

Registration Authority

Handbook FirmaCerta for Windows

Category	TSP-Firma Digitale	Document ID	NAM-User Guide	Namirial S.p.A.
Written by	Michelangelo Bonvini	Confidentiality note	Public Document	Registration Authority
Verified by	Gabriele Bocchini	Version	1.0	Gabriele Bocchini
Approved by	Gabriele Bocchini	Issue date	01/02/2019	<hr/>



– This page is intentionally left blank –



INDEX

Index	3
Revision History	7
1 Introduction	8
1.1 Document Purpose and field of application.....	8
1.2 Definitions and Acronyms used in this document.....	8
2 Installation	10
3 Graphic interface.....	12
4 Main Functions	12
4.1 Signature:	12
4.1.1 Signature.....	13
4.1.2 Countersign.....	13
1.1 Sign and time stamp.....	13
1.2 Verify	13
1.3 Timestamp	14
1.4 Device Manager.....	14
4.1.3 Change Pin	14
4.1.4 Unlock Pin	15
4.1.5 Change PUK	15
4.1.6 View Certificates.....	16
4.1.7 Device Check.....	17
4.1.8 Certificates Renewal	17
4.2 Graphometric Signature.....	17
4.2.1 Sign Document.....	18
4.2.2 Signatures Template	18



4.3	Utility.....	21
4.3.1	Encrypt and Decrypt.....	21
4.3.2	General Options	21
4.3.3	Proxy and Connections	24
4.3.4	Signature Options	25
4.3.5	Verify	26
4.3.6	Graphometric Signature options.....	27
4.3.7	Timestamp Options	29
4.4	Help.....	29
5	Appendix A: How to sign and countersign	31
5.1	How to sign a document	31
5.1.1	Sign in CADES - XAdES.....	31
5.1.2	Sign in PAdES	32
5.2	How to Countersign.....	35
6	Appendix B: How to timestamp a file.....	38
6.1	Configuration of Timestamp Parameters.....	38
6.2	How to Sign and Timestamp.....	39
6.3	How to Separate the timestamp	40
6.3.1	How to Sign a file in .p7m	40
6.3.2	How to timestamp a Signed file .p7m	41
6.3.3	Separate the Timestamp	43
7	Appendix C: How to verify and View a file	45
7.1	How to automatically set the launch of verification of signatures	46
7.2	How to view a signed file	46
8	Appendix D: How to Encrypt and Decrypt a file	47



8.1	How to Encrypt a File	47
8.2	How to decrypt a file	47
9	Appendix F: Command Line	49
9.1	Commands and Parameters	49
9.2	Examples:	49
10	Appendix G: Advanced Features	50
10.1	Signature of more document	50
10.2	Multiple Document Timestamp	50
10.3	Sign and Timestamp more documents	51
11	Appendix H: Certificate Renewal	52
11.1	Proxy Configuration	52
11.2	Methods of Renewal: Smartcard and token	53
11.3	Methods of Renewal: Automatic and remote certificates	55
12	Appendix I: Setting up Remote Signature	57
12.1	Introduction to Namirial Otp app	57
12.1.1	How to open it	57
12.1.2	Namirial OTP configuration	57
12.1.3	Android	58
12.1.4	iOS	58
12.2	Enabling Namirial SignEngine Service	59
12.3	How to sign a document	60
12.3.1	Username	61
12.3.2	Remote Device selection	62
12.3.3	Sign in PAdES format	63
12.4	OTP SMS procedure	64



12.5	Mobile OTP procedure: namirial OTP.....	65
12.6	OTP Hardware procedure.....	66
12.6.1	OTP activation.....	66
13	web Authentication.....	68
14	Appendice J: Bit4id – Linux.....	68
14.1	Change PIN.....	69
14.2	Unlock PIN.....	70
14.3	Change PUK.....	70
15	Appendice K: Bit4id – MacOS	71
15.1	Change PIN.....	72
15.2	Unlock PIN.....	72
15.3	Change PUK.....	73
References.....		73
Tables Index.....		74
Figures Index		74



REVISION HISTORY

VERSION	<version>
Date	01/02/2019
Reasons	First document issue with new functionality
Modifications	---



1 INTRODUCTION

Into Italian law system the term DIGITAL SIGNATURE refers to a type of qualified electronic signature which ascribes full evidential value comparable, substantively, to an original signature. As well as the signature on a paper document the digital signature can be placed in an electronic document.

The technology behind the digital signature ensures, moreover, that the signed document cannot be modified without invalidating the same signature, and gives the possibility to assign to the document a certain date and time through the timestamp mechanism.

FirmaCerta is the ideal tool to sign at the same time large volumes of digital documents such as invoices, insurance policies, receipts, payments, transfers, and any other digital document;

It makes possible:

- The signature of the documents keeping the original format (.PDF or .XML after being signed by maintaining the same format);
- The possibility to choose the hardware device you want to use to put the signature (Smart Card – Token – remote signature);
- The possibility to put / associate a timestamp to a document or a signature (graphometric);
- It enables drag and drop one or more files within the same signature box;
- Allows the signature of PDF documents protected by password.

1.1 DOCUMENT PURPOSE AND FIELD OF APPLICATION

This document, identified by the code shown in the title, describes the steps to follow to install the Client FirmaCerta and bit4id drivers for the recognition of the certificates; it describes also the functions of the Client FirmaCerta which is a software for managing digital signatures and personal timestamps.

A signed document cannot be modified by the software used to create it. In any case, if it would be possible, for the principles of asymmetric cryptography there can no longer be correspondence between the contents of the document and its associated signatures, FirmaCerta during the verification operation of the document will fail.

1.2 DEFINITIONS AND ACRONYMS USED IN THIS DOCUMENT

TERM	MEANING
Digital signature	It is a particular type of qualified electronic signature and represents the set of data in electronic form, attached or connected via logical association with other electronic data, used as a method of electronic identification.
Time Stamp (timestamp)	Is a sequence of characters that represents a date and / or time to assure the real occurrence of a certain event. The date is usually presented in a compatible format, so it will be easy to compare with another to determine the temporal order. The practical application is called timestamping. A marked file extension has temporally .m7m
Graphometric Signature	It is an electronic signature realized according to a process that is able to assemble to an electronic document a set of data obtained by sampling a common signature
PDF: (Portable Document Format)	Graphics file format developed by Adobe Systems. This standard is normally used to make available representative documents, printed pages of books, magazines, brochures, catalogs, price lists, etc. and for all those documents for which is important to preserve the graphic aspect. The pages visible on the screen may usually be (but not always) printed but not changed using Acrobat Reader, which is a free application used to read PDF documents.
XML: (Extensible Markup Language)	It is a metalanguage for the definition of markup languages based on a syntactic mechanism to define and control the meaning of the elements contained in a document or in a text.



Smart Card	It is a hardware device similar to a credit card that has potential for processing and storing high-security data.
USB Token	It is a usb key that includes a similar chip to that of a smart card and it is put directly into a USB port: thus have the same smart card functions with the same chip, drivers and bundled software but do not require a reader having a connection direct to your PC via USB port.
Drag and Drop	Drag and Drop. Technique that enables to transfer files from one point to another inside a program by a simple drag, holding down the left mouse button (drag: drag - drop: fall).
PIN	(Personal Identification Number) unique code to identify a user.
Electronic signature	For electronic signature law means a set of data in electronic form, attached or connected via logical association with other electronic data, used as the computer identification method.
Tool	Instrument, tool.
Template	Shape. It is a pre-designed template that allow composing a letter, creating a small file etc., much faster and easier.
Adobe	It is an application developed by Adobe Systems to create and edit PDF files. Adobe Acrobat, as produced by the same company that developed the PDF, was the first program which can process this format.
screenshot	This term refers to an image, or a portion of an image, "captured" from the screen (screen).
Label	Label, Mark
.bmp	Bitmap File. It is the official graphics format for Windows (see Bitmap)
Bitmap	Literally: "bitmap". graphic format (raster), among the most popular, supported by all applications. It allows storing an image without loss of information. Some typical bitmap file extensions are .BMP, .GIF, .JPG, .PNG, .TIFF.
Base64	It is a positional numbering system which uses 64 symbols. It is mostly used as encoding binary data in emails, to convert the data in ASCII format. The Base64 encoding causes an overall increase of 33% of the volume of data to be decoded.
PDF / A	International Standard (ISO19005), subset of the PDF standard, specifically designed for long-term archiving of electronic documents that need to be always displayed in the same way, even after a long time and with different software programs.
Proxy	Local network protection system from access by other Internet users. The proxy server acts as a security barrier between internal network and Internet, preventing other users access to confidential information of the internal network. The server also greatly reduces network traffic storing locally cached documents frequently used.
Add-on	Accessory. In hardware environment can represent any external "device" (modem, scanner, mouse, monitor, etc.) to be added to the computer, in the software environment, however, it refers to a module which adds or extends the capabilities of a certain base program's functionality.

Table 1 - Definitions and Acronyms

Table 1: Definitions and Acronyms



2 INSTALLATION

Download the software from the site www.firmacerta.it section Download > Software Firmacerta > Desktop Version for Windows (LINK).

And proceed with the wizard.



Figure 1 - Wizard firmacerta

After confirming the copyright laws of the software the installation will propose the default user folder.

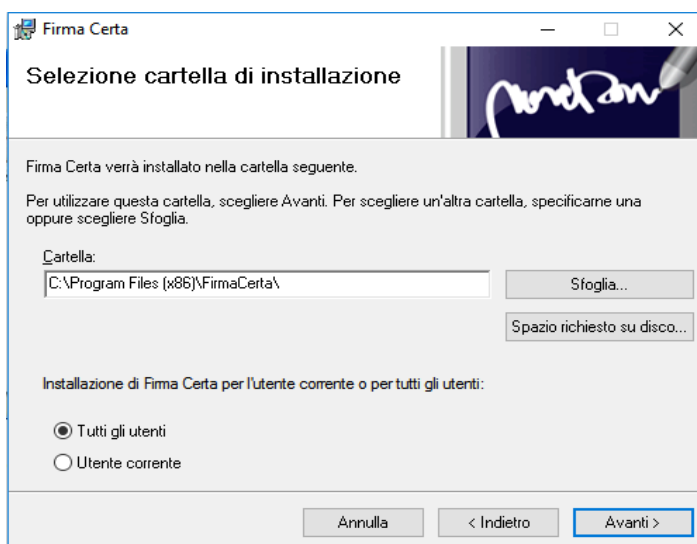


Figure 2 -Select the destination folder

ATTENTION: to modify the destination folder make sure to have the necessary permission or ask your system administrator support.



Press forward to start the installation.

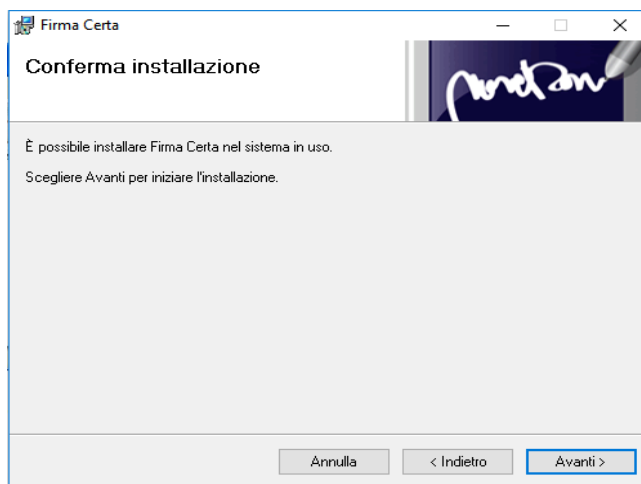


Figure 3 -Installation confirmation

Wait until installation has been completed.

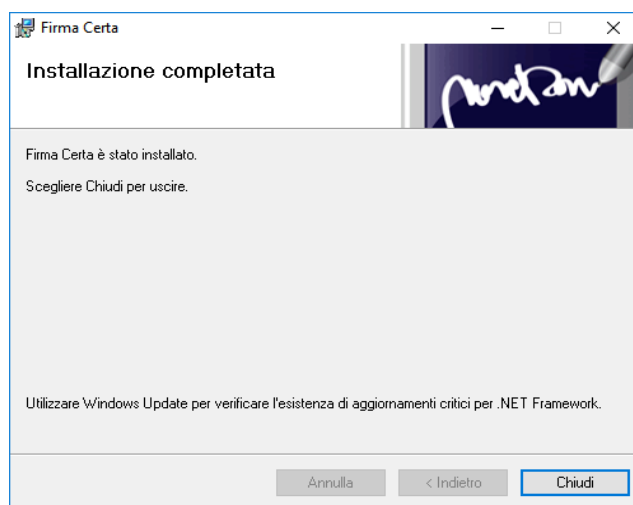


Figure 4 - Successful installation message



3 GRAPHIC INTERFACE

FirmaCerta graphic interface is simple and intuitive.
The menu is made up of the main functions of software:

- Digitally sign any files;
- Affix Timestamp;
- Use the Graphometric Signature;
- View and Verify digitally signed files;

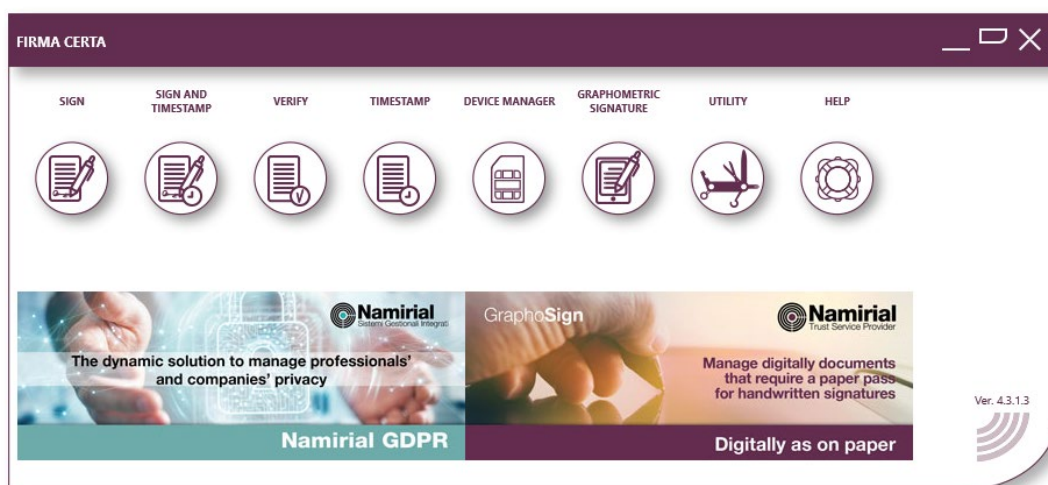


Figure 5 - FirmaCerta Graphical Interface

4 MAIN FUNCTIONS

4.1 SIGNATURE:

Clicking on the icon Sign you will choose if sign or countersign the file

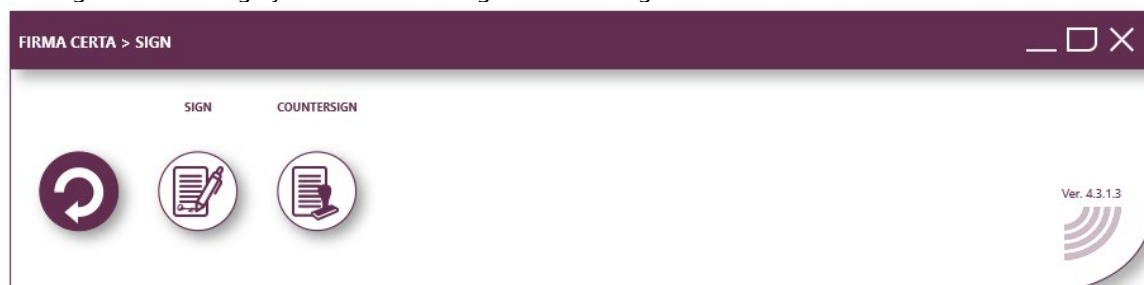


Figure 6 - Sub-menu of signature



4.1.1 SIGNATURE

With FirmaCerta you can sign any document thanks to one of the following ways:


	Drag & Drop: Dragging (drag & drop) simultaneously one or more files inside the FirmaCerta Software window and clicking on the icon "Sign".
	From File: Clicking directly on the icon of the file/files to sign with the right mouse button, then selecting the item "Sign" inside the drop-down menu.
	From Software: Clicking on the icon Sign you can search, inside the folders of your computer, the file you want to sign.

Figure 7 - Introduction of the signature's function

Once you press "Sign" the software will ask you to choose the directory where you want to save the file/s signed and then the PIN of your signature device (Smart Card / Token Sim card).

- to view the whole procedure to sign a document Appendix A: How to sign a document
- to view the procedure for Remote Signature holders Appendix I: Remote Signature

4.1.2 COUNTERSIGN



With this function it is possible to countersign a signature already present in the document giving a kind of hierarchical validation.

After clicking on Countersign the software will require the destination folder to save the file countersigned, then a confirmation about the selected document to be signed and finally to enter the PIN of the signature device connected to the computer.

