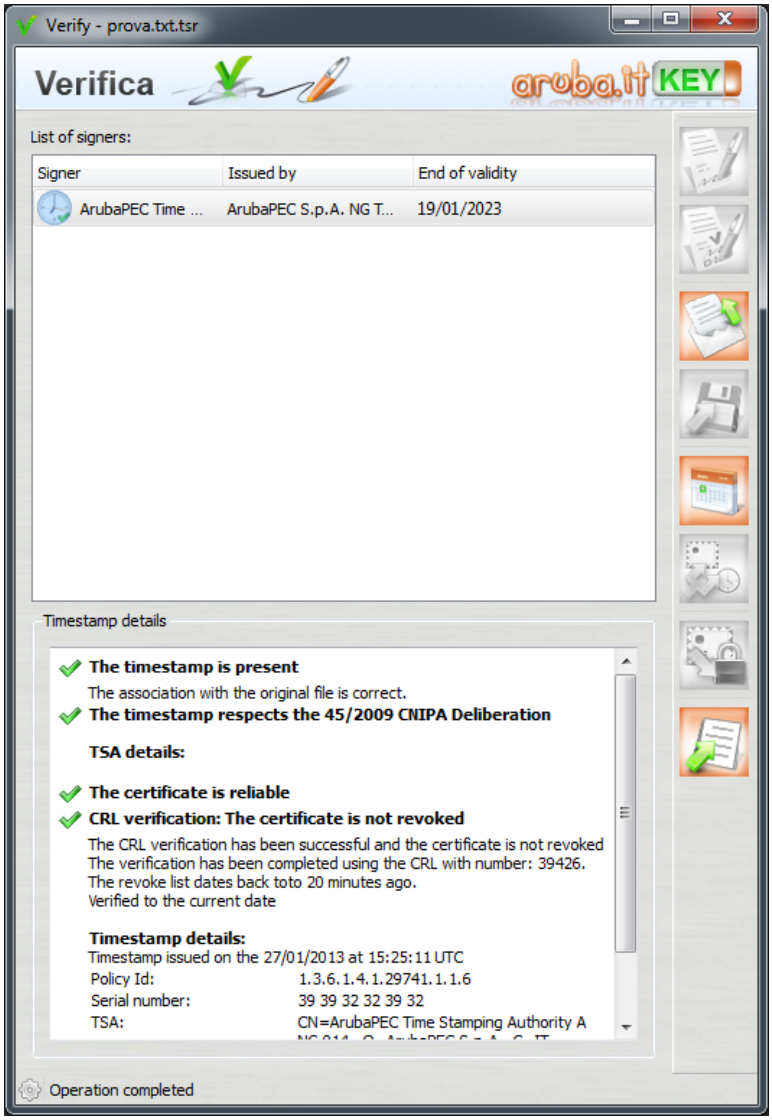
The timestamp is present
This message indicates that the timestamp is complete and is correctly associated to the selected document.

The timestamp respect the 45/2009 CNIPA Deliberation.
Confirms the compliance with the provisions included in the latest law updates according to the Italian Regulation

The certificate is reliable
This message indicates that the Timestamp has been issued by a Certificate Authority that is included in the Public List of Certifiers

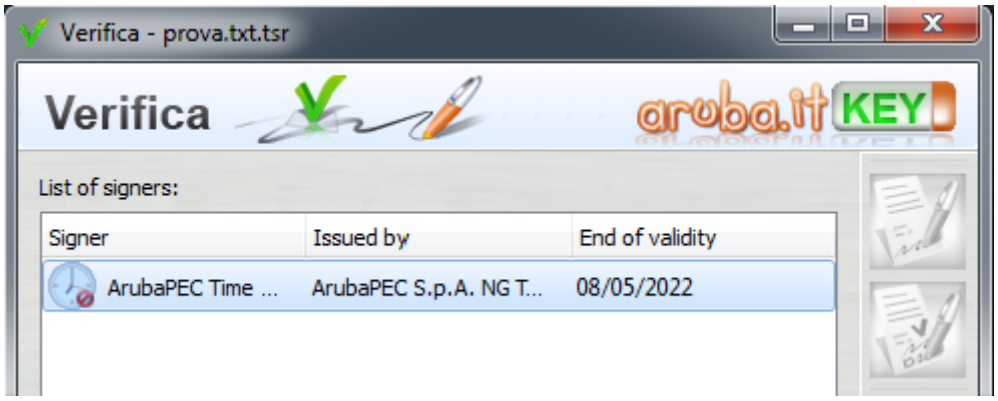
The certificate is not revoked
This message indicates that the certificate of the Timestamp System is not revoked nor suspended.

Timestamp details
In this section you will find details of the timestamp.



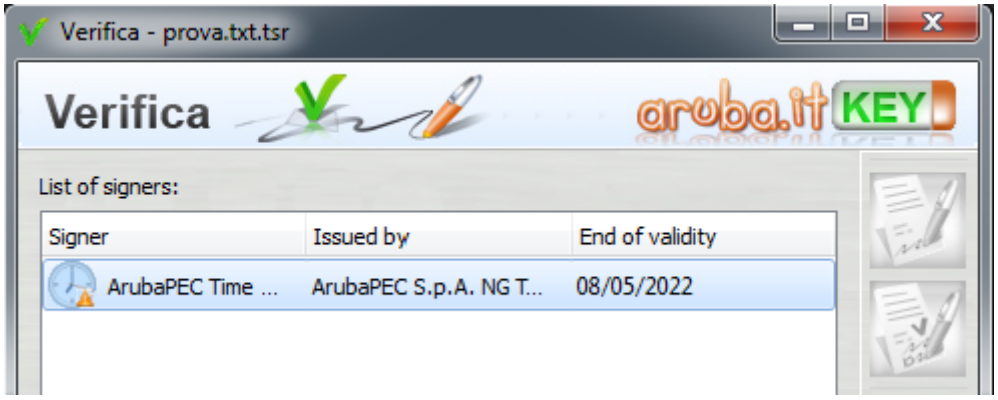
Should the summary window display a result like the following:

Copyright © Aruba Pec S.p.A. - All Rights Reserved



then this shows that all the verification checks on the validity of the timestamp have been completed, but some of these were not successful. To analyze the type of error that was detected simply see the messages provided by the application in the “Timestamp Details” section.

Should the summary window display a message like the following:



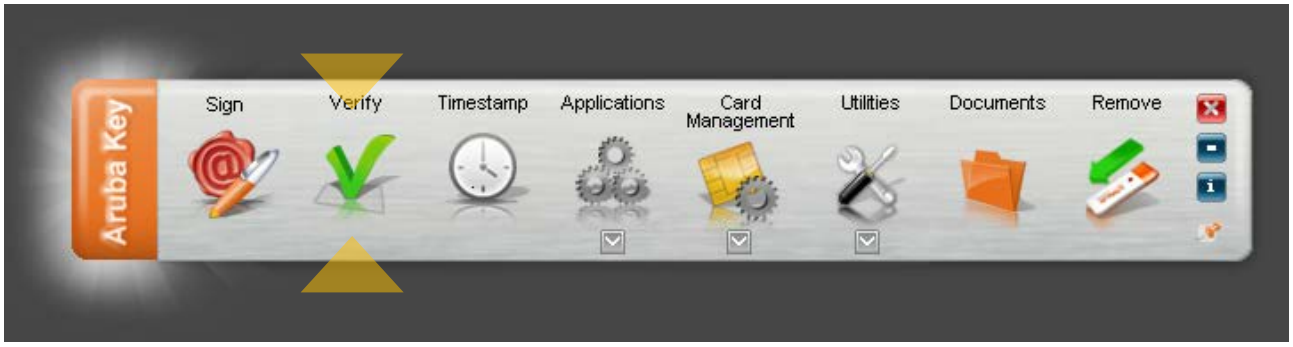
then this shows that it has not been possible to complete all the verification checks on the validity of the timestamp and you are required to analyze the type of error that has been detected by seeing the messages provided by the application in the “Timestamp Details” section.

Copyright © Aruba Pec S.p.A. - All Rights Reserved

11 Verification of Timestamps in .TSD format

Step 1

Drag the timestamp you wish to verify over the **"Verify"** button.



Step 2

The software activates the verification and, after completing the operations, shows a summary window like the following:

The timestamp is present

This message indicates that the timestamp is complete and is correctly associated to the selected document.

The signature respects the 45/2009 CNIPA Deliberation.

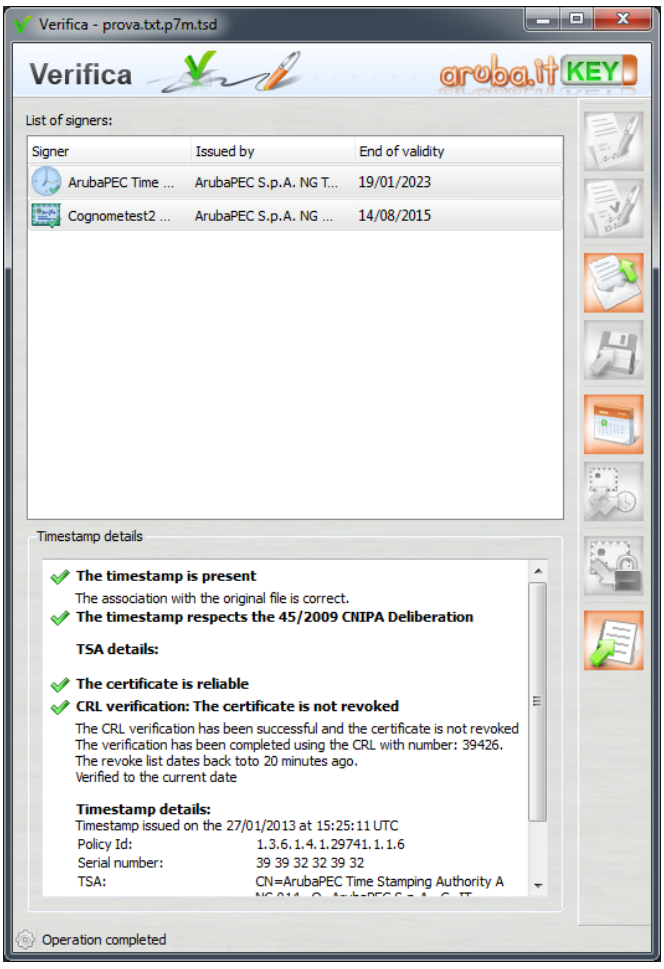
Confirms the compliance with the provisions included in the latest law updates according to the Italian regulation

The certificate is reliable.
The message indicates that the Timestamp has been issued by a Certificate Authority that is included in the Public List of Certifiers.