See the whole procedure to countersign a document Appendix A: How to countersign

Figure 8 - Introduction of countersignature function

1.1 SIGN AND TIME STAMP



Through this function is possible to sign and to mark temporally in a single operation one or more digital documents. The Signature client asks you to select the destination folder of the signed file. Once you press "Sign and Timestamp" and entering the PIN code the software will require to enter the credentials "User" and "Password" to use the time stamps.

See the whole procedure for Sign and Timestamp a document: Appendix B: How to Sign and Timestamp a document

Figure 9 - Introduction function signature and Brand

1.2 VERIFY



This function allows verifying and displaying the signature/signatures status on the document. The window Result will confirm the integrity, the reliability, the legal validity of the certificate and the verification of CRL and OCSP, that is the certificate is active. Furthermore, thanks to this function it's possible to open the window of the details that will show the main features of the certificate (Type, Issuer Entity, Owner, Certificate validity)

See the whole procedure to check a document: Appendix C: How to verify and view a file

Figure 10 - Introduction verification function



1.3 TIMESTAMP



After selecting a file, with this feature you can temporally mark the same file giving a certain date and time to the document, opposable against third parts.
Also for this operation you will be required to select a destination folder and to enter the PIN code of the signature device.

See the whole procedure to Mark a document: Appendix B: How to Mark a file

Figure 11 - Introduction of Brand function

1.4 DEVICE MANAGER

This function allows the user to access to signature device settings.



Figure 12 - The Device Management Panel

4.1.3 CHANGE PIN

It allows editing the current PIN code through the insertion of a new PIN (insertion and verification).
NB: The Remote Signature holders cannot change the PIN with FirmaCerta.

Figure 13 - Function Code Change




4.1.4 UNLOCK PIN

Function useful to unlock the PIN code, if locked. Enter the PUK code (8-digit code number) the user find in the blind envelope.

ATTENTION: To complete the procedure is mandatory to have the blind envelope provided after the issuance.

After 3 wrong writing PUK attempts the device will permanently be locked and it will be necessary to request a new signature device.

Unlock device

 Insert PUK and new PIN

PUK

New PIN

Confirm PIN

OK Cancel


Figure 14 - PIN Unlocking function

4.1.5 CHANGE PUK

It allows to modify the current PUK through the insertion of a new PUK (insertion and verification).

ATTENTION: for Remote Signature it is not possible to change the PUK.

Change PUK

 Insert old and new PUK

Old PUK

New PUK

Confirm PUK

OK Cancel

Figure 15 - Puk change function



4.1.6 VIEW CERTIFICATES



With this function is possible to export the certificates of the device in the following formats:

```
File certificato (*.der)
File certificato (*.pfx)
File certificato (*.spc)
File certificato (*.pem)
```

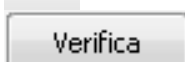
- DER:** It's simply a binary version of PEM format. The extension is .der but sometimes .cer; in this case the only way to distinguish the format is to open the file with an editor to see if is in ASCII or binary format. They are typically used in Java platform
- PFX:** The PKCS# 12 or PFX is a binary format that allows saving in encrypted form both the server certificate and the intermediate ones and the private key. The extension is usually .pfx or .p12. The PFX files are typically used on Windows machines to backup and for migration from one server certificates to another, with their respective private keys.
- SPC:** Most commonly format used by Certification Authorities to test
- PEM:** Most commonly format used by Certification Authorities to issue certificates, normally using conventional extensions .pem, .crt, and cer. They are ASCII files with Base64 encoding and contain "----- BEGIN CERTIFICATE -----" at the beginning and "----- END CERTIFICATE -----" at the end. They can be in PEM format for server certificates, private keys and intermediate certificates.



Pressing this button you will simply carry out a cancellation of the certificate lists recorded in the device from the active window (without removal from the device connected).



To accesses to check options, also accessible from Firmacerta menu > Utility.



Pressing this key is carried out the verification of the device's certificates. Clicking on the label Result and/or Details you can view the result of the check and the peculiarities of the selected certificate.

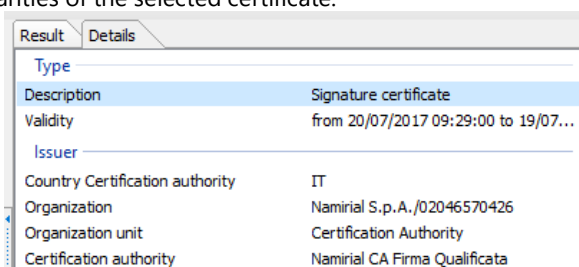
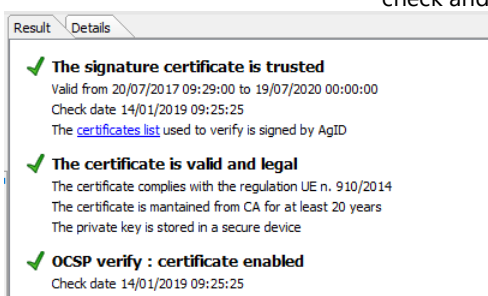


Figure 16 - Displays of Certified function



4.1.7 DEVICE CHECK

With this function you can carry out a test for the smart card reader, entering the device PIN code the user will be receive the informations about the hardware status (supposing that the device has been correctly activated).

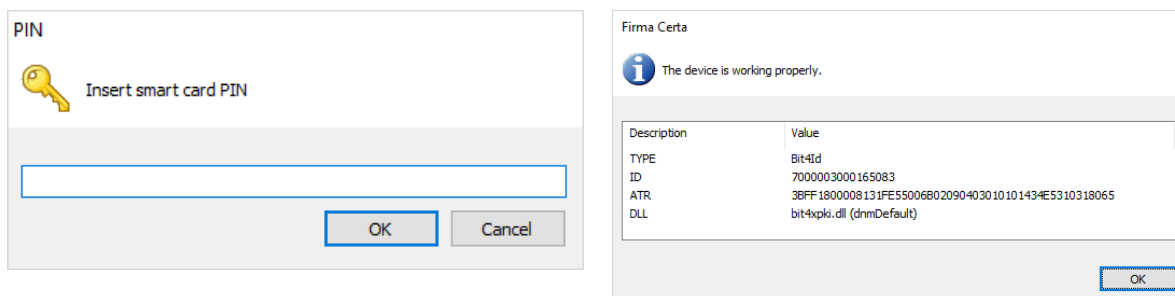


Figure 17 - Verification function device

4.1.8 CERTIFICATES RENEWAL

Function required to renew digital signature certificates for three years further.
Please, see the **guide** with the essential informations to carry out the renewal (View [Appendix H](#)).

ATTENTION:

1. If doesn't appear in the menu, download the software FirmaCerta Device Manager;
2. If the user has not been unlocked by RAO the renewal cannot be completed;
3. It's impossible renew the certificates for a second time.

Figure 18 - Introduction of certificates renewal's function

4.2 GRAPHOMETRIC SIGNATURE



The graphometric signature is an electronic signature realized according to a process able to associate to an electronic document a set of data obtained by sampling a common signature.

These data are obtained using a device that detects and digitalizes the graphical image of a signature to which generally are added, according to the characteristics of the device used, other biometric parameters such as pressure and speed of the graph trait. The device consists of a tablet able to show to the subscriber the document being signed, recreating an experience very similar to that of signing a paper document.



4.2.1 SIGN DOCUMENT



With this function you can load the .PDF file you want to sign with the graphometric signature.

4.2.2 SIGNATURES TEMPLATE



This tool allows creating different models to be used with the combination of PDF documents, during the actual graphometric signature phase. The templates allow, by selecting a specific document, to immediately detecting the signature fields highlight them on the tablet, without skim the PDF by the user. To understand how it works, it will use as example a generic document for vacation and permits request (fig. Below).

Click on "Signature Template", then FILE -> open -> select the .pdf you want to keep as parameter. In correspondence with the pointer will appear a yellow rectangle corresponding to the signature area, the surface can be increased or decreased by pressing the corresponding buttons on the toolbar (fig. Below).



Click with the left mouse button (or right) to save the first field of the template

Once the field has been selected, the following window will appear.

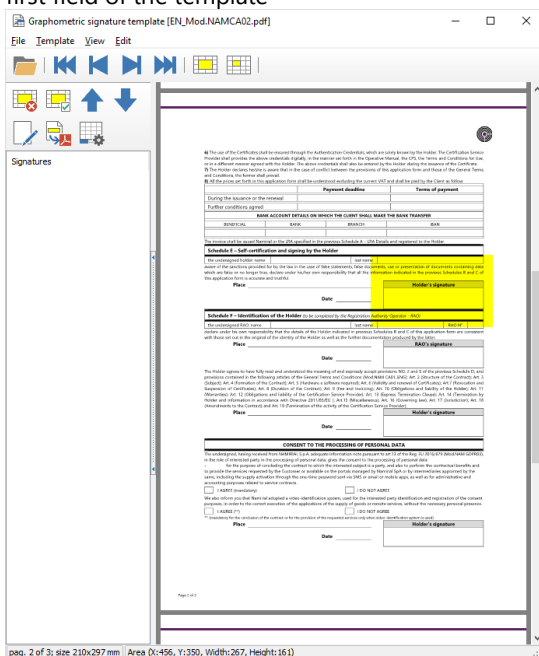
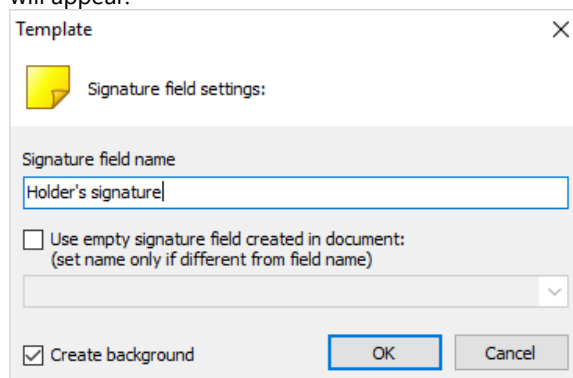


Figure 19 - Marker in the template





Use the empty signature field that is already present into the pdf

It detects any signature fields previously created on the document using Adobe Acrobat.

Create Background Image

Thanks to this feature it is possible to take a screenshot of the selected signature area that can be personalised and employed, with any kind of modifications done during the handwritten signature, in this way the user who is going to sign with the graphic tablet will see on the display not only the section corresponding to the selected area, but also the indications entered manually by the operator.

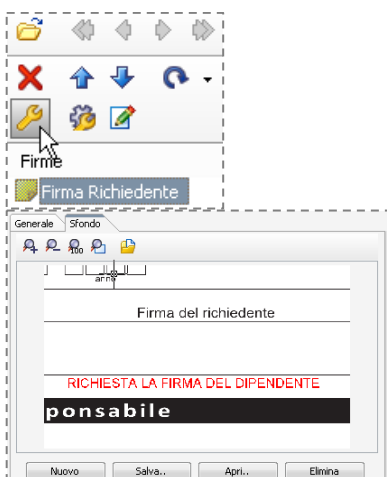
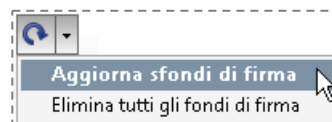


Figure 20 - Background Signature

To modify the background you need to access to the signature field property saved, clicking on the corresponding icon (img. at your side) and then move on the label Background.

Press the Save button to save the image in .bmp format. At this point it will be possible to edit the file with a graphic editor or use one already present in the operating system such as Paint. Once the changes have been completed simply recover the image inside the signature field using the Open button (img. at your side) and finally press OK to confirm the operation.

It's strongly advisable to save the bitmap of a template in the same folder because, after being modified, they can be updated inside the template with the function Update signature backgrounds.



Don't use background for the signature

The background saved will not be showed on the tablet display during the original signature

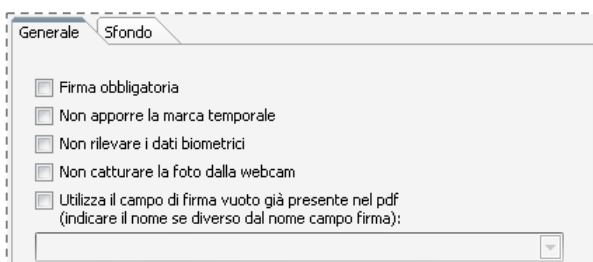


Figure 21 - General Signature Properties

In the General part of the Signature Properties the following options are included:

Obligatory Signature

It forces the user to draw an original signature on the tablet in the selected field, without allowing the possibility of proceeding to the next field or saving the document.

Don't put the timestamp

Through FirmaCerta Software is also possible to put the Timestamp on the whole document or for individual signatures contained in it, by selecting the specific check-box it will be possible not to put any timestamp on the selected signature field.



Don't detect biometric data

This feature prevents to detect from the signature the data of the signatory, by acquiring the only graphic hand.

Don't capture pictures from webcam

This function may be set if the PC is not equipped with a webcam or is not necessary to capture any image of the subject petitioner (in any case would be encrypted inside the document)

Figure 22 - Search keywords

Search key

Entering a word present in the document you want to sign or specifying exact coordinates you can create signature fields free of other parameters, that will appear to the signer during the signature procedure. For example, this function would have a great utility applying a label with a title on a .PDF model used as a template for other



This feature allow you to extend two important preferences (described above) to all signature fields saved in the template:

- Do not use the background for the signature
- Not capture pictures from webcam



4.3 UTILITY

This feature allows the user to access to the main settings of Firmacerta software.

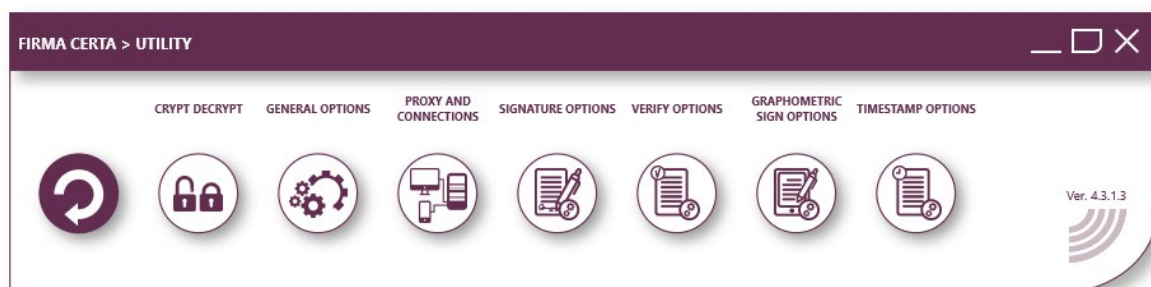


Figure 23 - Utility Panel

4.3.1 ENCRYPT AND DECRYPT



Is an application useful to encrypt files of all type and size, according to the current regulations and the technical standard references.

Very adaptable and easy to use, Firma Certa Protect is available for Windows.

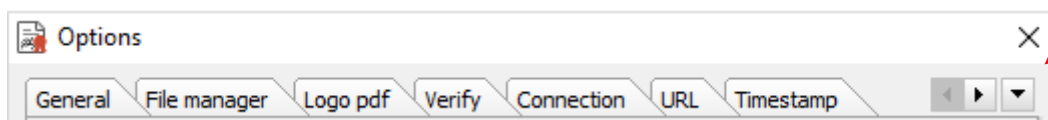
To use Firma Certa Protect, please consult the **guide** to find the basic informations (See [Appendix D](#)).

Figure 24 - Introduction to Protect FirmaCerta

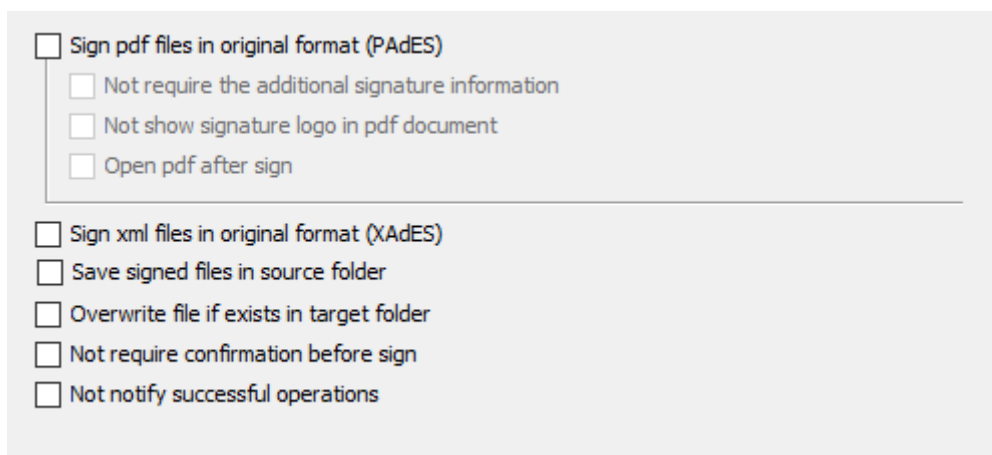
4.3.2 GENERAL OPTIONS

In this section you can manage Firmacerta software's settings.