The certificate is not revoked
This message indicates that the certificate of the Timestamp System is not revoked nor suspended.

Timestamp details
In this section you will find details of the timestamp.

NOTE:
Should the summary window mark an error (in red) or a warning (in yellow) related to the timestamp, you need to consider the notes indicated in Chapter 10.



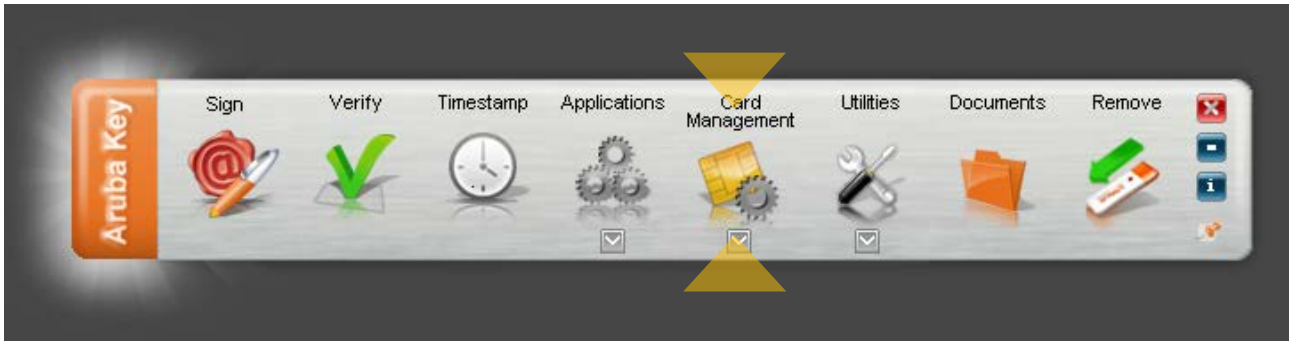
Copyright © Aruba Pec S.p.A. - All Rights Reserved

12 Management of smart card

12.1 Change pin code

Step 1

To change the PIN code of the smart card found in the Aruba Key click on the "**Card Management"** button.



Step 2

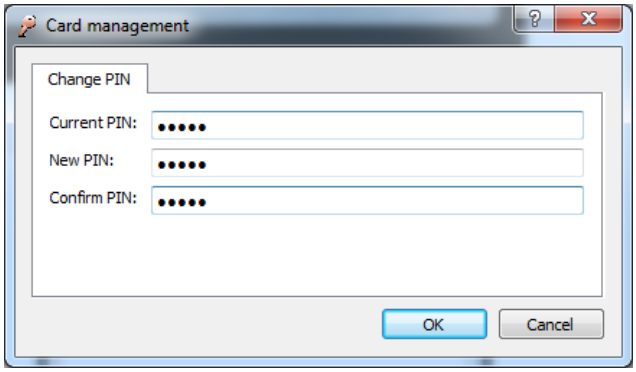
Click on **"Change PIN".**



Step 3

In the "Change Pin" window enter the previous PIN, then enter the new Pin and click on OK

ATTENTION:
For the PIN code it is possible to use letters (a,b,A,B, etc..) and numbers (0,1,2,3,4,5,6,7,8 and 9). For security reasons we recommend that you use PIN codes with at least 8 numbers.

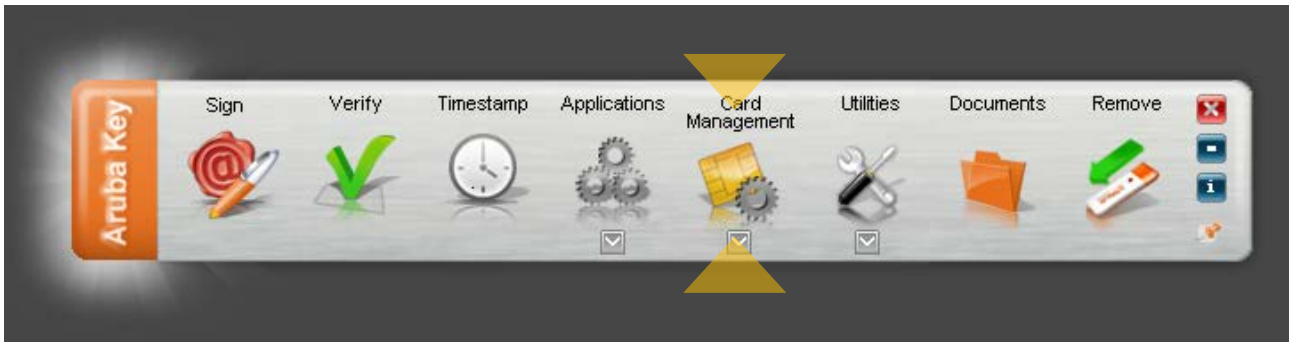


Copyright © Aruba Pec S.p.A. - All Rights Reserved

12.2 Unlock PIN

Step 1

To unlock the PIN code of the smart card found in the Aruba Key click on the **"Card Management"** icon.



Step 2

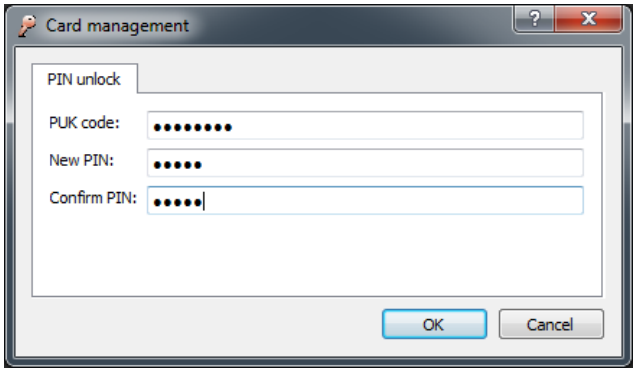
Click on the **"Unlock PIN"** icon.



Step 3

In the "Unlock Pin" window enter the PUK code, then enter the new PIN and click on OK.

ATTENTION:
For the PIN code it is possible to use letters (a,b,A,B, etc..) and numbers (0,1,2,3,4,5,6,7,8 and 9). For security reasons we recommend that you use PIN codes with at least 8 numbers.

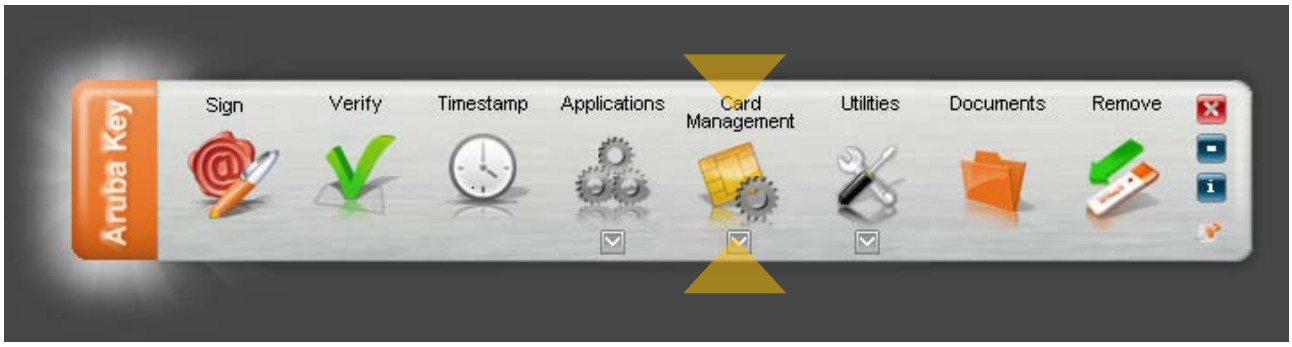


Copyright © Aruba Pec S.p.A. - All Rights Reserved

12.3 Change PUK code

Step 1

To change the PUK code of the smart card found in the Aruba Key click on the "**Card Management"** icon.



Step 2

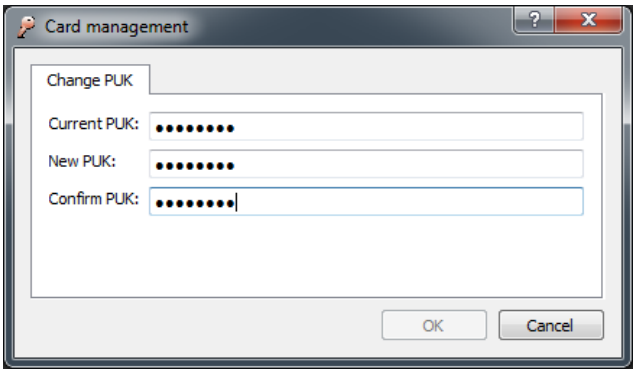
Click on **"Change PUK"**.



Step 3

In the "Change PUK" window enter the previous PUK, then enter the new one and click on OK.

ATTENTION:
For the PUK code it is possible to use letters (a,b,A,B, etc..) and numbers (0,1,2,3,4,5,6,7,8 and 9). For security reasons we recommend that you use PUK codes with at least 8 numbers.

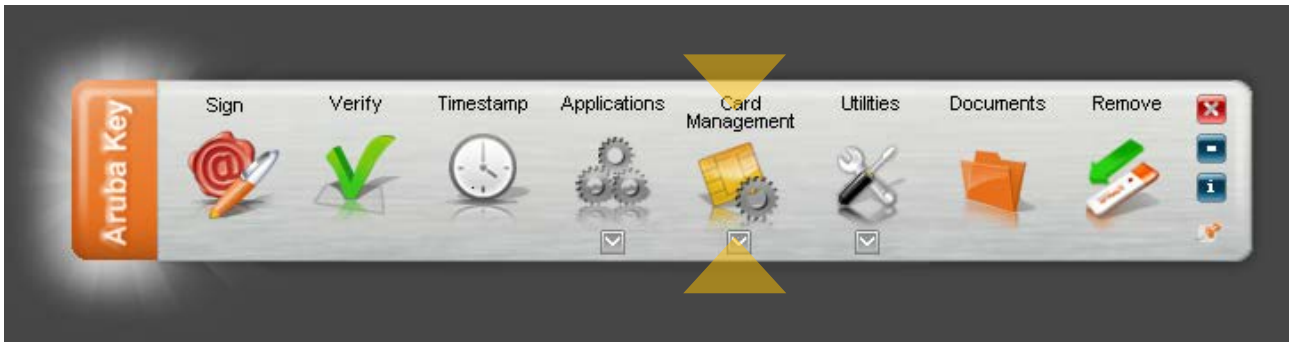


Copyright © Aruba Pec S.p.A. - All Rights Reserved

12.4 Smart card information

Step 1

To get the information on the smart card found in the Aruba key click on "**Card Management".**



Step 2

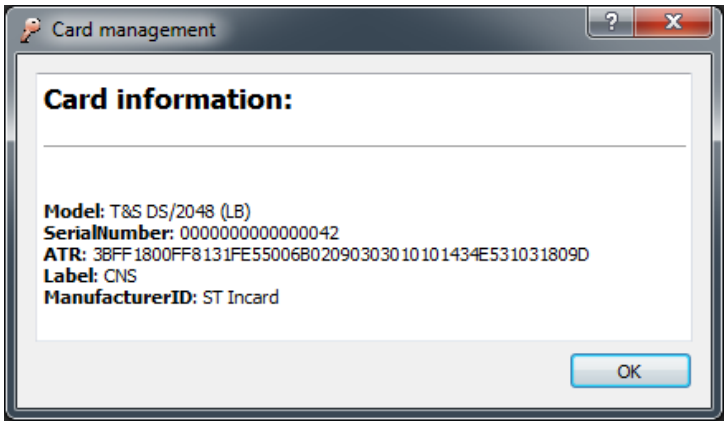
Click on **"Card Info"**.



Step 3

In the "Manage Smart Card" window you will find the following information:

- Model;
- Serial Number of the smart card;
- ATR of the smart card;
- Any Label that is associated to the smart card;
- Manufacturer of the smart card



Copyright © Aruba Pec S.p.A. - All Rights Reserved

12.5 Smart card management error codes

When **changing the PIN**, **unlocking the PIN** and **changing the PUK**, the Aruba key may give the following error messages:

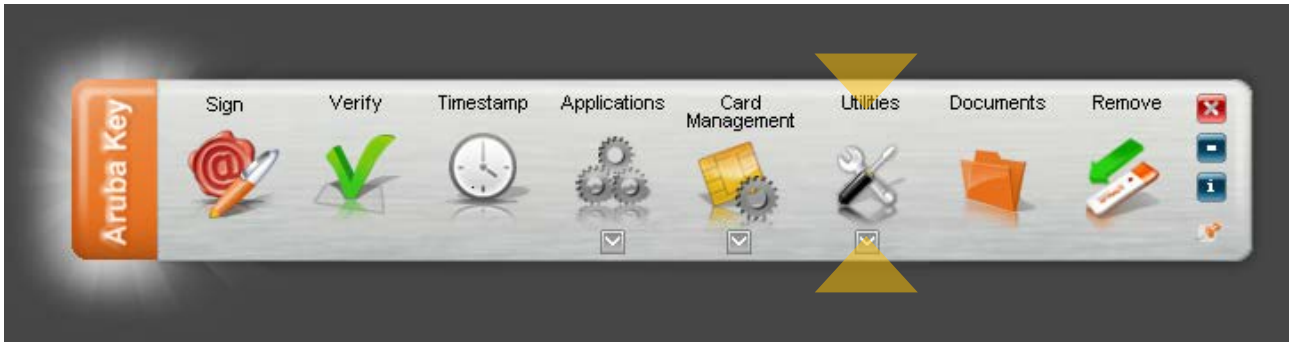
Error: The current Pin is not correct. Warning: too many incorrect attempts may lock the PIN.	This message indicates that the "Old Pin" field of the "Change Pin" window, is not correct. In this case the user needs to bear in mind that by attempting to enter the incorrect PIN repeatedly may cause the PIN to lock and therefore the smart card.
Error: The PIN is locked.	This message indicates that the PIN of the smart card is locked. You need to unlock the PIN by following the indications found in the "Unlock PIN" paragraph.
Error: The PUK Code is not correct. ***Warning: too many incorrect attempts may lock the PUK!***	This message indicates that the "Puk" field of the "Unlock Pin" window, is not correct. In this case the user needs to bear in mind that by attempting to enter the incorrect PUK repeatedly may cause the smart card to lock permanently.
Error: The current PUK is not correct. ***Warning: too many incorrect attempts may lock the PUK!***	This message indicates that the "Puk" field of the "Change Puk" window, is not correct. In this case the user needs to bear in mind that by attempting to enter the incorrect PUK repeatedly may cause the smart card to lock permanently.
Error: The PUK is locked.	This message indicates that the PUK of the smart card is locked. The user needs to contact the Certification Authority in order to revoke the current certificates and purchasing a new smart card.

Copyright © Aruba Pec S.p.A. - All Rights Reserved

13 Auto-diagnosis of the Aruba Key device

Step 1

To access the auto-diagnosis application found in the Aruba Key click on "**Utilities".**



ATTENTION: On Macosx platform users need to have the admin password of the workstation to allow the software to analyze the memory of the device.

Step 2

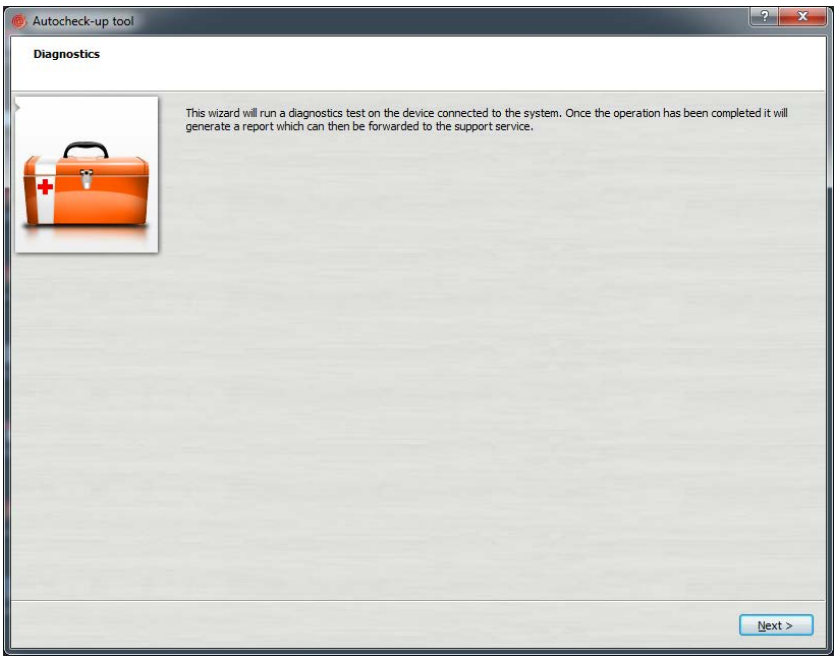
Click on "**Autocheck-up**".



Copyright © Aruba Pec S.p.A. - All Rights Reserved

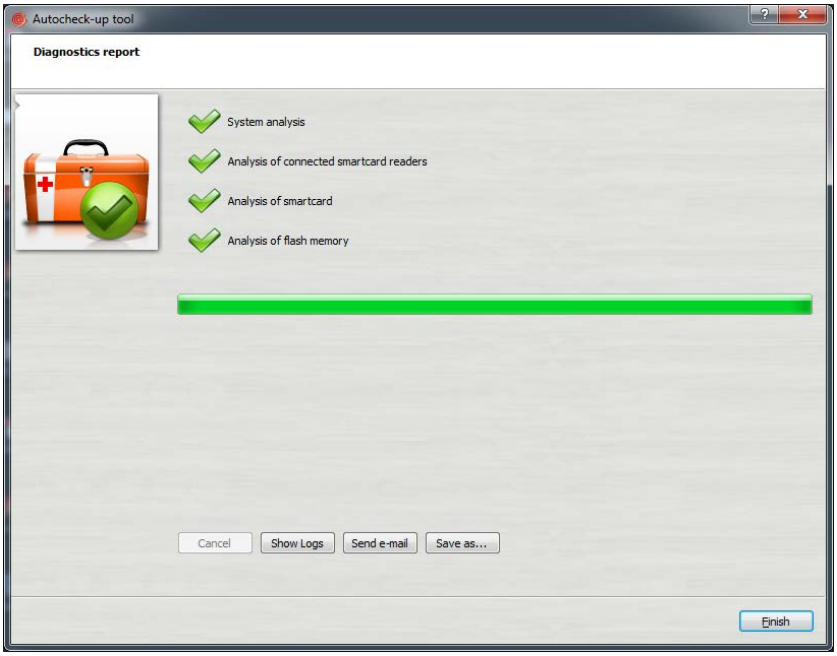
Step 3

Click on "**Next**" and wait for the Aruba key to complete the analysis of the device



Step 4

After completing the analysis, if faults are not found, a page like the following will appear.