Attention: using the arrows you can find in the upper right corner you can skim through the various profiles.



It is possible to do some operations to customise the signature.





Signature of pdf files maintaining the format (PAdES):

It keeps the original file format (otherwise converted into .p7m format), providing the ability to view documents even for a user with no specific digital signature software.

- **Do not request additional signature informations:**
- **Do not show the signature logo in PDF documents:**

Optional informations will not be displayed in the signed document;
Setting this preference before signing and then viewing the digitally signed PDF file, the signature logo with signer's information will not be reported.

NB: You can customise the logo through the corresponding setting **Logo pdf**, in absence of this kind of customisation the software will use a logo by default

- **Open the PDF after the signing process**

The PDF file will be opened with the default program of the computer after the application of the digital signature.

Signature of xml files maintaining the original format (XAdES):

It keeps the original file format providing the ability to view the document even for a user with no specific digital signature software.

Save signed files in the same folder of the original file:

It allows saving the signed file in the same directory as the original file is placed;

Overwrite files if already existing in the destination folder:

The message that inform about the presence of the original file will not be noticed;

Do not ask any confirmation before signing a file:

Avoids any confirm each time the signer make the signature of a document.

Do not notify the successful outcome of the operations:

The success message at the end of the procedure will not be shown.

[Attiva dispositivo di firma](#)
[Visualizza certificati contenuti nel dispositivo di firma](#)
[Verifica dispositivo di firma](#)
[Cambio PIN](#)
[Sblocca dispositivo di firma](#)
[Visualizza logo pdf](#)

Figure 25 - Panel General Options



4.3.2.1 FILE MANAGEMENT

Thanks to the following choices you can:

- use Firma Certa as default program to open digitally signed files (.p7m), timestamped files (.tsd, .tsr, .tst) and protected files (.p7e).
- encode digitally signed files (.p7m), timestamped files (.tsd, .tsr, .tst) and protected files (.p7e) in Base64 format.
- Create the file containing the stamp of a timestamped file.

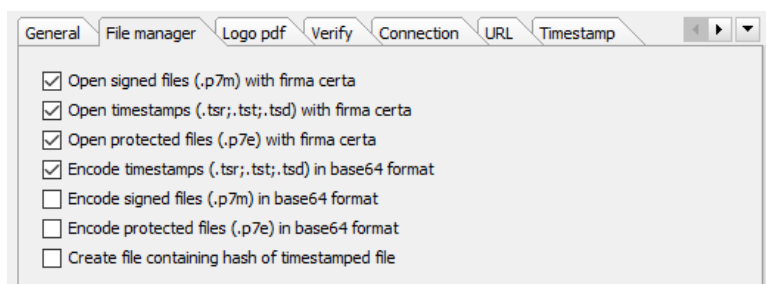


Figure 26 - Options: File Management

4.3.2.2 URL

Shows the address to which the software connects to download updates (it is strongly recommended not to change the default data).

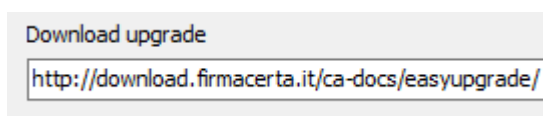


Figure 27 - Options: URL

4.3.2.3 WEB SERVICES

In this section you can enable the plug-in to use the Remote Signature service, selecting the service and clicking on Enabled/Disabled.

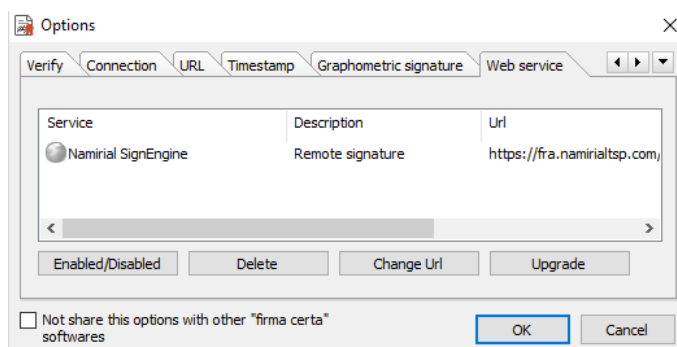


Figure 28 - Options Web Services



4.3.2.4 INFORMATION

Section in which you can check Firmacerta informations such as last software version, language set up, etc.

Attention: we strongly recommend to keep the software up to date, to ensure regulatory compliance and improvements.

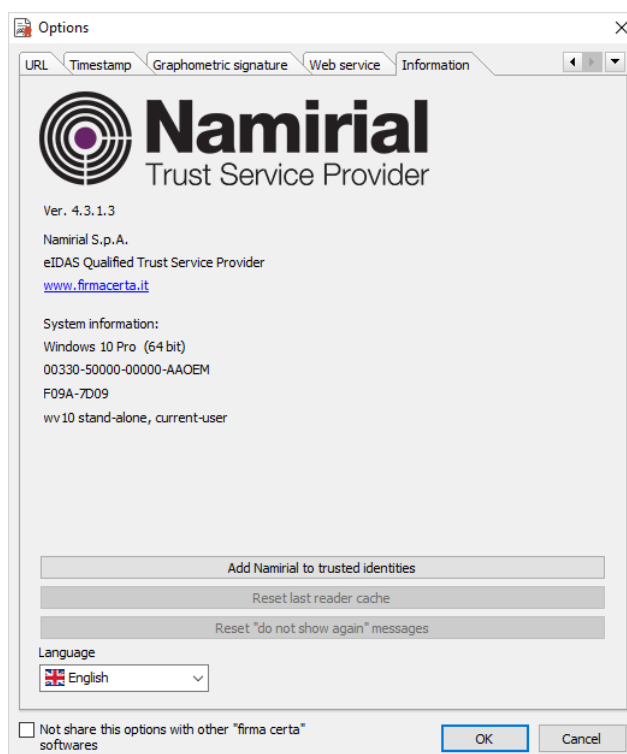


Figure 29 - Options Information

4.3.3 PROXY AND CONNECTIONS

This feature should be used only if Internet access for HTTP protocol is accessible via proxy server. The system allows setting the name, the port to join the web, and the ID and password for Internet access, of a FirmaCerta user.

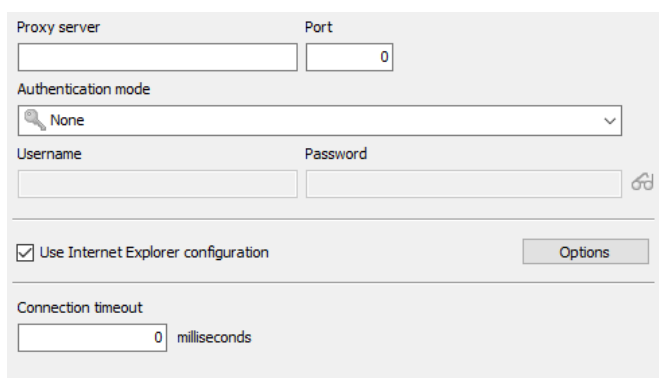


Figure 30 - Options: Configure Proxy



4.3.4 SIGNATURE OPTIONS



Figure 31 - Signature Options Panel

4.3.4.1 PDF LOGO

It allows you to change the default logo of Namirial and set up a personal logo in a PDF document, during the application of the signature in this kind of document.

You can set the transparency effect by selecting two different colors, customise the text to be applied over the logo, incorporate the font in the operating system for a greater compatibility with PDF/A.

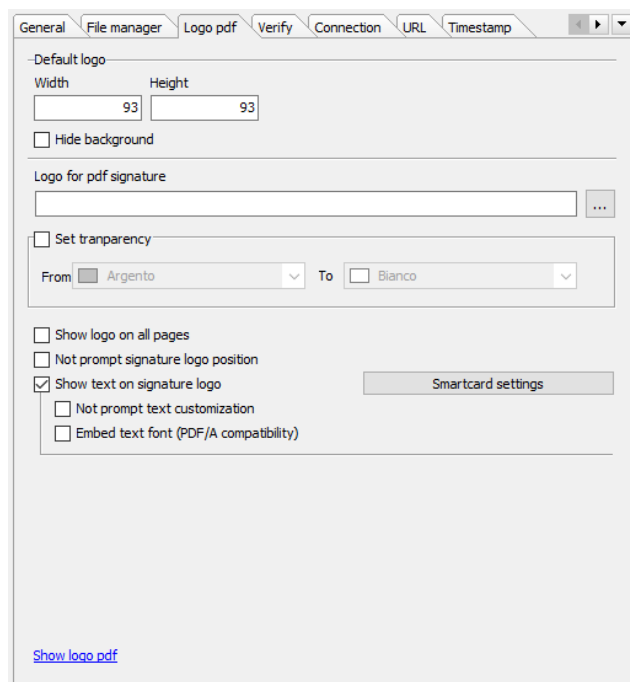


Figure 32 - Options: PDF Logo

4.3.5 VERIFY

To verify and display at the same time the certificate status (active/revoked/suspended) of a digitally signed file.

- ☒ Verify at startup
- ☐ Enabled cache for CRL verification
- ☐ Activate cache for TSL verify (expiry: 7 days)
- ☒ Verify certificates when signed document is open

Figure 33 - Options: Verification Options



4.3.6 GRAPHOMETRIC SIGNATURE OPTIONS

This feature allows the user to access to the Utilities referred to graphometric signature devices.



Figure 34 - Graphometric Signing Options Panel

4.3.6.1 OPTIONS

Within the preferences of graphometric signature you can use both one of the three Wacom tablet models in the drop-down menu and, alternatively, one of the certificated tablet for this operation (for more information visit www.firmagrafometrica.it section "Dispositivi Utilizzabili").

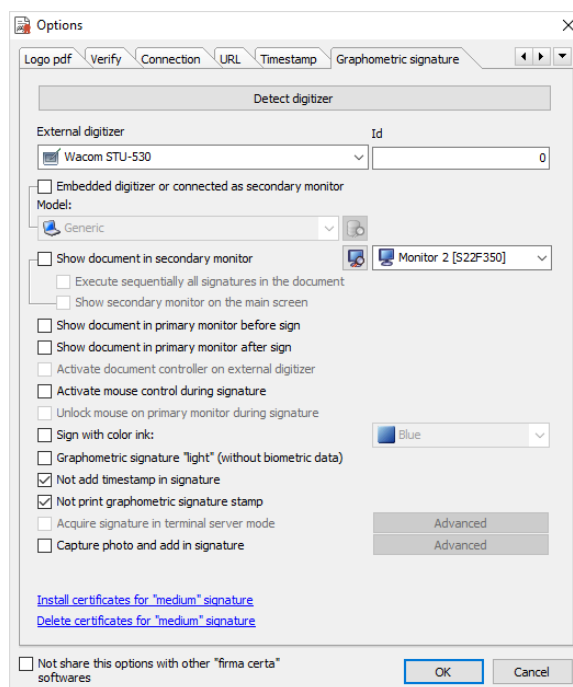


Figure 35 - Options Signature graphometric



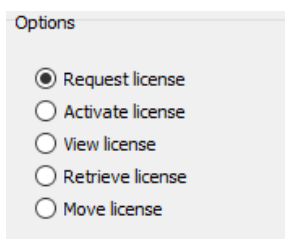
4.3.6.2 ACTIVATION

The user who want to activate the software receives by mail a technical encryption certificate that must be installed on the PC.

This certificate is required for the activation of graphometric signature license.

To request the activation of graphometric Signature function, proceed as follows:

Select the Request License option and press **Next**;



Options

- ☒ Request license
- ☐ Activate license
- ☐ View license
- ☐ Retrieve license
- ☐ Move license

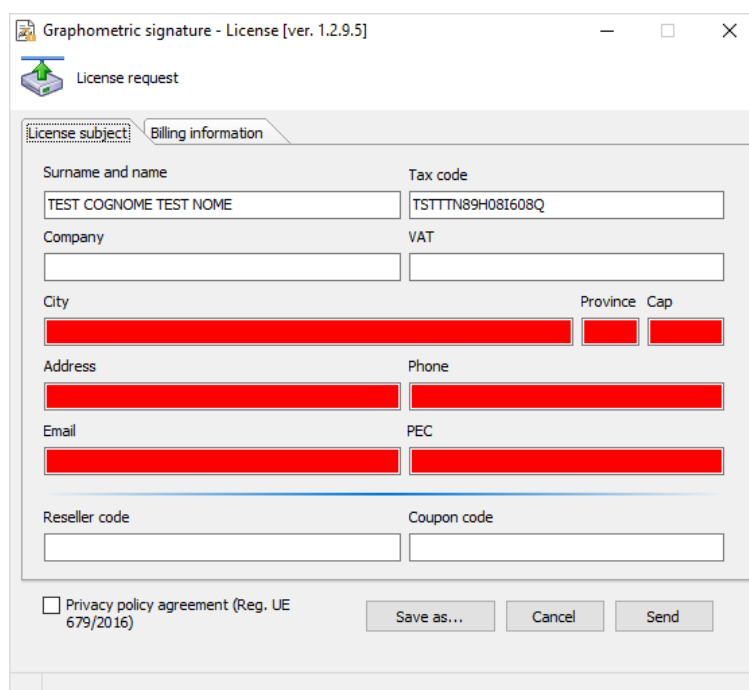
Press **Next**;



Device selection

Select device that you want to activate to graphometric signature and press "Next >"

Fill the fields with the license holder's data and press **Send**.



Graphometric signature - License [ver. 1.2.9.5]

License request

License subject: Billing information

Surname and name	Tax code	
TEST COGNOME TEST NOME	TSTTTN89H08I608Q	
Company	VAT	
City	Province	Cap
Address	Phone	
Email	PEC	
Reseller code	Coupon code	

☐ Privacy policy agreement (Reg. UE 679/2016)

Save as... Cancel Send

At the end of the procedure the CA Namirial will process the request and in a few hours will enable the digital device to Biometric Signature.

Figure 36 - Graphometric Options: License Activation



4.3.6.3 INFORMATIVE

The function allows the signer the compilation by to draft and sign with the graphometric signature an informative PDF document about the general operation of graphometric Signature and the processing of electronic documents in place of paper, using a digital device connected (graphics tablet or other hardware supported). To carry the operation out the petitioner will be required, after inserting the Tax code and Name in an initial window (fig. At side), using the procedures applied to graphometric signature and writing on the device the date and signature. If you will not allow to use this process by accessing this menu this kind of request will be show to the signer during the first signature operation.

The dialog box titled "Firma Certa - Documents" contains a PDF icon and the text "Subject information". It has four input fields: "Tax code" (highlighted with a red border), "Surname and name", "City of birth", and "Date of birth" (a date picker). At the bottom are "OK" and "Cancel" buttons.

Figure 37 - Graphometric Options: Information Privacy

4.3.7 TIMESTAMP OPTIONS

This section allows saving the credentials Username and Password to use the timestamps (if the holder has one) without entering them every single time the user want to use a timestamp.

Clicking on **Check Available timestamps** you can verify the number of residual timestamps.

LINK to the use timestamping service

Figure 38 - Options Time Stamp

The "Options" dialog box has several tabs: General, File manager, Logo.pdf, Verify, Connection, URL, and Timestamp. The "Timestamp" tab is active, showing fields for "Default TSA URL" (with the value "https://timestamp.namirialtsp.com"), "Username", and "Password". There is a checkbox for "Not prompt timestamp credentials" and a "Check available timestamps" button. At the bottom, there is a checkbox for "Not share this options with other 'firma certa' softwares" and "OK" and "Cancel" buttons.

<https://timestamp.namirialtsp.com>
<http://timestamp.namirialtsp.com>

4.4 HELP

Section in which you can find the software User Guide, manually check available updates clicking on **Check Upgrade**.



Figure 39 - Panel: Support

Figure 39: Panel: Support



5 APPENDIX A: HOW TO SIGN AND COUNTERSIGN

5.1 HOW TO SIGN A DOCUMENT

Choose the file to be sign and click **Sign**.



Figure 40 - Signature Panel

Attention: Firmacerta software allows signing any type of file in in CADES .p7m format, but only for PDF or XML files the software will ask the user to choose if sign in .p7m or maintain the original format.

5.1.1 SIGN IN CADES - XADES

After clicking on "sign" a window to ask you the format to sign the document will be opened.

- Press Yes for a XAdES signature, keeping the .xml format (valid only for XML files)
- Press No for a CAdES signature in a .p7m format

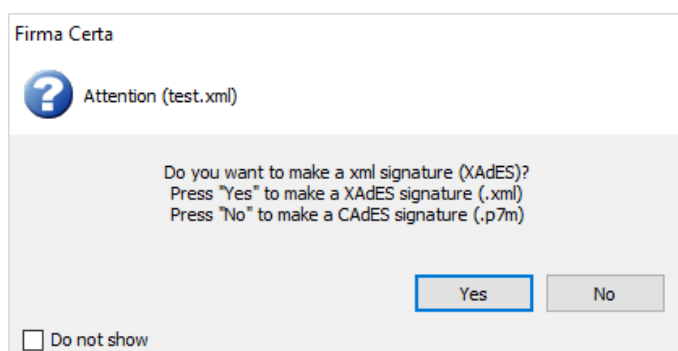


Figure 41 - Selection of Cades-XAdES signature format



Select the destination folder of the signed file, then click OK.