The user will be able to send the result of the analysis via e-mail or save it in a .txt file.

Note: *To use this function of the Aruba key the user must have administrator privileges.*

Copyright © Aruba Pec S.p.A. - All Rights Reserved

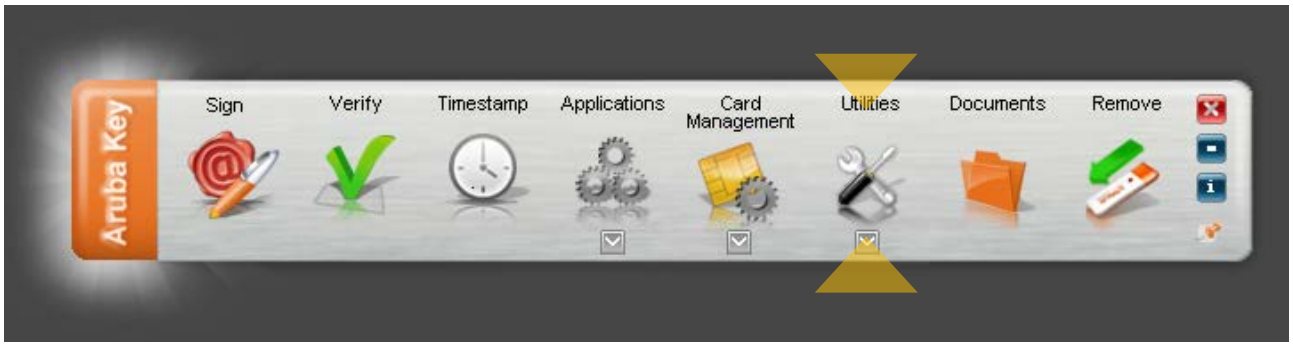
14 "Import" certificate

The “Import” certificate function allows you to import the Aruba Key certificates in the local certificates store making it possible for the applications found in the host pc to interface with the device like for example: Internet Explorer, Adobe Reader (Professional), Safari, Digital Signature software, etc…

NOTE: To activate this function you must have the PC administrator privileges.

Step 1

To activate the “import” of the certificate, click on “**Utilities”.**



Step 2

Click on “**Import” Certificate**.



Step 3

Follow the installation wizard accepting the contract conditions and clicking on OK in each page.

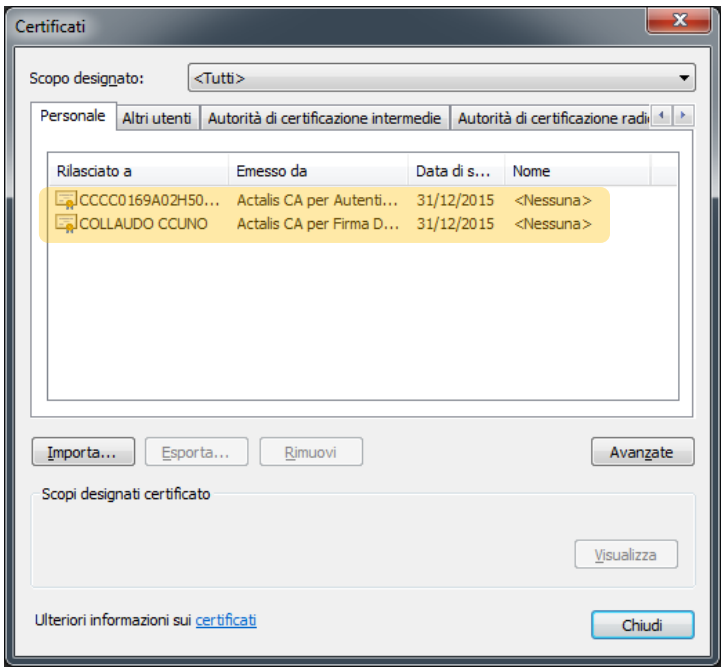
Copyright © Aruba Pec S.p.A. - All Rights Reserved

Step 4

Verify that the certificate has been installed correctly by following these steps:

1. Start Microsoft Internet Explorer;
2. Select Tools → Internet Options;
3. Select the Content tab, click on the Certificates button and then the Personal tab.
4. Check that the certificates installed on the Arubakey are listed
5. Click on “Close”

Follow the same process with the Macosx Keychain to check for correct installation in the Apple environment

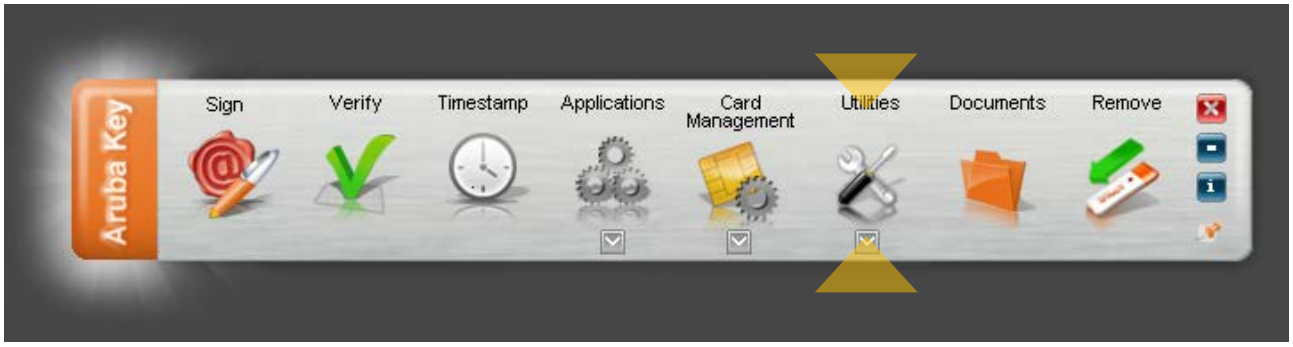


Copyright © Aruba Pec S.p.A. - All Rights Reserved

15 File encryption

Step 1

To encrypt a file select **“Utilities”.**



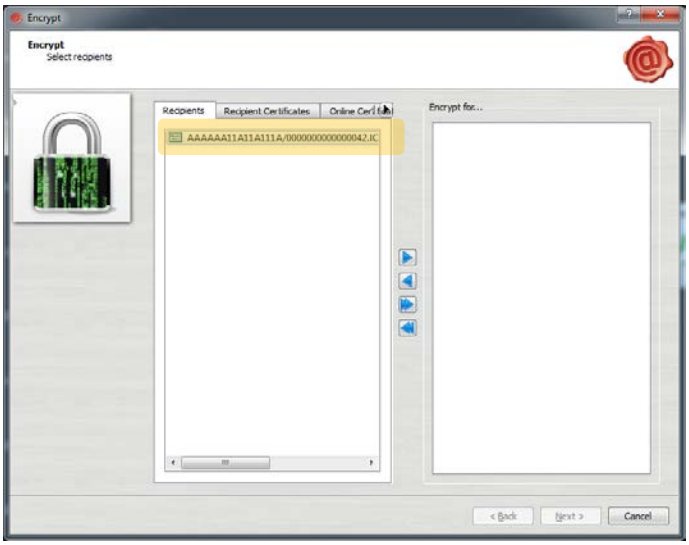
Step 2

Drag the file you wish to encrypt over the **“Encrypt”** icon.



Step 3

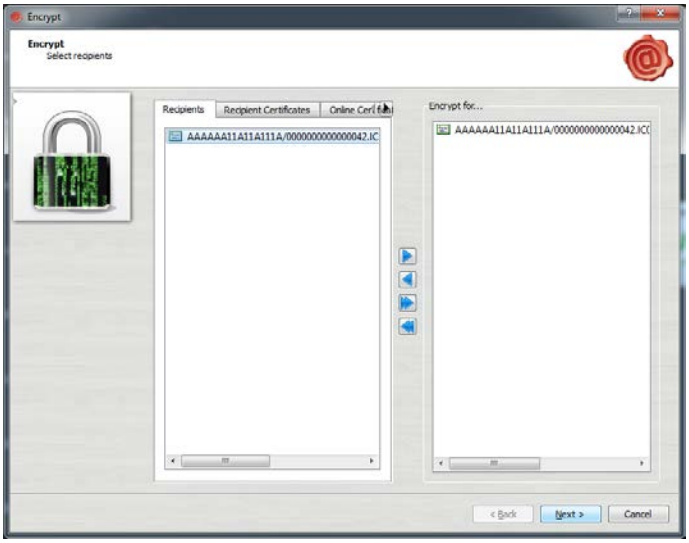
In the encryption window select, from the section on the left, the list of recipients of the encryoted file and click on “**Add**”.