Proceed with the signature operation pressing Yes.

Attention: We recommend to create a specific folder for Digitally Signed File, in order to avoid problems.

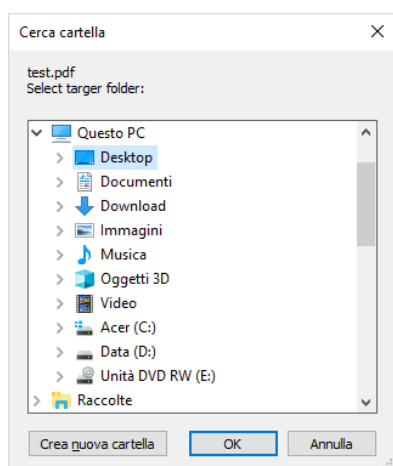


Figure 42 - Select the destination folder

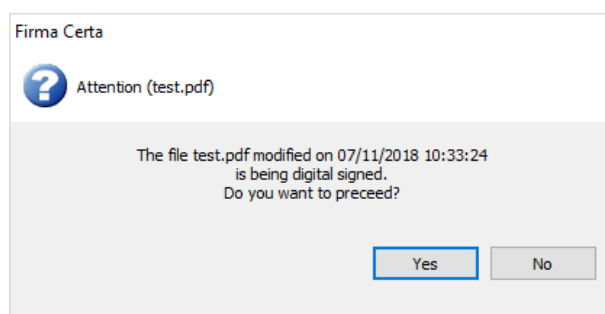


Figure 43 - Signature Confirmation

Enter the PIN of the digital signature device and click OK.

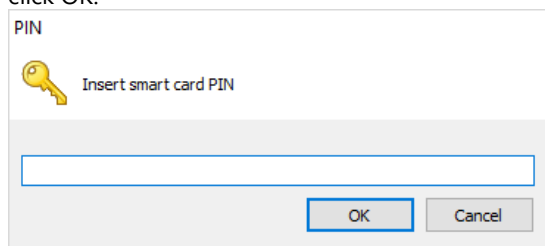


Figure 44 - Enter the PIN code

Wait the processing time and press OK to complete the operation.

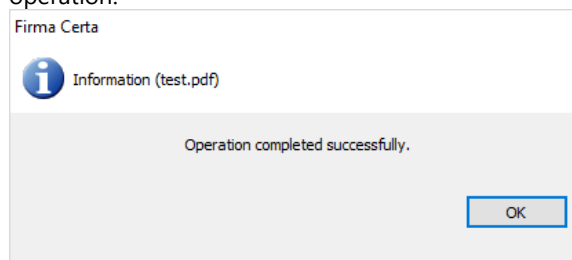


Figure 45 - Operation completed

5.1.2 SIGN IN PADES

After clicking on "sign" a window to ask you the format to sign the document will be opened.

- Press Yes for a PAdES signature, keeping the .pdf format (valid only for PDF files)



- Press No for a CAdES signature in a .p7m format

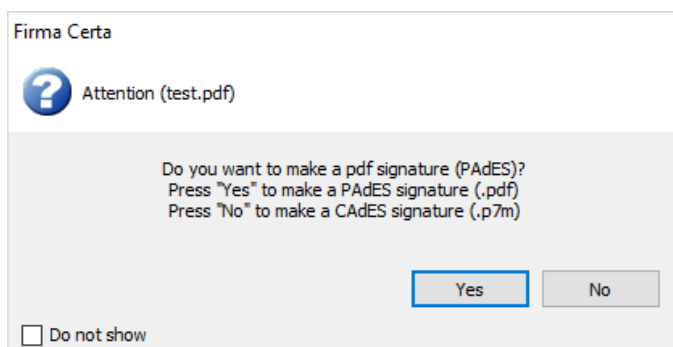


Figure 46 - Selection of Cades-Pades signature format

Select the Destination Folder of the signed file, then click OK.

Proceed with the signature operation pressing Yes.

NB: We recommend you to create a specific folder for Digitally Signed Files, in order to avoid problems.

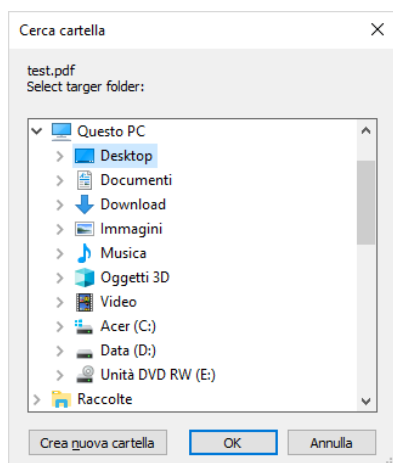


Figure 47: Select the destination folder

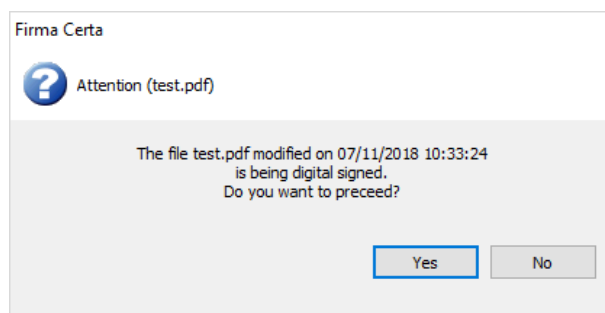
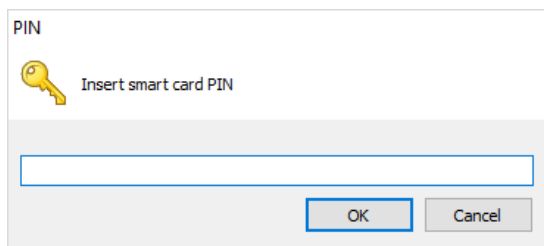


Figure 48: Signature Confirmation

Enter the PIN of the Digital Signature device and click OK.

Select the signature reason (optional).



PIN


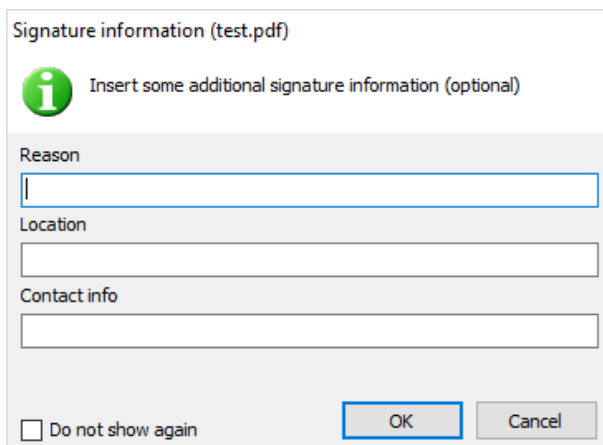

 Insert smart card PIN

Figure 49: Enter the PIN Code



Signature information (test.pdf)

 Insert some additional signature information (optional)

Reason

Location

Contact info

☐ Do not show again

Figure 50: Signature information

Select the position of the logo using the green marker

To confirm the operation press "Yes".

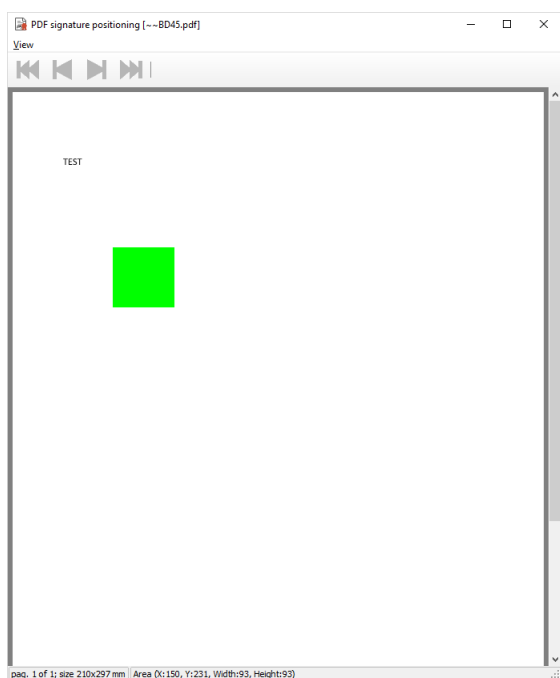
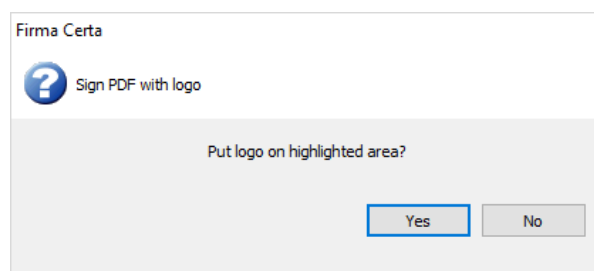



Figure 51: Positioning of the signature marker



Firma Certa

 Sign PDF with logo

Put logo on highlighted area?

Figure 52: Positioning Confirmation



To customise the logo (optional), press OK.

Logo customization (test.pdf)

i Insert logo text customization values (optional)

☒ Show date and time
☒ Auto generate text

Header
Title 1
Text 1 (max 4 lines)
Title 2
Text 2

☒ Automatic font size

Date and time	4,89	Header	8,77
Title	7,00	Text	5,00

☐ Save values in smartcard
☐ Do not show again

OK Cancel

Figure 53: Customized Logo

Wait the processing time and press OK to complete the operation.

Firma Certa

i Information (test.pdf)

Operation completed successfully.

OK

Figure 54: Operation completed

5.2 HOW TO COUNTERSIGN

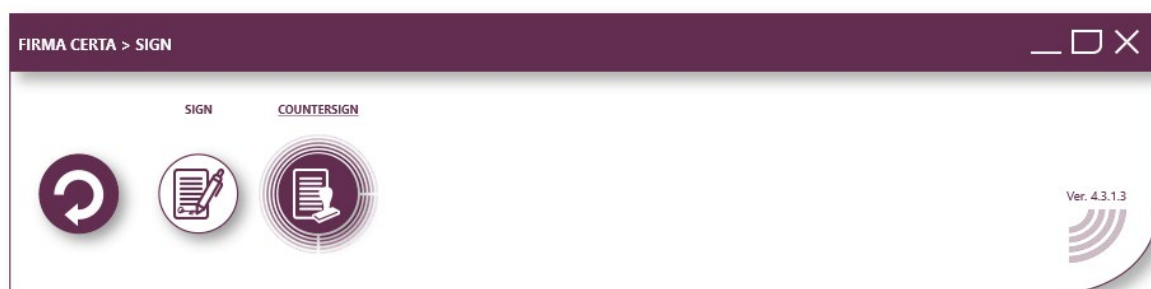


Figure 47 - Panel of Countersign

With this function it's possible to countersign a signature already present in the document, giving at this latter signature a kind of hierarchical validation.

After loading the file digitally signed that you want to countersign, click on the button "Countersign".

ATTENTION: You can only countersign a digitally signed file with the format .p7m



Select the Destination Folder of the signed file, then click OK.

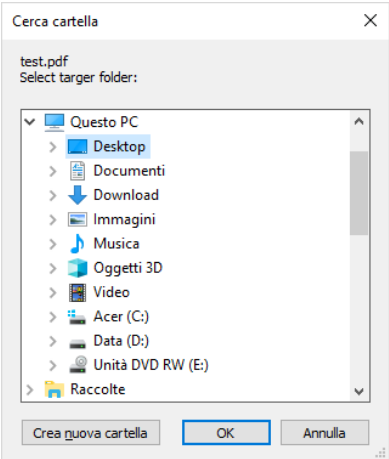


Figure 48 - Select the destination folder

Confirm if you want to overwrite the existing file and click Yes.

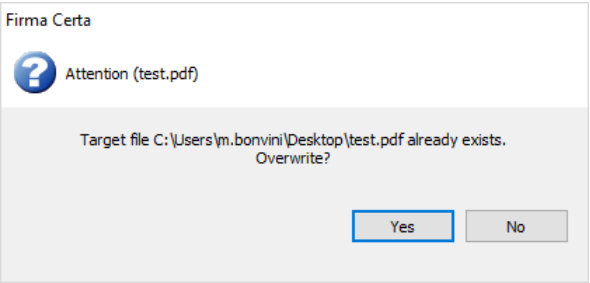


Figure 49 - Confirmation of overwriting

Select the signature you want to countersign and click on OK.

Example: In the following picture the user TEST NAME SURNAME 2 countersign the signature of TEST NAME SURNAME 1

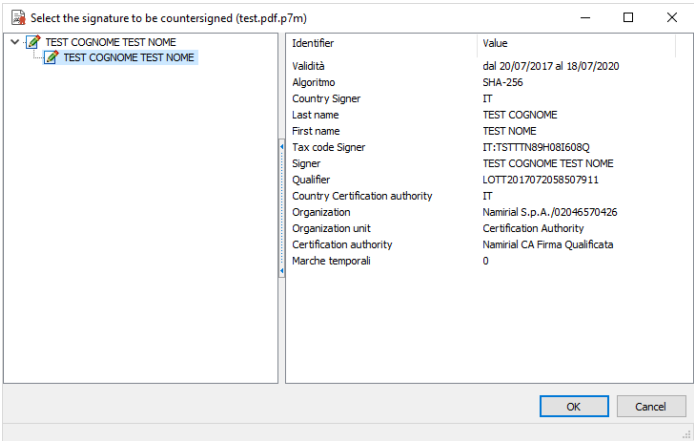


Figure 50 - Example screen: verification of the countersigned file



Proceed with the signature operation pressing Yes.

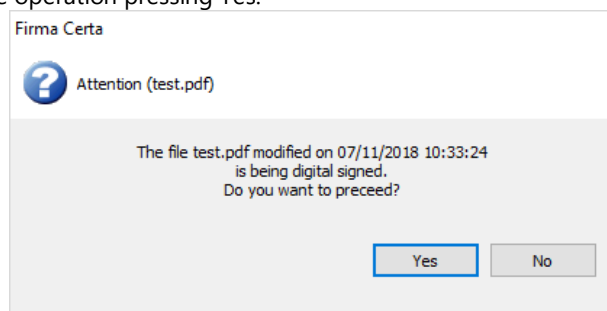


Figure 51 - Signature Confirmation

Enter the PIN of the Digital Signature device and click OK.

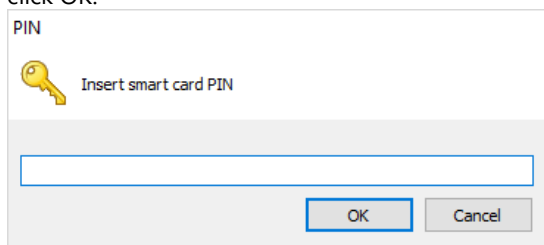


Figure 52 - Enter the Pin Code

Wait the processing time and press OK to complete the operation.

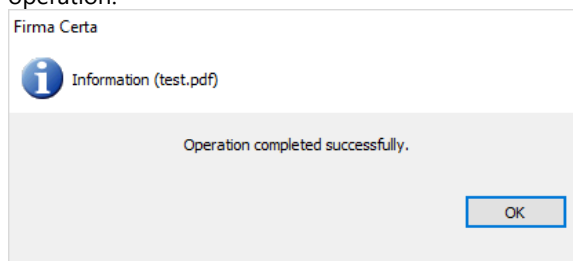


Figure 53 - Operation completed



6 APPENDIX B: HOW TO TIMESTAMP A FILE

Before using the Timestamp Service you must configure FirmaCerta software.

ATTENTION: The timestamp service is not included with digital signature. The timestamps can be purchased in our Shop. To configure the timestamp open FirmaCerta Software > Utility > Timestamp Options

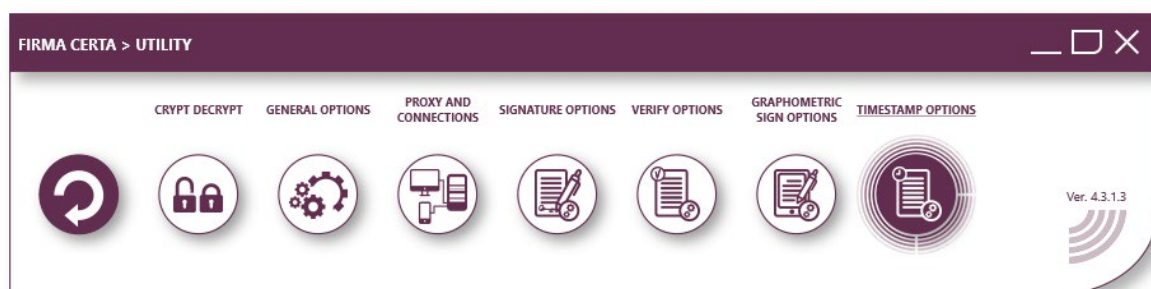


Figure 54 - Utility Panel

6.1 CONFIGURATION OF TIMESTAMP PARAMETERS

From the menu **Utility->Timestamp option**

- Check that the URL is <http://timestamp.namirialtsp.com> or <https://timestamp.namirialtsp.com>
- Insert Username and Password, then click OK.

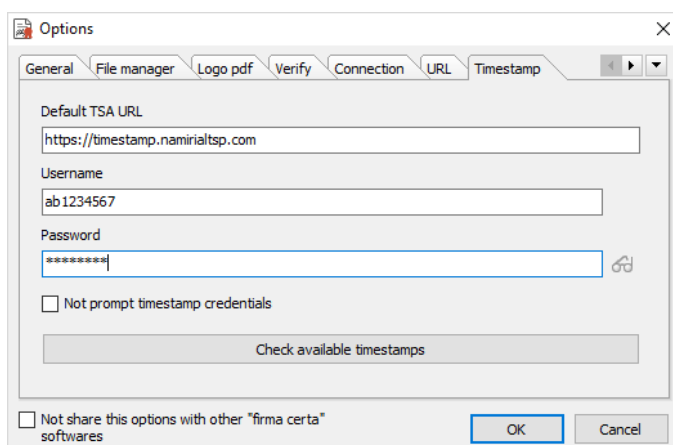



Figure 55 - Timestamp Configuration Options

ATTENTION:

- Clicking on the icon  next to the field Password, it's possible to view clearly the password you are entering.
- in case of loss of timestamp credentials the user can request them sending a PEC to firmacerta@sicurezza postale.it or an email to helpdesk@firmacerta.it specifying the username and / or Tax Code.

The function **Check Available Timestamp** verifies the residual timestamp (in case the query fails you should check the correct insertion of the credentials)

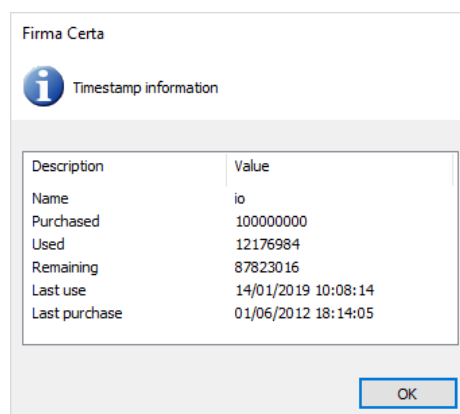


Figure 56 - Checking Timestamps

6.2 HOW TO SIGN AND TIMESTAMP

After selecting a file you can choose this function to sign and timestamp in one singular session.

The file signed and timestamped will be a CADES-T format (file stamped.pdf.P7M).

In CADES-T format (the default format) the timestamp is associated to a single signature and NOT severable.

To Sign and Timestamp proceed as in the following steps:

- Select Sign and Timestamp inside the software,

Select the signed file destination folder, then click OK. Proceed with the signature operation, so press "Yes".

NB: We recommend you to create a specific folder for the files, in order to avoid problems.

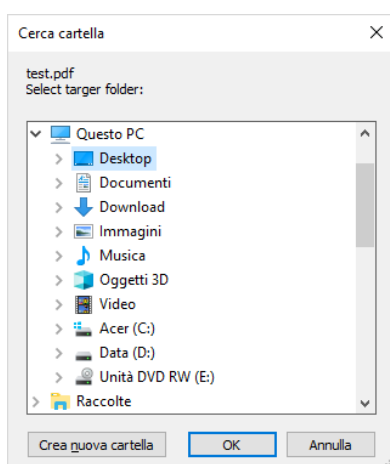


Figure 57 - Select the destination folder

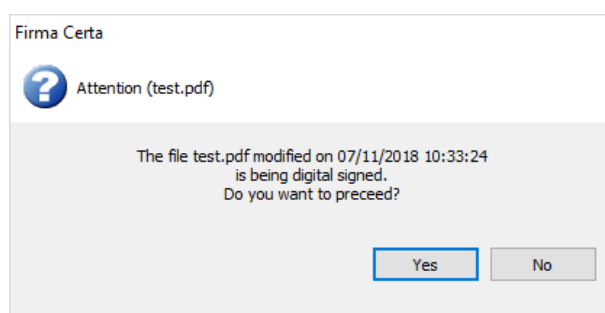


Figure 58 - Signature Confirmation

Enter the PIN of the digital signature device, then click "OK".

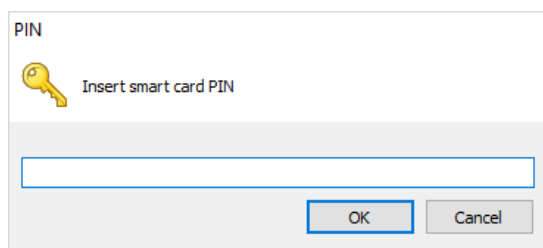


Figure 59 - PIN Entry

Confirm the application of the timestamp, then click OK.

Wait the processing time and press OK to complete the operation.

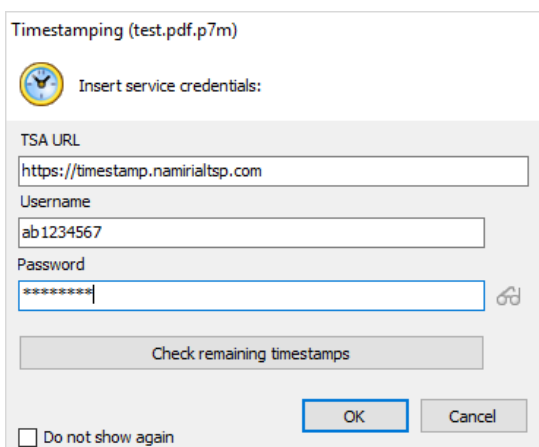


Figure 60 - Confirmation of the entered timestamp credentials

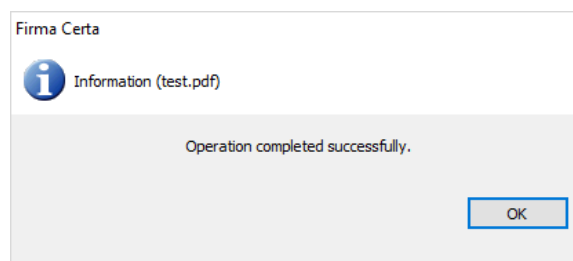


Figure 61 - Operation completed

6.3 HOW TO SEPARATE THE TIMESTAMP

This feature allow the user to separate, from a file in a .TSD format (timestamped-date) the timestamp.

ATTENTION: it's possible to do this operation just for signed files in .p7m

6.3.1 HOW TO SIGN A FILE IN .P7M

Load the file that will be signed and click "Sign".



Figure 62 - Signature dashboard



ATTENTION: The software Firmacerta allows signing any type of file in CAdES format, also called .p7m. Only for PDF or XML files the software will ask the user to choose if sign in .p7m or maintain the original format.

After clicking on sign the software will open a window to ask you in which format you want to sign the document. Press **No** for a CAdES signature (.p7m format)

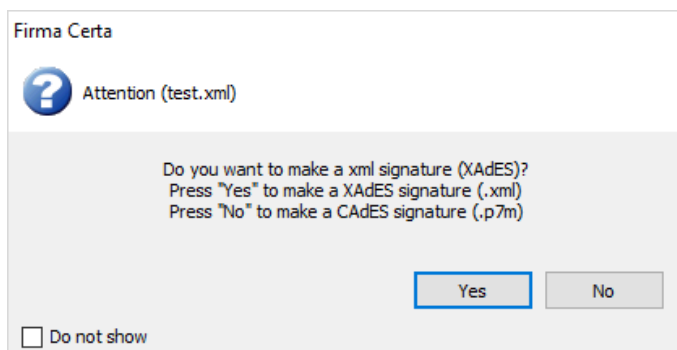


Figure 63 - Selecting the Cades signature format

Follow the procedure described in point [Appendix A: How to sign a document](#).

6.3.2 HOW TO TIMESTAMP A SIGNED FILE .P7M

Load the file to sign inside the software and click on **Timestamp**.

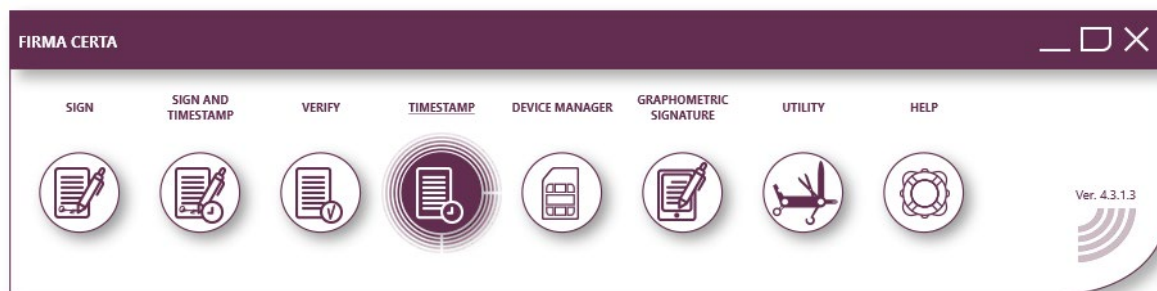


Figure 64 - FirmaCerta Panel Timestamp

Select the .TSD format for the Timestamp.

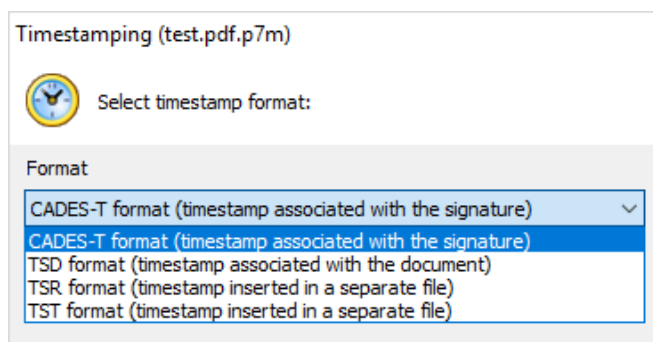


Figure 65 - Selecting time stamp format

Select the destination folder for the signed file, then click OK.

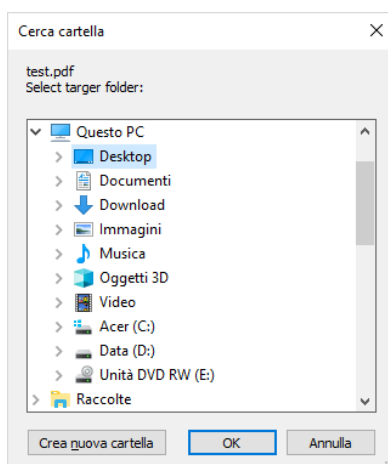


Figure 66 - Selection of destination folder

Confirm the application of the timestamp, then click OK.

Wait the processing time and press OK to complete the operation.

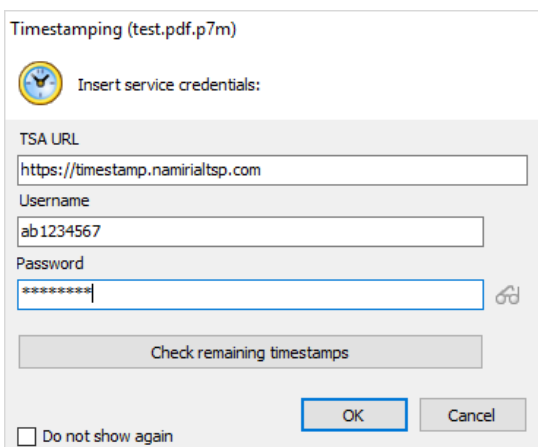


Figure 67 - Confirms configuration timestamp

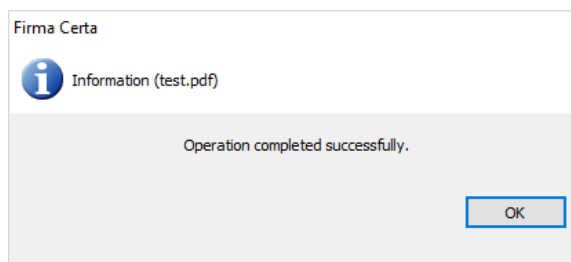


Figure 68 - Operation completed

At the end of the operation a new file will be created by FirmaCerta software.

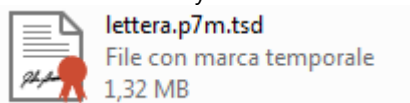


Figure 69 - Example: file marked temporally

6.3.3 SEPARATE THE TIMESTAMP

Load the file timestamped inside the software and click **Verify**.

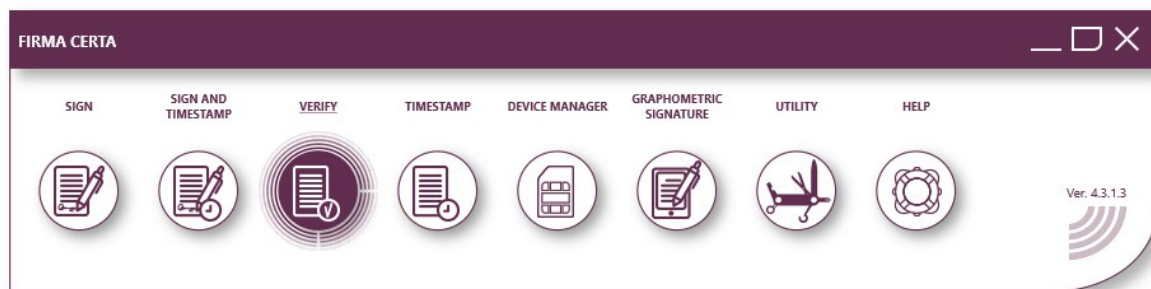


Figure 70 - FirmaCerta Panel Verify for separate the timestamp

Inside the profile "Verify", select the Timestamp and from the tools menu click on **"split timestamp and document"**.

Select the required format of the timestamp, .TSR / .TST, and then press OK.

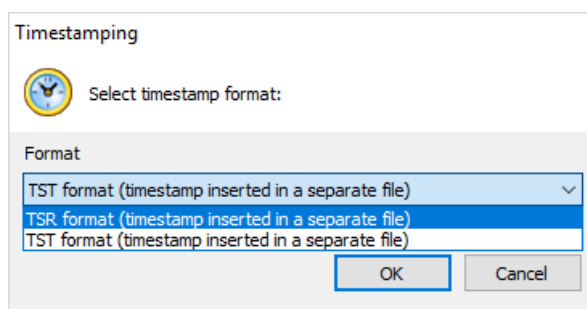
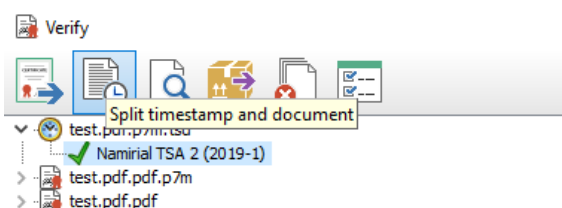


Figure 71 - Timestamp Separation

Figure 72 - Select the format

At the end of the operation the user will have two files:

- A .TSR or .TST file containing the timestamp.
- A .p7m file containing the file digitally signed.



Figure 73 - Example of timestamped files



7 APPENDIX C: HOW TO VERIFY AND VIEW A FILE

To check the validity of a digital signature in a document proceed as in the following steps:

Load the file digitally signed into the program and click **Verify**.



Figure 74 - FirmaCerta Panel Verify

After clicking **Verify** a summary window will be opened as follows:

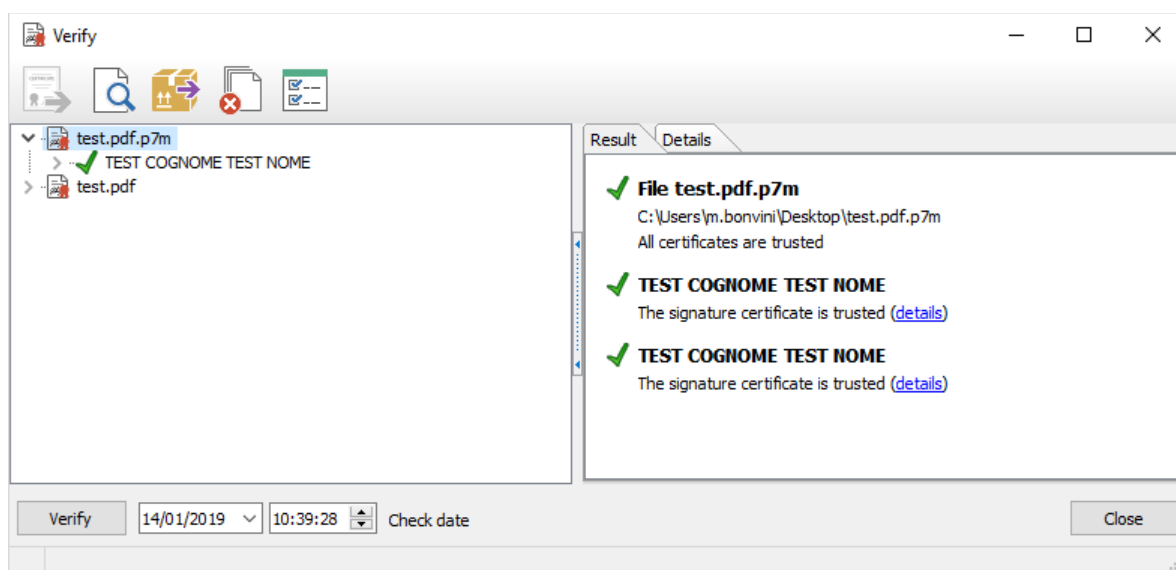


Figure 75 - Verification Screen

ATTENTION: if appear the lettering “**the certificate has not been verified**” it means that the check of the signature has not been automaticcaly started, so it will be suitable manually start the verification clicking on the **Verify** button. In the left column it’s possible to view the file that has been digitally signed and who have signed it.