Copyright © Aruba Pec S.p.A. - All Rights Reserved

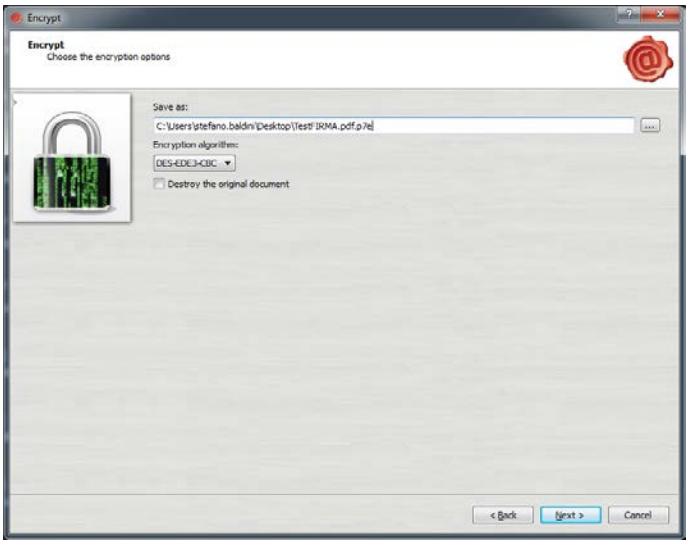
Step 4

Click on "**Next**".



Step 5

Select the folder where you wish to save the coded file and click on "**Next**".



NOTES:

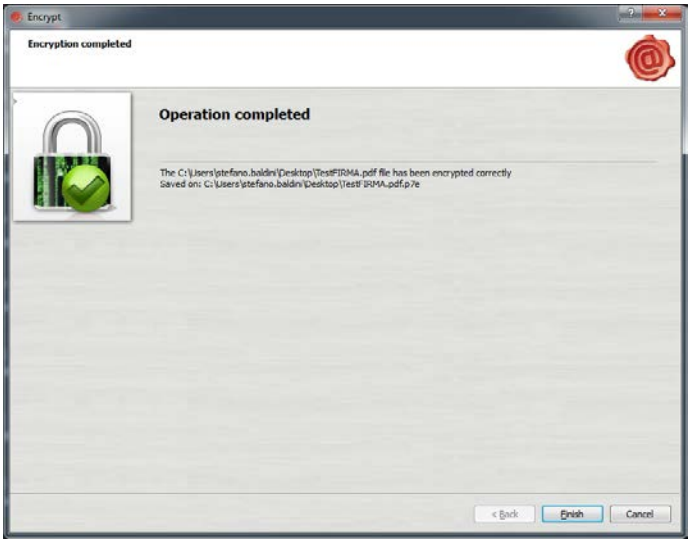
- *If you select multiple certificates for the coding of files, you will end up with one single file that is decryptable by each owner of the selected certificates.*
- *During the file encryption process the Aruba key automatically indicates, in the "recipients" area, its authentication certificate, that which is found in the SIM plugged in the Aruba Key.*

Copyright © Aruba Pec S.p.A. - All Rights Reserved

Step 6

After completing the process the following page will appear, click on **“Finish”**.

NOTE: The encrypted file generated by the process will have the additional “.p7e” extension and will include the original file.

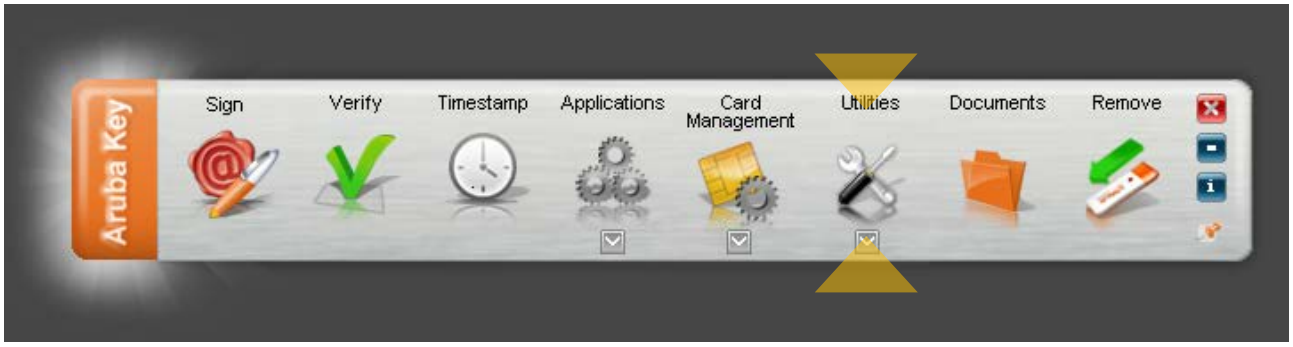


Copyright © Aruba Pec S.p.A. - All Rights Reserved

16 File decryption

Step 1

To decrypt a file select "**Utilities"**.



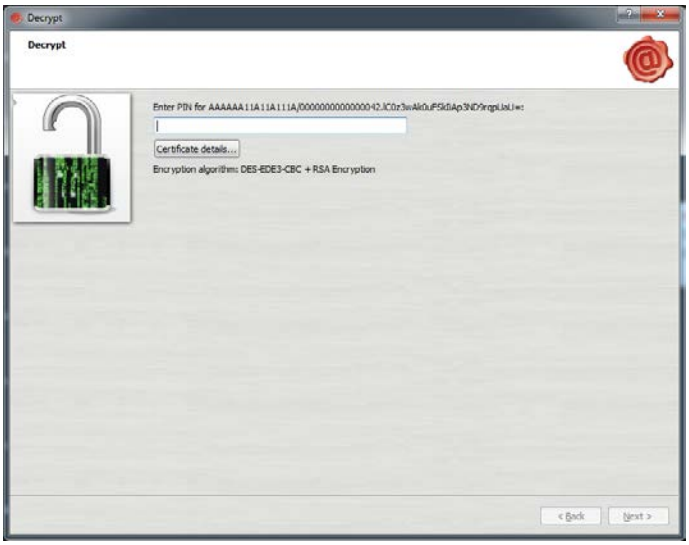
Step 2

Drag the **".p7e"** file over the **"Decrypt"** icon.



Step 3

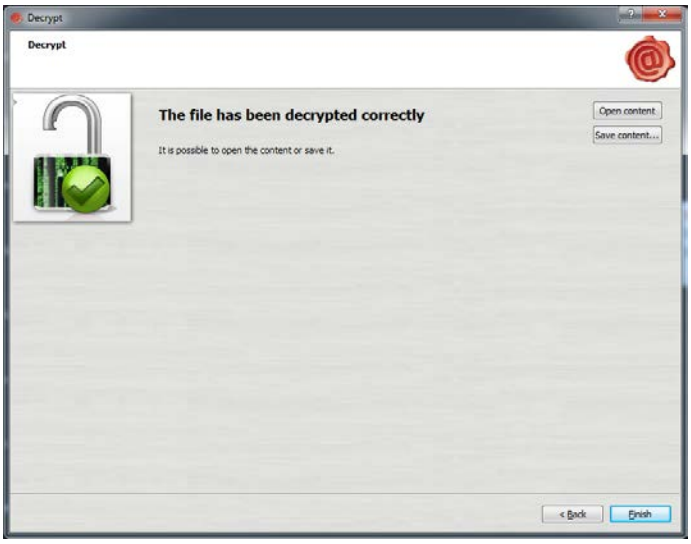
The Aruba key will verify that the SIM contains at least one of the certificates indicated during the encryption process.
At this stage you will need to enter the PIN code of the SIM plugged in the Arubakey.



Copyright © Aruba Pec S.p.A. - All Rights Reserved

Step 4

The Arubakey, after completing the decryption process of the file, will ask if the user wishes to open it or save it.



Copyright © Aruba Pec S.p.A. - All Rights Reserved

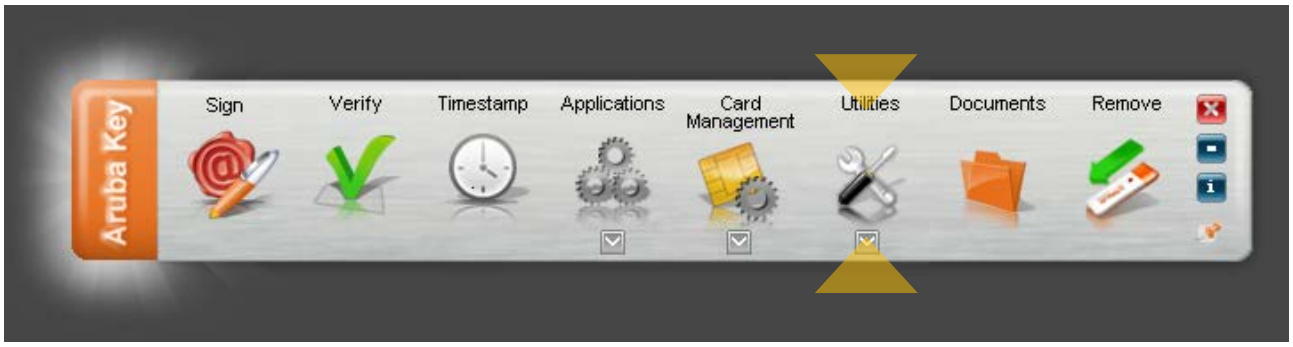
17 Options

17.1 Proxy settings

To use the Aruba key in a network protected by Proxy, follow these steps:

Step 1

Select the "**Utilities"** icon.