Example: In this case the signed file “is test.pdf.p7m” and it has been signed by two users: TEST COGNOME1 and TEST NOME COGNOME2

In the right column it’s possible to find the **Result** of the verification and the **Details** of the certificate, so that is:

- the type of signature and its validity;
- the entity that issued the certificate;
- the data of the holder;

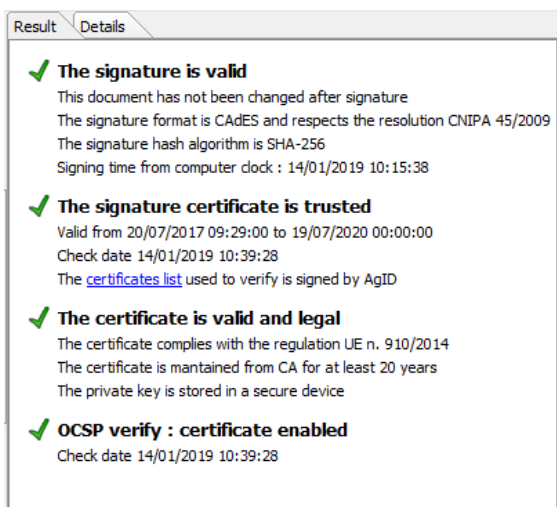


Figure 76 - Screen of Result Tab

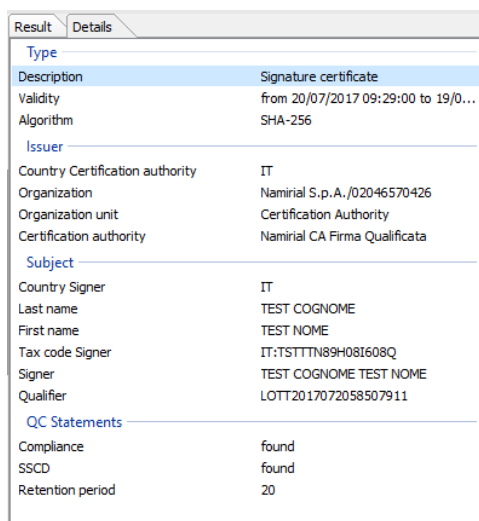


Figure 77 - Screen of Details Tab

7.1 HOW TO AUTOMATICALLY SET THE LAUNCH OF VERIFICATION OF SIGNATURES

Click on **Utility -> Verify options.**

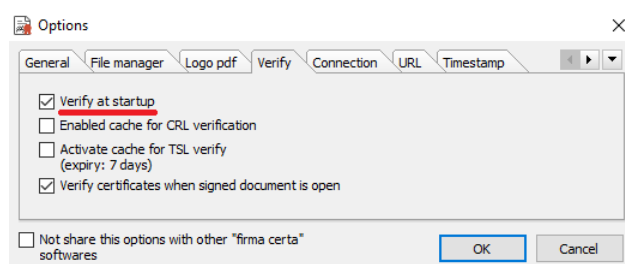


Figure 78 - Verification Settings

7.2 HOW TO VIEW A SIGNED FILE

To view a digitally signed document proceed as in the following steps:

Add the file into the software and click **Verify**;

Click on the icon showed below:



Figure 79 - Screen to view the signed file in verify option

ATTENTION:

- The user has to verify to have the latest version of Adobe Reader to use this option;
- Just for digitally signed .PDF files will be possible to view a PDF logo.



8 APPENDIX D: HOW TO ENCRYPT AND DECRYPT A FILE

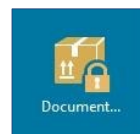
The encryption of a document (also called cryptography) is a particular operation through which the document will be completely unreadable for anyone, except those who have the key to decrypt it, to bring it back "to the clear form". Encryption, therefore, makes possible to ensure the confidentiality of confidential informations.

To encrypt a document, so only a particular recipient can read it, the sender needs to have the recipient digital certificate, since the encryption operation request the use of the public key.

To decrypt a document the recipient must have your own signature device SmartCard/Token, since the decryption request the use of the private key.

The digital signature and the encryption operation can be combined that is: a document can be signed and then encrypted to ensure both the paternity and that secrecy.

The icon of an encrypted document with Firma Certa Protect looks like the following:



8.1 HOW TO ENCRYPT A FILE

Remembering that **to encrypt a document you must have the encryption certificate of the recipient** (of the user we want to be the only one who can decrypt the document).

It can be obtained by requesting the digital certificate of the recipient and, then, manually importing it into your own Firma Certa Protect certificate database.



You can encrypt a document for multiple users simultaneously, so for different people.

To encrypt a document click on "Protect Document" in the main window of Firma Certa Protect.



At the end of the operation the encrypted file will be created in the same position where the document is originally saved.

8.2 HOW TO DECRYPT A FILE

Opening the document with a double click, you will be asked to enter the PIN to open both the verification and viewing window.

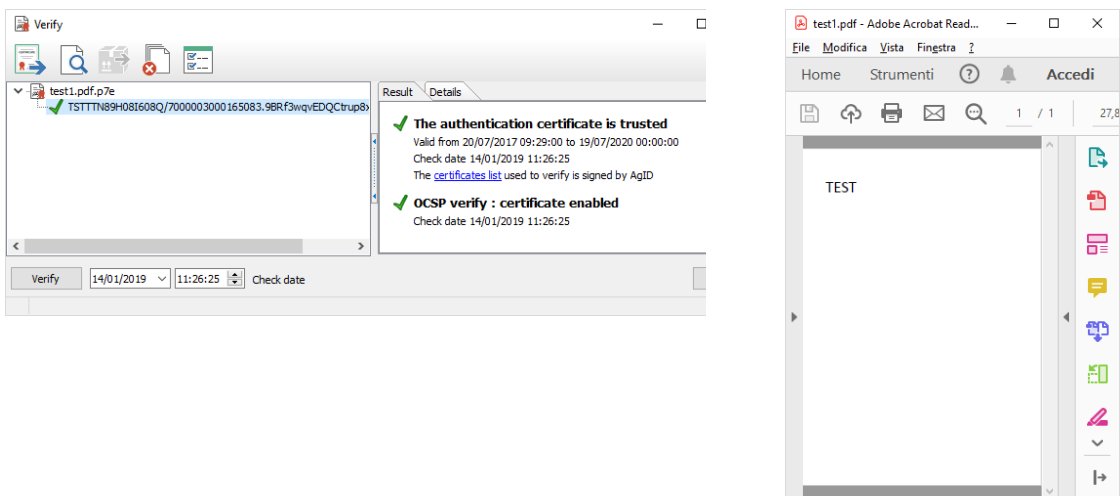


Figure 80 - Verification with Sample Screen

ATTENTION:

If you do not have the private key needed to decrypt the file, an error message will occur:

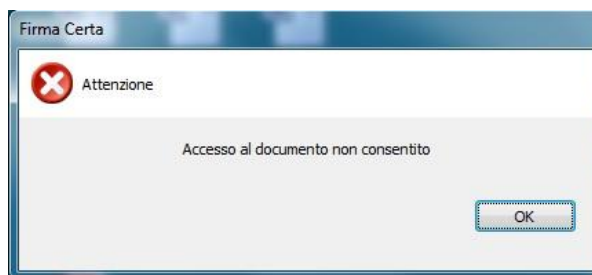


Figure 81 - Access denied



9 APPENDIX F: COMMAND LINE

The FirmaCerta client can be used from the command line to allow the integration with applications that require signatures and timestamp without any operator assistance. In Windows environment to check the position of FirmaCerta, read the PathApp value of the following key:

```
[HKEY_CURRENT_USER\Software\Namirial\Firmacerta\fcsign.exe] "PathApp" = ""
```

9.1 COMMANDS AND PARAMETERS

fcsign.exe: <file> <action> <mode> <params>

<**File**> full path of the file to operate

<**Action**> 0 = Signature 1 = Signature and Timestamp 2 = Countersignature 3 = Timestamp 4 = Verify 5 = Display 7 = Options

<**Mode**> m if massive signature is required, in this case it must be a text file containing the list of the files to be processed one per line

<**Params**>

- **TargetDir**= <destination folder for processed files>
- **LogFileName**= <process log file that is run in silent mode (without showing any unnecessary windows)>
- **OverwriteLog**= <File>
- **Pin**= <pin code to access to the signature device>
- **UrlTSA**= <server url for time stamps>

NOTE: If you do not set up it, the url set up will be taken during the configuration

- **UsernameTSA**= <user for access to the timestamp services>
- **PasswordTSA**= <password for access to the timestamp services>
- **OverwriteFile**= <1 Overwrite the processed file if present; 0 add an underscore (_) in the name (default)>

IMPORTANT: The parameters in the form "key1=value1;key2=value2" (separated by a semicolon (;) and enclosed by double commas (")).

9.2 EXAMPLES:

Following few examples to make the use of commands more simple and intuitive.

Signing a document fcsign.exe "C:\Documents and Settings\User\Desktop\Documento.pdf" 1

Signing a document without a GUI

```
fcsign.exe "C:\Documents and Settings\User\Desktop\Documento.pdf" 1  
"TargetDir=C:\Folder\;LogFileName=C:\firmacerta.log;Pin = 999999"
```

Multiple Document Signing

```
fcsign.exe "C:\temp\list.txt" 1 m
```

the file "C:\temp\list.txt" contains:

```
C:\Documents and Settings\User\Desktop\Documento1.pdf  
C:\Documents and Settings\User\Desktop\Documento2.pdf  
C:\Documents and Settings\User\Desktop\Documento3.pdf
```



10 APPENDIX G: ADVANCED FEATURES

The Client FirmaCerta has a number of unusual features that allow the holders to make the signature operations more simple.

IMPORTANT: *all the signature functions of several documents at the same time are possible only with certificates issued by the Certification Authority Namirial SpA*

10.1 SIGNATURE OF MORE DOCUMENT

The client allows the user to select multiple documents simultaneously, by inserting the PIN code only one singular time and signing the documents consecutively.

Before performing the Massive Signature procedure you must configure the program, from Utility> General Options> General:

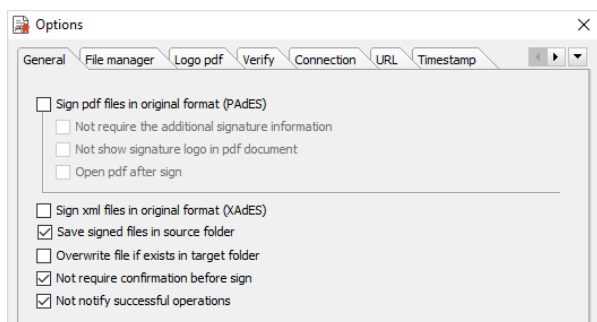


Figure 82 - Configuration for automating Pades signature

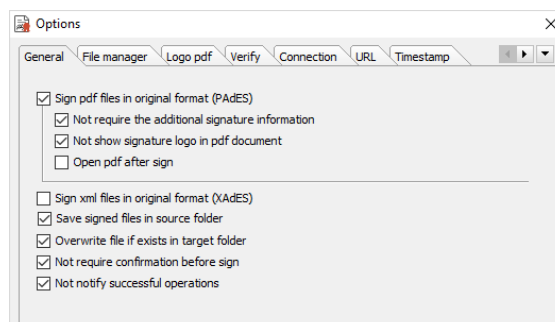


Figure 83 - Configuration for automating Cades signature

10.2 MULTIPLE DOCUMENT TIMESTAMP

The client allows the user to select multiple documents simultaneously and put the timestamp consecutively.

Before performing the Massive timestamp procedure you must configure the program, from Utility> General Options> Timestamp:

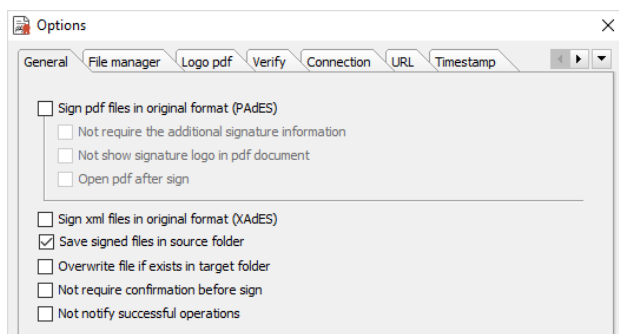


Figure 84 - General Options for timestamp multiple documents

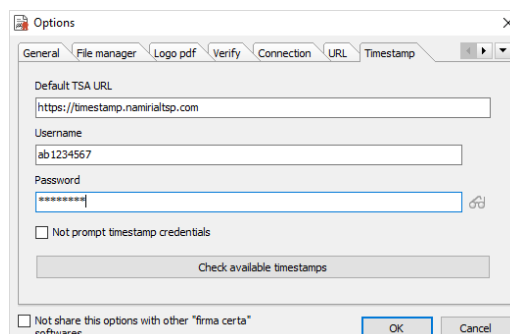


Figure 85 - Configuration Timestamp Option



Select the timestamp format and select "Keep values for all timestamps" if you want to maintain the same value for all the files to be timestamped.

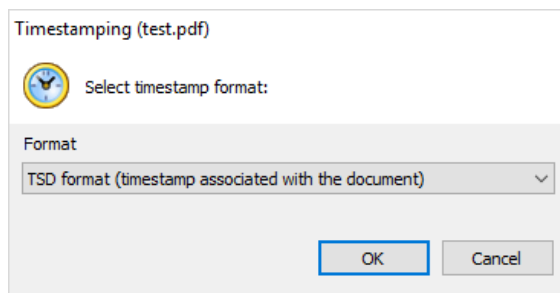


Figure 86 - Select Timestamp Format

10.3 SIGN AND TIMESTAMP MORE DOCUMENTS

The client allows the user to select multiple documents simultaneously and put the timestamp consecutively, by inserting the PIN code one singular time to sign and timestamp the documents consecutively.

Before performing the Massive Signature and timestamp procedure you must configure the program, from Utility> General Options> General first and Timestamp then:

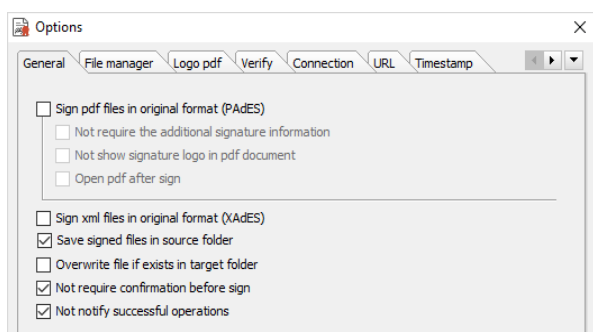


Figure 87 - Configuration for sign and timestamp multiple documents

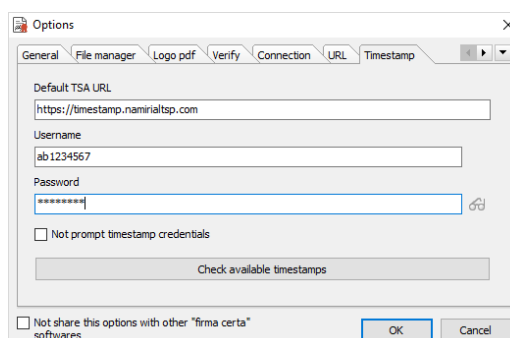


Figure 88 - Configuration Timestamp Option

The software will request to enter the PIN code once.

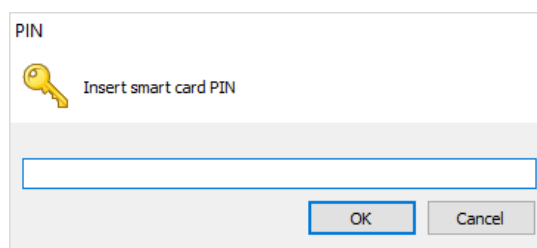


Figure 89 - Insert PIN



11 APPENDIX H: CERTIFICATE RENEWAL

Before proceeding ensure to have been installed on your desk the signature software [FirmaCerta](#) properly updated.
If the you are using a proxy please ask your network administrator the parameters configuration.
If there is no voice Certificate Renewal you must download the software FirmaCerta Device Manager.

11.1 PROXY CONFIGURATION

Open Firmacerta software and click on Device Manager> Certificate Renewal, confirm the terms and click **Next**.

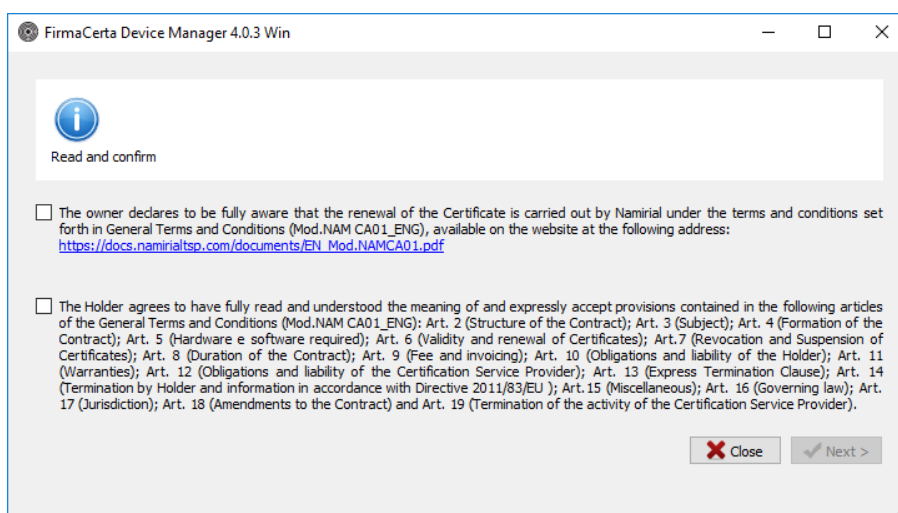


Figure 90 - Restrictive clauses

Select "ACTION" and set the proxy (for the parameters contact your network administrator) Click SAVE.

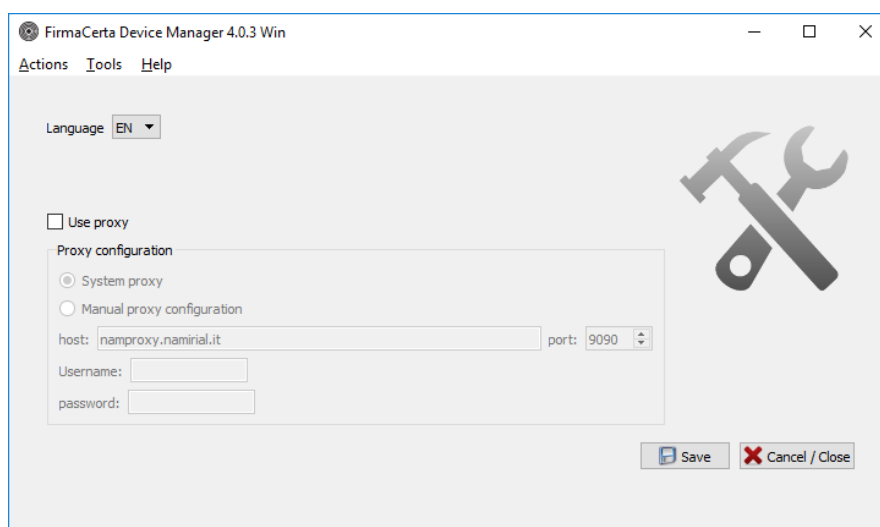


Figure 91 - Proxy Configuration



11.2 METHODS OF RENEWAL: SMARTCARD AND TOKEN

Open FirmaCerta with the signature device connected to the computer, then click on "*Device Manager > Certificates Renewal*".

Read and confirm the restrictive terms and click **NEXT**.

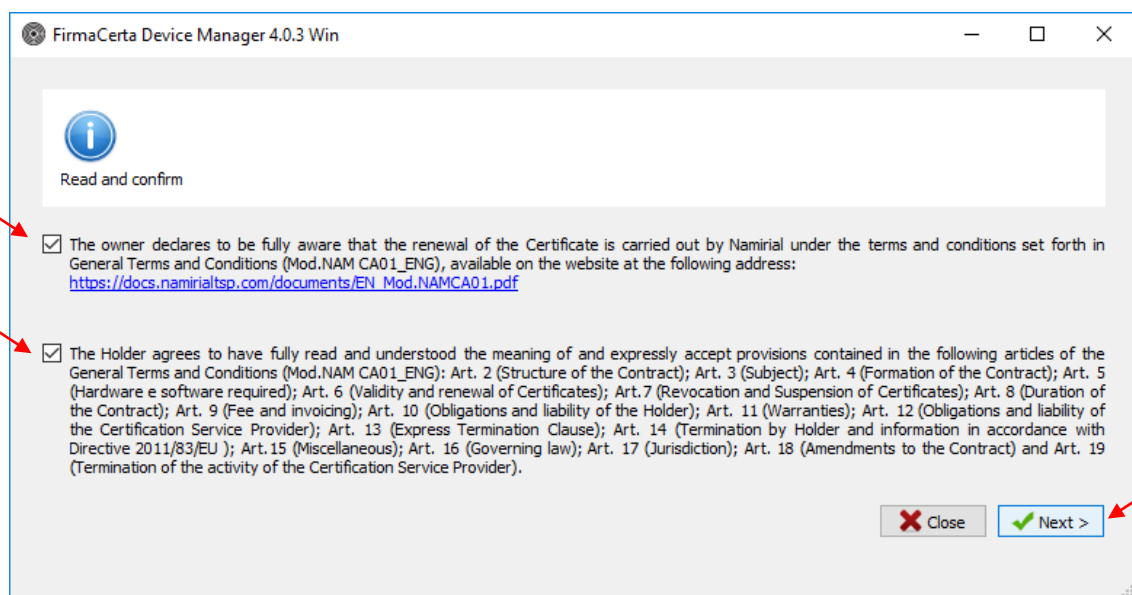


Figure 92 - Restrictive clauses

Then click "**Select Device**" and enter the Pin for the recognition of the device and the reading of the certificates.

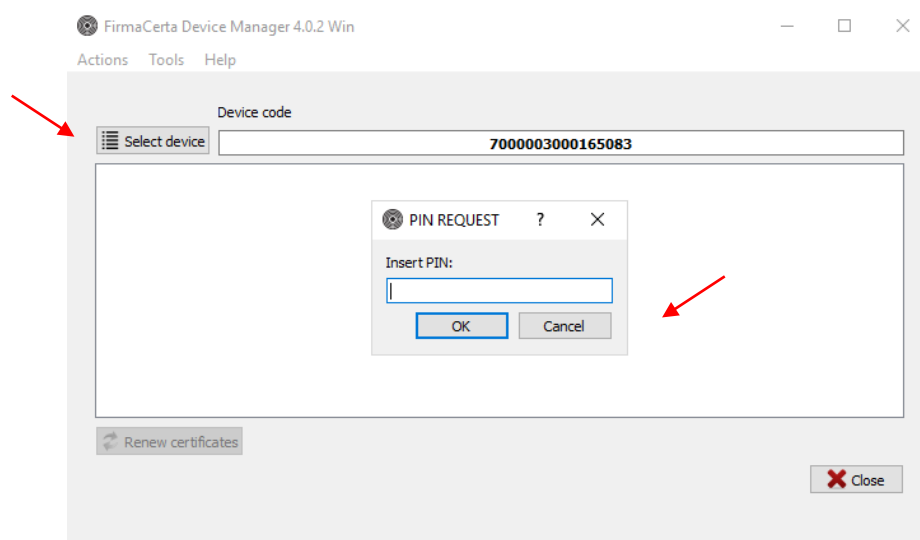


Figure 93 - Insert PIN



The tool will propose to display (optional) and digitally sign (mandatory) a .pdf file for the request of the certificates renewal. Select "OK", when required, to complete the signature operation.

Wait until the renewal procedure will be completed.

At this point, the tool will propose to sign the renewal certificates contract automatically, asking the user if view it or not.

Once the certificates will be displayed select **"Renew Certificates"**.

Then, the tool will propose to display or not the request for renewal, in both cases, the file will be digitally signed.

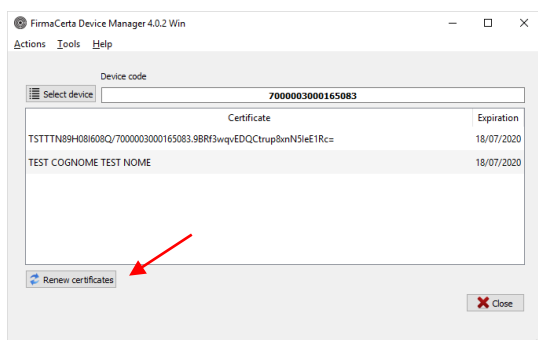


Figure 94 - Renew Certificates

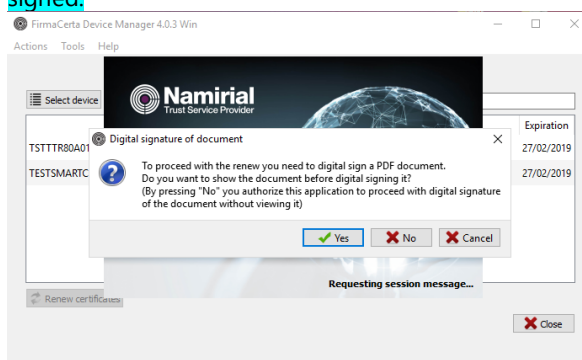


Figure 95 - Request to view the contract before signing it

If you have selected to view the PDF document the program will show the certificate renewal contract. To complete the whole process the user must apply his/her signature by clicking on the file shown.

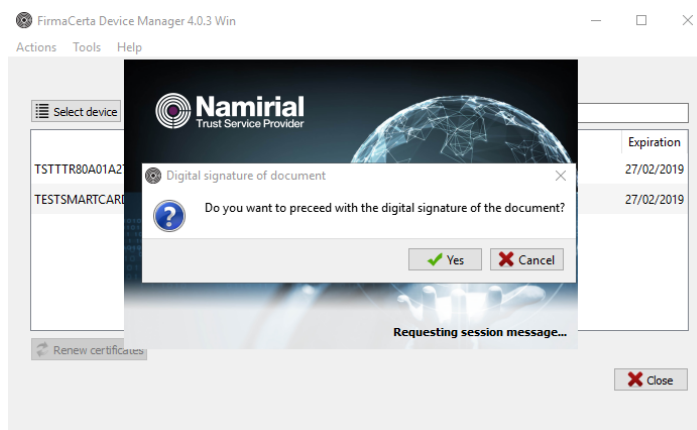


Figure 96 - Confirmation of affixing signature

Wait to complete the renewal process and end the operation pressing **OK**.

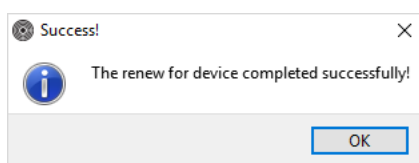


Figure 97 - Renewal successfully completed



11.3 METHODS OF RENEWAL: AUTOMATIC AND REMOTE CERTIFICATES

Access to your personal area at the following address: <https://portal.namirialtsp.com>

Click on LOGIN and insert username and password previously received via email at the time the digital signature certificate has been issued.



Figure 98 - Namirial Private User Area

ATTENTION: In case of loss of credentials you can recover the individual data by clicking on "I don't remember the username" or "I don't remember the password", and then following the instructions. If the problem persists the credentials may be requested by email helpdesk@firmacerta.it specifying the signature holder's tax code.

After successfully logging in.

- In the home page, find the box *Functionality or services to activate* on the right side > click on *Renew certificates*;
- Alternatively, click on *User > Digital Signature > Management* on the left side;

To proceed you will be asked to enter the OTP code.

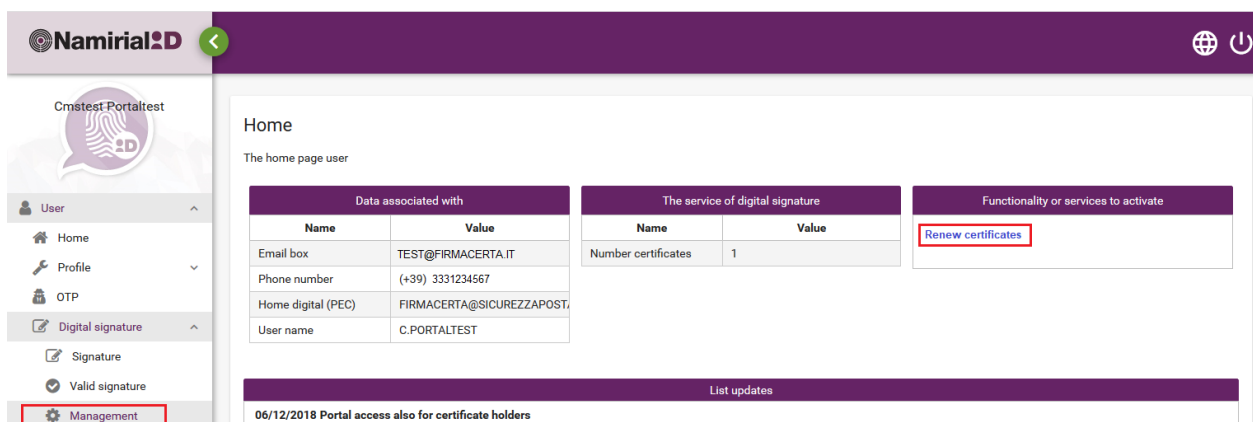


Figure 99 - Private User Dashboard




In **Certificate Management** will be displayed all the certificates associated with the user, under the Renewable column it will be possible to choose which certificate will be renewed.

Selecting the certificate and click on the **RENEW** button the panel will open: Procedure to renew the subscription certificate autonomously, it will be necessary to enter first the PIN of the certificate (present in the digital blind envelope received upon the issuance of the certificate) and then the verification OTP code (in this case OTP SMS).

Certificate management

You can manage the life-cycle of your certificates through the functions below. Select it and use the green buttons.

Certificates issued 			
Device code	Expiration date	State	Renewable
2201000009002609	27/02/2019	Active	Renewed
2201000009002609	27/02/2019	Active	Renewed
2201000009002609	28/03/2019	Active	By request
2201000009002609	28/03/2019	Active	By request
RH12760138582183	30/03/2019	Active	To renew



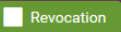
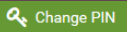
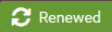







Figure 100 - Certificate Management


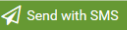
After entering all the data click on **"SIGN AND RENEW"** and wait until the certificate renewal procedure will be completed.

Procedure renewal in the autonomy of the certificate of subscription

Below, you will be issued the new certificate in place of the one expiring. The missing days to expire will be added to the new that will be usable immediately. In order to proceed you must affix a digital signature to the remote using the certificate to be renewed. The new certificate will retain the code device and PIN.

 Displays the contract precompiled

PIN _____

SMS - 326484   Code OTP _____

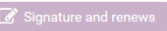




Figure 101 - Signature and renew Process



12 APPENDIX I: SETTING UP REMOTE SIGNATURE

12.1 INTRODUCTION TO NAMIRIAL OTP APP

Namirial OTP is a mobile device application which generate one-time password (or disposable passwords) and is useful for a first use of Firma Certa software remote signature for Windows operating systems. This type of password are normally used to complete an authentication with high level of security (strong authentication).

The Virtual OTP may be needed for:

- the use of remote digital signature (briefly Remote Signature);
- SPID access with 2nd level or superior, trough Namirial ID services;
- to access to the private area of Namirial TS services.

12.1.1 HOW TO OPEN IT

For security issues, opening the App is possible only after the device unlocking operation.

This is:

- If already set up by the user, through a standard mechanism managed by the smartphone.

New generation mobile phones normally provide for:

- Entering a PIN code;
- Using a sign;
- Biometric Recognition: Fingerprint (Touch ID), Face Detection (Face ID)
- If the user has not set up any lock/unlock mechanism, the application will request to choose/set up an appropriate PIN code to open it.

12.1.2 NAMIRIAL OTP CONFIGURATION

To proceed with the first activation the user must launch the application and enter the code previously received via SMS to the mobile number registered during the application process for service activation (Remote Signature, SPID Namirial TSP or other service).

Following, an example of message to activate the Virtual OTP.