Step 2

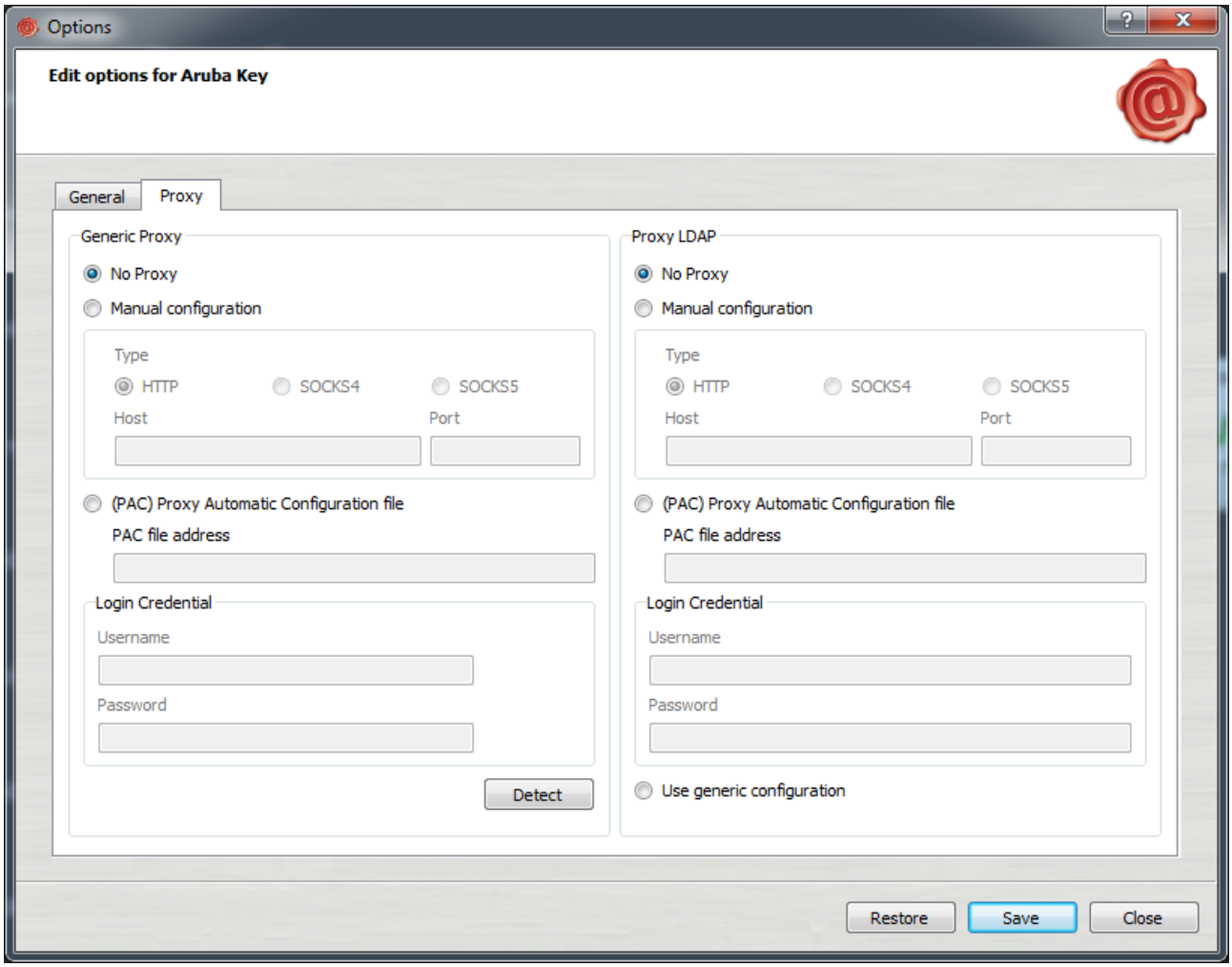
Click on "**Options and Proxy"**.



Copyright © Aruba Pec S.p.A. - All Rights Reserved

Step 3

Proceed with the configuration of the Proxy (HTTP/LDAP) section



For each configuration (generic Proxy and LDAP Proxy) it is possible to select the following options:

- **No proxy**: if selected no proxy is used;
- **Manual configuration**: if selected the proxy specified by 'Type', 'Host' and 'Port' is used;
- **Auto-configuration (PAC)**: if selected you need to specify a valid address for the proxy auto-configuration (PAC) file in the 'PAC file address' field.
  The address can be entered in the format *http://address/to/file* or *file://path/to/file*. Such file is used to determine the address of the proxy that will be used (or if not to use the proxy) for a specific address.
  NOTE 1: This option is not currently available in the Macosx and Linux distributions.

The access credentials specify the user name and password which should be used for the proxy authentication.
If not specified on Windows operating systems, the system will use, if possible, the credentials of the user that is currently logged in the system. If however, the credentials are not valid for the currently used proxy, each application will request the credentials when required.

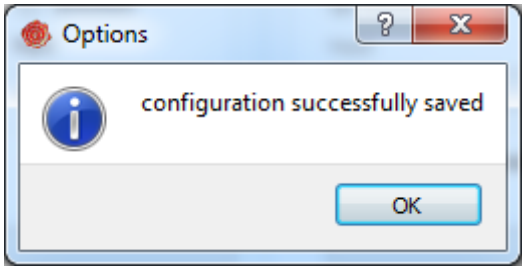
For the 'Proxy LDAP' configuration it is also possible to select the **Use generic configuration** option so that for the LDAP addresses the same configuration specified in 'Generic Proxy' will be used.

NOTE: If the details relevant to either the HTTP or LDAP section are not available (e.g. because the network does not support both configurations), proceed only with the section relevant to the supported type of Proxy.

Copyright © Aruba Pec S.p.A. - All Rights Reserved

Step 4

If the configuration has been saved correctly the following window will appear.

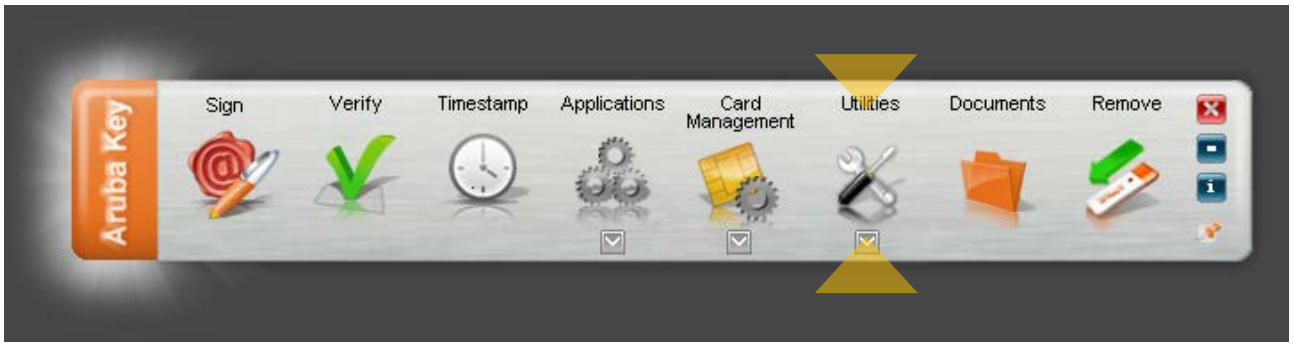


17.2 Language settings

To change the Aruba key language, follow these steps:

Step 1

Select the "**Utilities"** icon.



Step 2

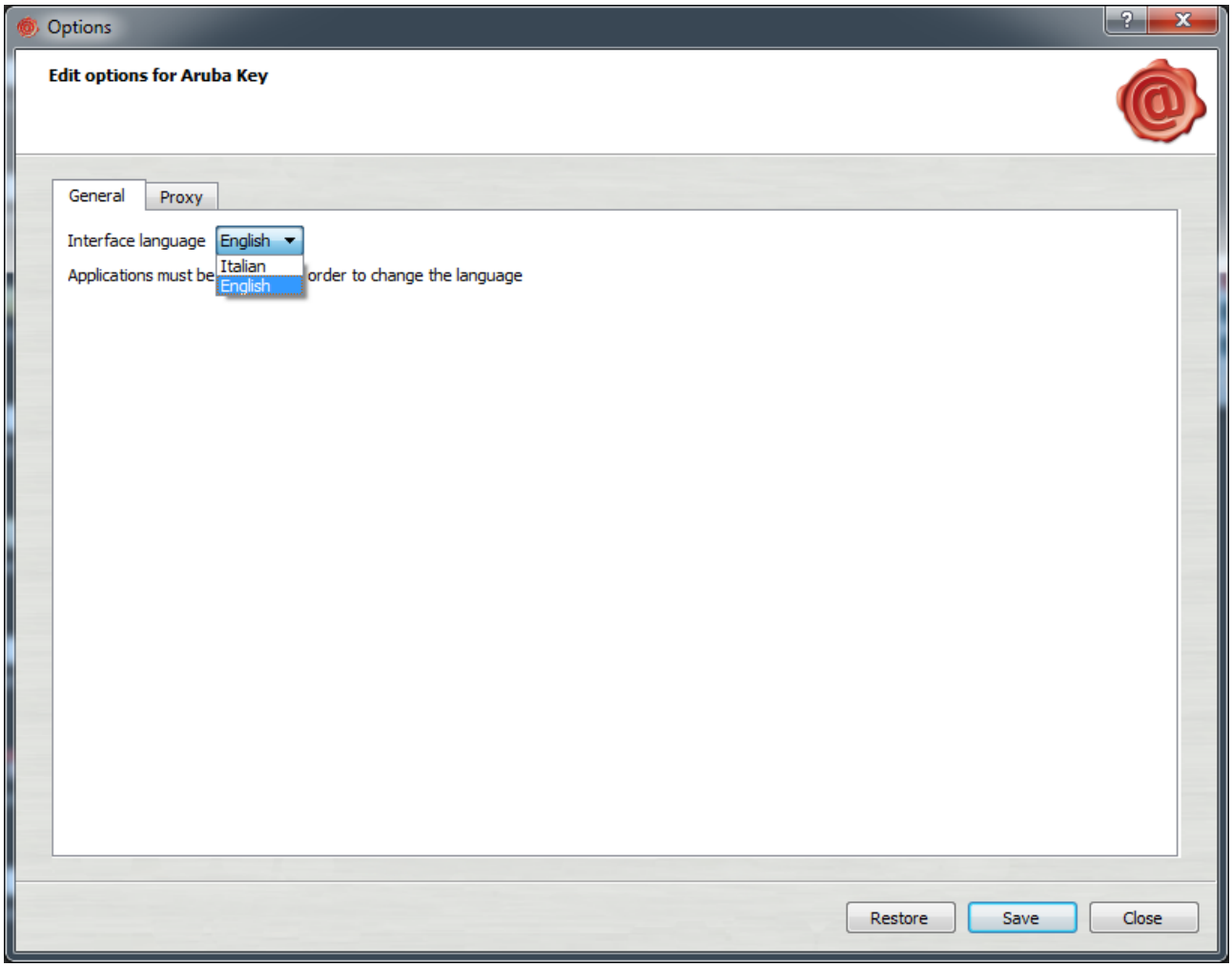
Click on "**Options and Proxy"**.



Step 3

Proceed with the configuration of the preffered Language

Copyright © Aruba Pec S.p.A. - All Rights Reserved



NOTE: Once you've changed the language settings you need to restart the Aruba Key software to activate them.

NOTE 2: In this version of the software the language settings do not apply to these applications:

- Firefox portable
- Thuderbird portable
- Filezilla portable
- AbiWord portable
- 7Zip

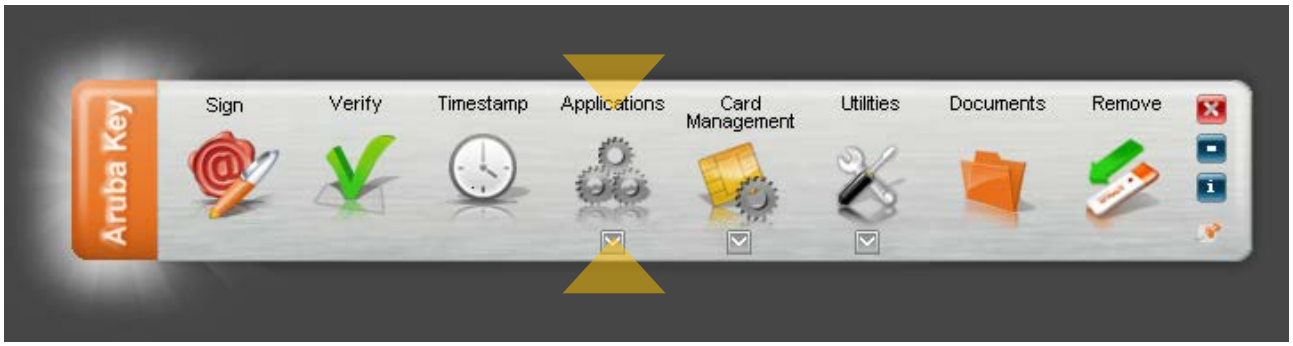
To retrieve the full English version of the Aruba Key software you need to, for the moment, format the device and download the archive from: https://ca.arubapec.it/downloads/AK_EN_VERSION.zip.

Copyright © Aruba Pec S.p.A. - All Rights Reserved

18 Display of certificates on FireFox Portable.

Step 1

To access the **"Mozilla FireFox Portable Edition**" found in the Aruba Key click on the **"Applications"** icon.



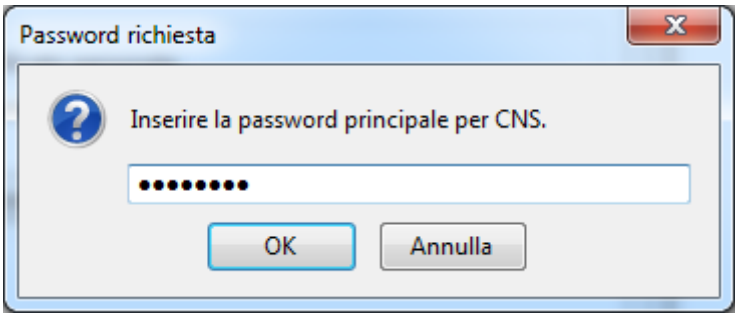
Step 2

Click on **"Firefox".**



Step 3

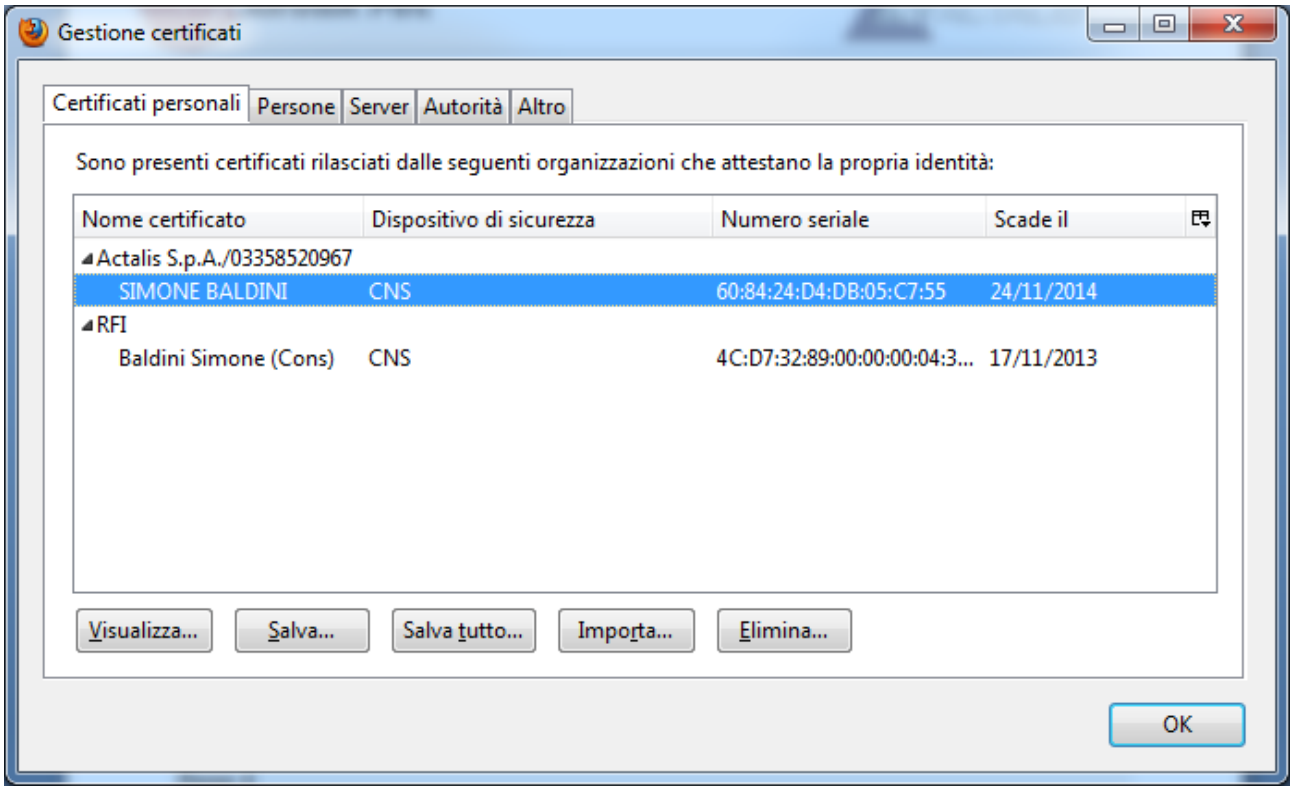
Select Tools → Options → Advanced → Coding → **"Show Certificates"** and enter the PIN when requested



Step 4

Copyright © Aruba Pec S.p.A. - All Rights Reserved

Your certificates, found in the Arubakey, are displayed in the 'Personal certificates' tab



ATTENTION: Should the Qualified and authentication certificates be imported in the Mozilla FireFox Store you must not click on the " Delete.." button. This could cause the certificates to be deleted from the smartcard and not be recuperated.

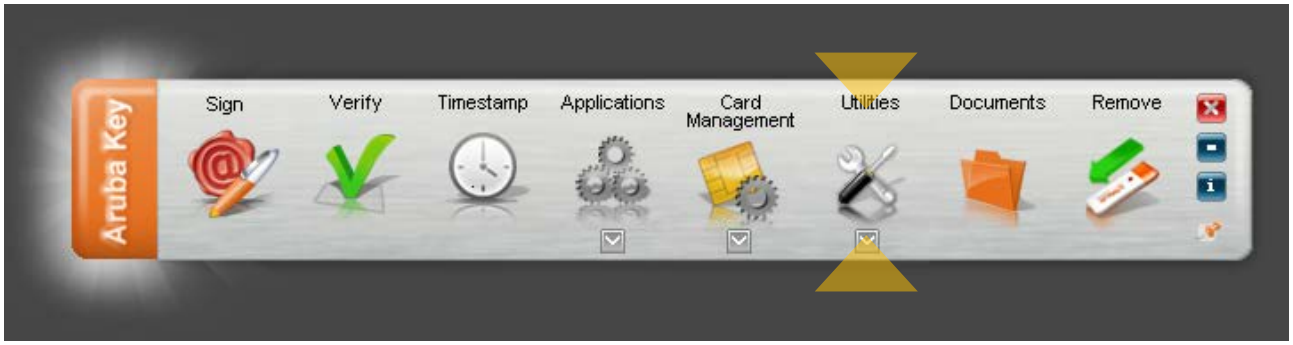
Copyright © Aruba Pec S.p.A. - All Rights Reserved

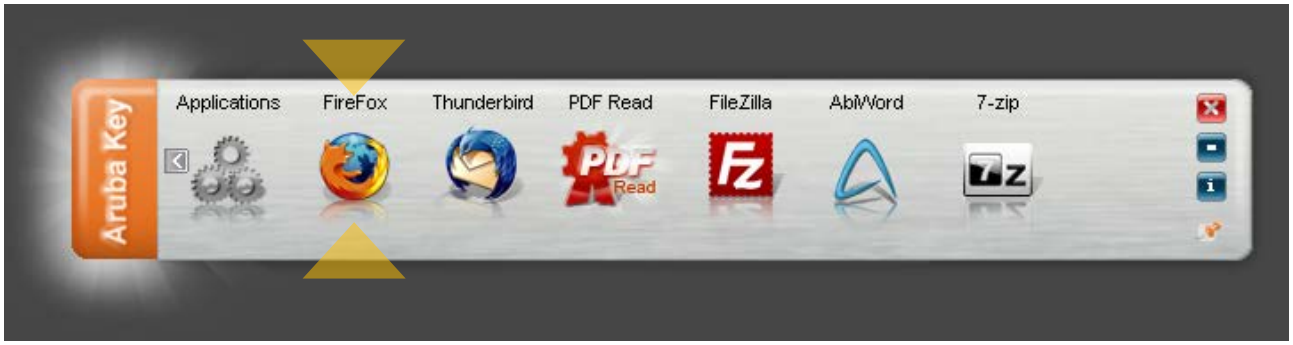
19 Uploading process of ACTALIS certificate

In general the smart card already includes the qualified certificate. There is however the possibility, **if the Aruba Key has been purchased from the Actalis system**, that the smart card is provided without any certificates. The owner must then follow the process below to upload the certificates and get the Aruba Key running.
In this case the owner, following or during the identification process made by a Registration Authority, will receive a closed envelope with a **Personal Private Code** (called **CRP** code).
To upload the certificate you need to follow the steps below.

Step 1

Access the "Mozilla FireFox Portable Edition" found in the Aruba Key by clicking on the **"Applications"** icon and then on the "**Firefox"** icon.





Copyright © Aruba Pec S.p.A. - All Rights Reserved

Step 2

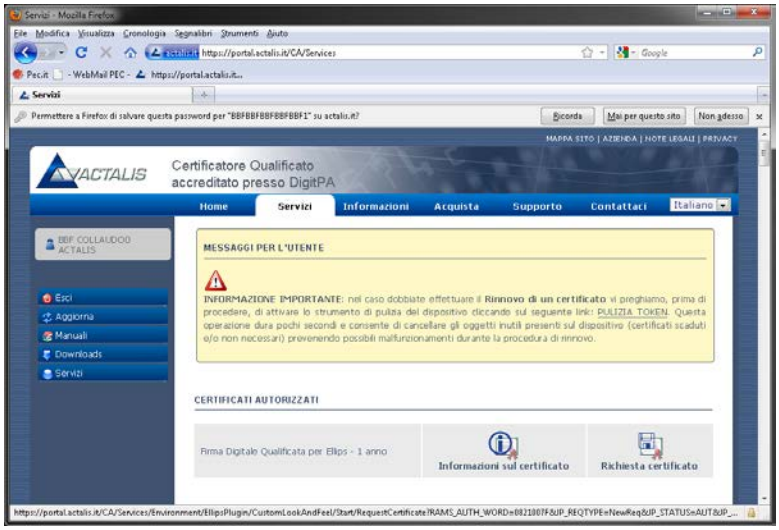
Go to https://portal.actalis.it



In the **"CUSTOMERS LOGIN"** section, found in the top left corner, type in the **National Identification Number** of the owner in capital letters and the **CRP code** received during the identification process of the owner. Then click on "**LOGIN**".

Step 3

You will then reach the page where you will find the **"AUTHORIZED CERTIFICATES"** for the owner. Click on "**Request certificate".**

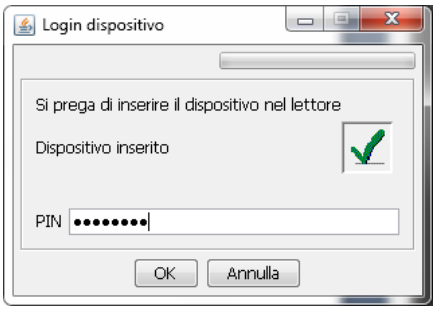


An automatic process will begin which asks the owner to enter the PIN code to access the device.

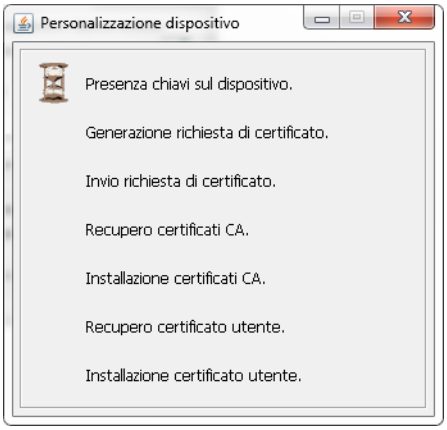
Copyright © Aruba Pec S.p.A. - All Rights Reserved

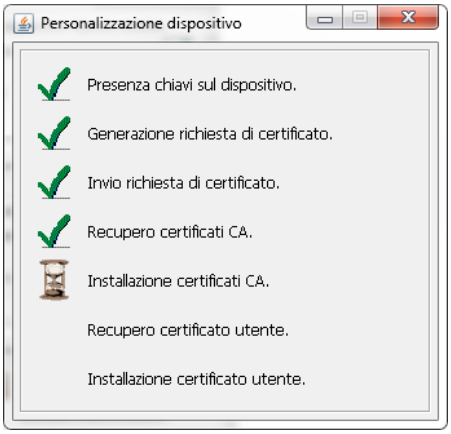
Step 4

Enter the PIN code you received with the Aruba Key and click on "**OK**".

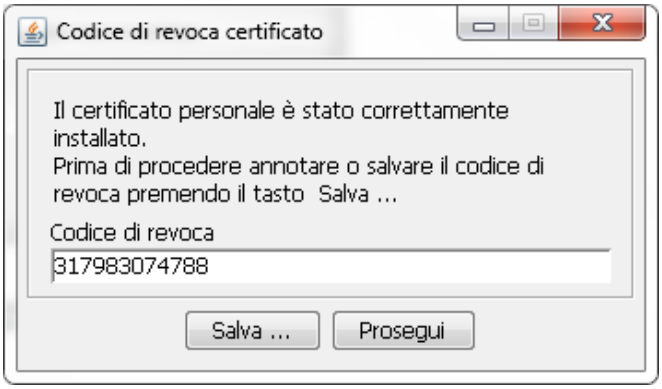


The system will perform the required steps to get the certificate.





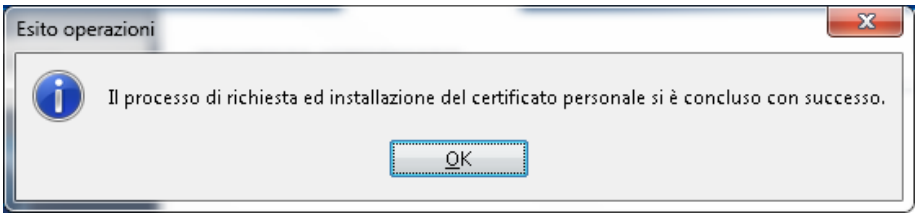
After completing the process you will get a **Revocation Code**, which can be used by the owner should he/she wish to invalidate the certificate. Such operation can be performed by connecting to the same portal again.

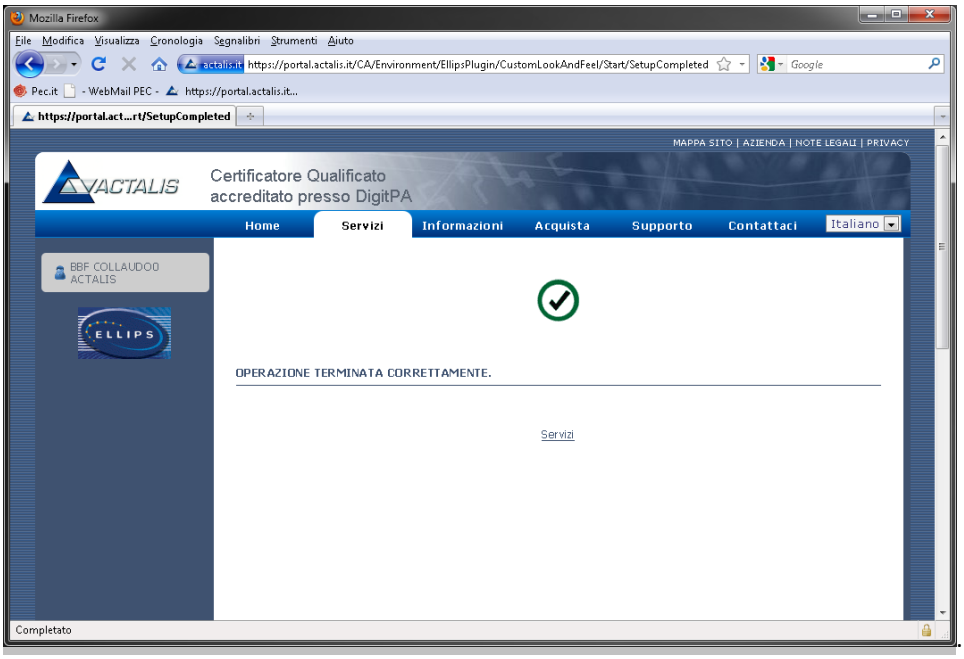


The code can be saved by clicking on "**Save**".

The system then informs you if the certificate uploading process has been successful.

Copyright © Aruba Pec S.p.A. - All Rights Reserved





The process has been completed and the owner can close the browser and operate all the Aruba Key functions.

Copyright © Aruba Pec S.p.A. - All Rights Reserved