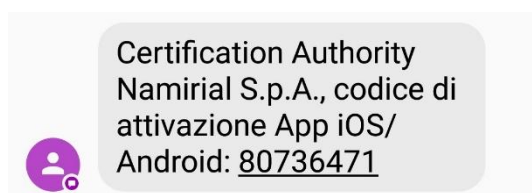


Figure 102 - Example SMS with activation code



12.1.3 ANDROID

For Virtual OTP activation you need to press on Add OTP
Below, a sequence of actions that show how to proceed:

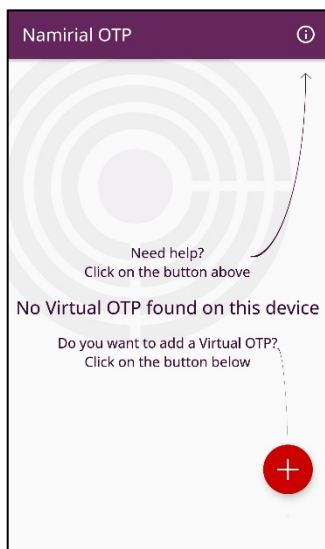


Figure 103 - Start screen of Virtual OTP.
Please tap on the red button

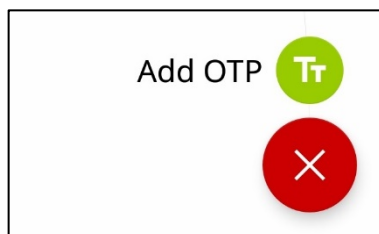


Figure 104 - Making tap the green button
(Add OTP)

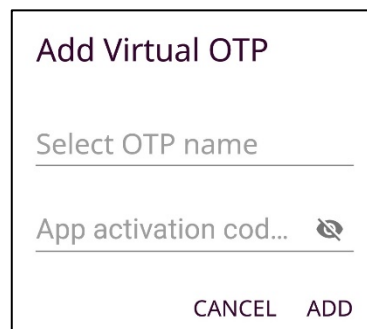


Figure 105 - Enter code and label
allocation

12.1.4 IOS

For Virtual OTP activation you need to press on Add OTP
Below, a sequence of actions that show how to proceed:



Figure 106 - Start screen of Virtual OTP.
Please tap on Add OTP

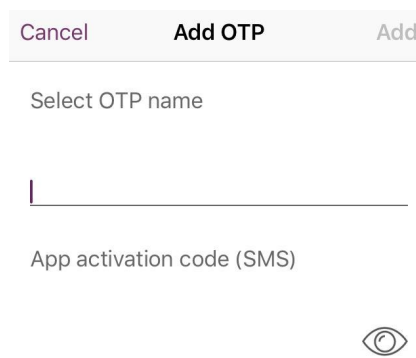



Figure 107 - Enter code and label allocation



Displaying in the last screen:

- **Virtual OTP Name:** is the identification tag associated to a single OTP (eg. Signature). The label is helpful to identify the token you want to use if multiple tokens have been simultaneously activated inside the application.
- **Activation SMS Code/Codice attivazione app:** is the activation code received via SMS, it must be inserted in the field Codice attivazione App SMS (8-digit number) and then click on Add.

Attention: clicking on the  icon you will clearly see the code just entered.

At the end of the procedure a 6-digit code (updated every 30 seconds) will be shown on the screen.

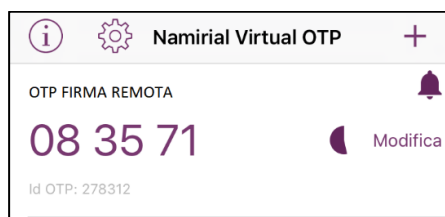


Figure 108 - Screenshot OTP code generated from APP

12.2 ENABLING NAMIRIAL SIGNENGINE SERVICE

Download Firma Certa software to the following link

To enable the Remote Signature service open **FirmaCerta -> Utility -> General Options -> Web Services**. Select Namirial SignEngine and click **Enabled/Disabled**.

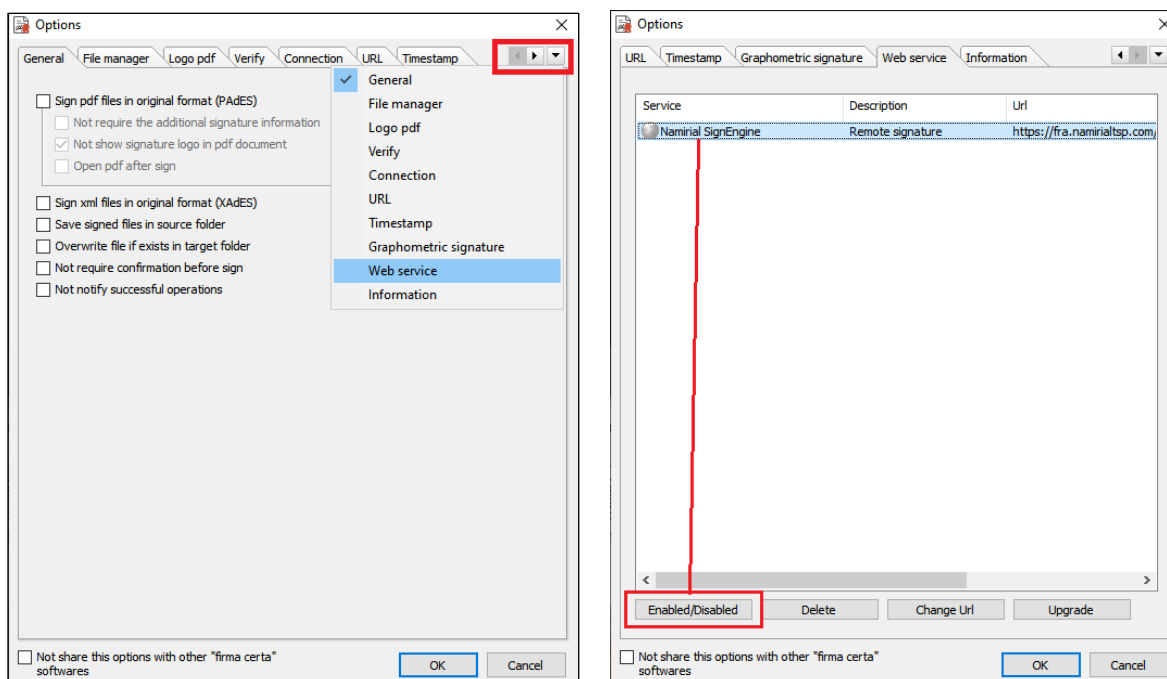


Figure 109 - Enabling SignEngine Service



12.3 HOW TO SIGN A DOCUMENT

Select the file you want to sign and click on **Sign**.



Figure 110 - Signature Panel

ATTENTION: Firmacerta software allows signing any type of file in in CADES .p7m format, only for PDF or XML files the software will ask the user to choose if sign in .p7m or maintain the original format.

Press **Yes** for a XAdES signature, keeping the .xml format (valid only for XML files)

Press **Yes** for a PAdES signature, keeping the .pdf format (only for PDF files)

Press **No** for a CADES signature with .p7m format

Press **No** for a CADES signature with .p7m format

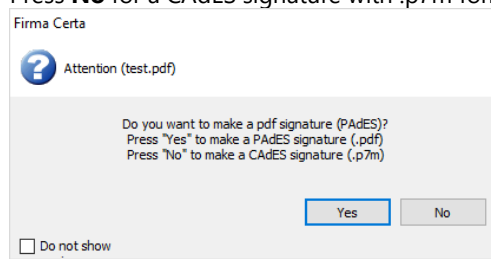
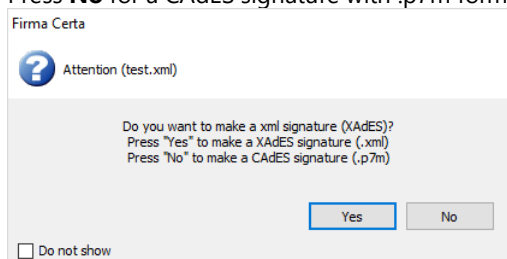


Figure 111 - Choosing signature format



Select the destination folder for the signed file and, Proceed with the signature operation by pressing **Yes**.
finally, click **OK**.

Attention: We recommend to create a specific folder for digitally signed file, in order to avoid problems.

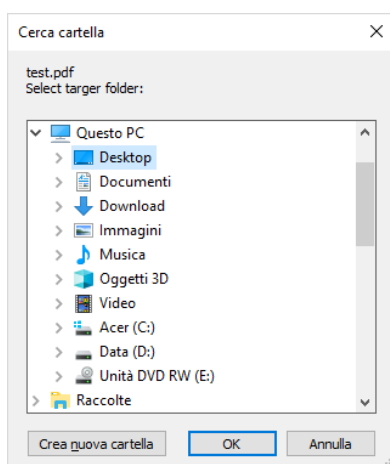


Figure 112 - Selecting the destination folder

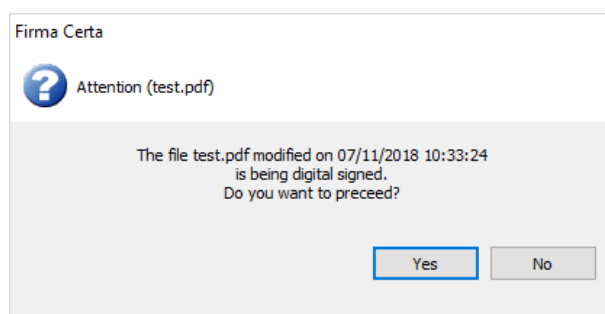


Figure 113 - Signature Confirmation

12.3.1 USERNAME

Click on **Settings** to enter the username:

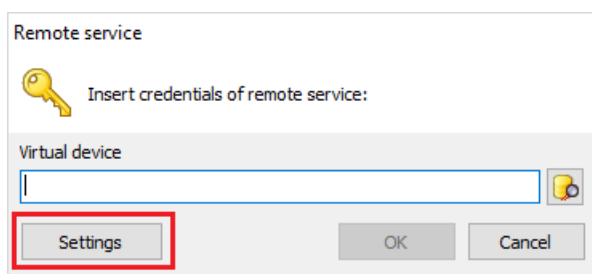


Figure 114 - Remote Service Configuration

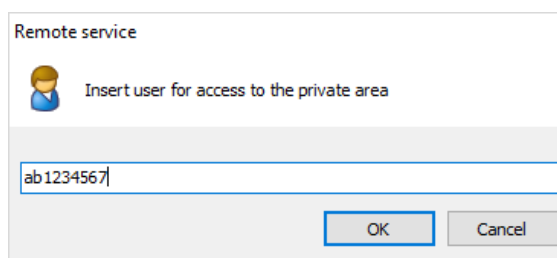


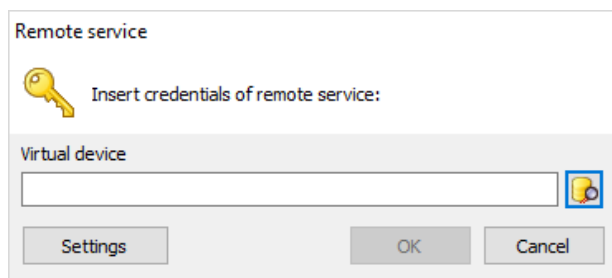
Figure 115 - Insert Username

ATTENTION: In case of lost of the username: access to your personal area at the following address:
<https://portal.namirialtsp.com>
Click on "*I don't remember the user name*" and follow the instructions.
If the problem will persist, please contact the technical support by email at: helpdesk@firmacerta.it



12.3.2 REMOTE DEVICE SELECTION

To configure the virtual device select the icon shown in the red box to get back the virtual device



The following window contains all the virtual signature devices informations, the user must select the device and then click OK.

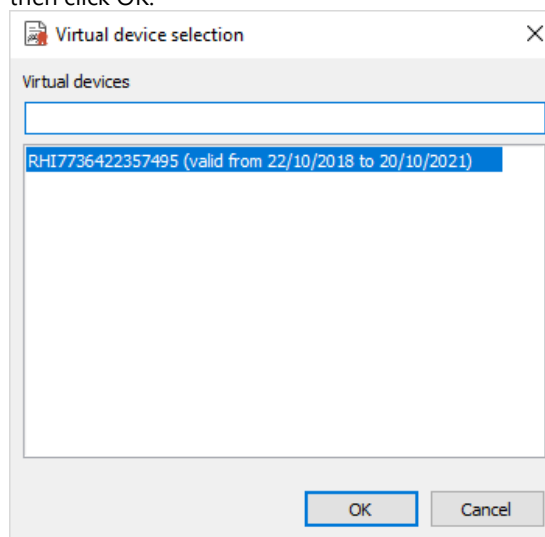


Figure 116 - Selection of the remote virtual device

Once added the virtual device confirm clicking OK

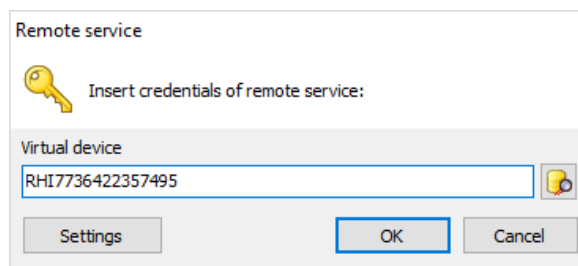



Figure 117 - Wizard Remote Service



12.3.3 SIGN IN PADES FORMAT

ATTENTION: The signature informations are optional and they are selectable only if the PAdES format has been previously chosen.

Signature information (test.pdf)

 Insert some additional signature information (optional)

Reason

Location

Contact info

☐ Do not show again

Figure 118 - Signature information

Example of e-mail with credentials to Private Area access:

Dear TEST NOME TEST COGNOME

thank you for choosing our digital signature products.

We herewith advise you of the USERNAME and the PASSWORD for accessing to your private area from the [ACCESSO UTENTI](#) section:

USERNAME: USERNAME

PASSWORD: PASSWORD

Within this area you can perform a series of operations directly related to the type of your device:

- [Suspension](#) - It may be used as often as it is necessary to suspend the validity of the certificates;
- [Reactivation](#) - It may be used on previously suspended certificates;
- [Revoke](#) - Require to interrupt permanently discontinue the validity of the certificates before their expiry date;
- [Change PIN](#) - It allows you to change the PIN code of the remote/automatic signature certificates;
- [Change Emergency Code](#) - It allows you to change the emergency number used for the remote/automatic signature certificates;
- [Reset OTP](#) - It allows you to reset the OTP token (does not apply to SMS OTP type);
- [Check Signature](#) - It allows you to run a check on the physical devices (smart cards, USB tokens or microSD);

Please note that the USERNAME is also necessary for the configuration of the "FirmaCerta" signature software for using the remote signature. Through the USERNAME, FirmaCerta (available both for PC and Mac and for iPhone/iPad App) is able to automatically associate the holding OTP device. To run the configuration please refer to the relative user guide.

Attention: This is an automatically generated email, please do not reply.

Best Regards,
Namirial S.p.A.
Email: helpdesk@firmacerta.it
Web: www.firmacerta.it

Safeguard clause
The information contained in this message are confidential and its diffusion, in any case, is strictly forbidden.
In the case you are not the intended recipient, we kindly ask you to delete this e-mail after having informed the sender and to not use, in any case, its content.



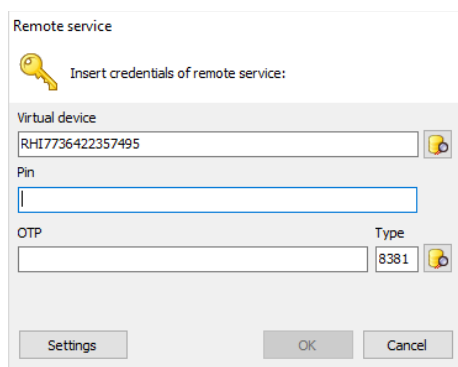
Figure 119 - Example of Blind Envelope



12.4 OTP SMS PROCEDURE

Enter the PIN received by digital blind envelope.

Click on the icon in the red box to select the OTP device, then click OK



Remote service

Insert credentials of remote service:

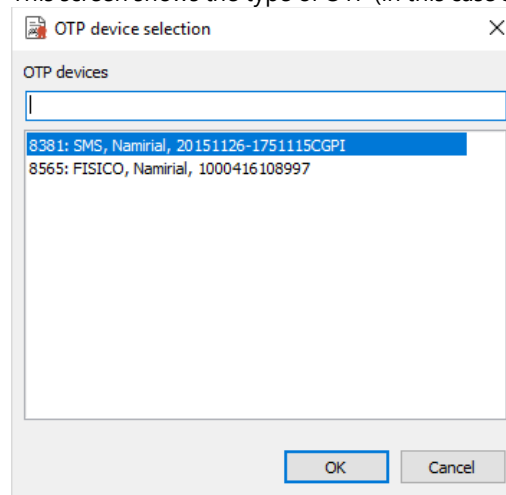
Virtual device
RHI7736422357495

Pin
[]

OTP [] Type 8381

Settings OK Cancel

This screen shows the type of OTP (in this case SMS)



OTP device selection

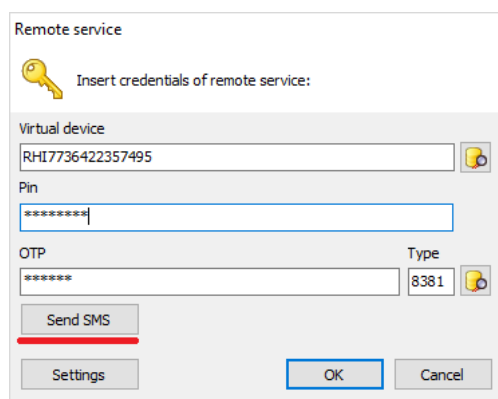
OTP devices

8381: SMS, Namirial, 20151126-1751115CGPI
8565: FISICO, Namirial, 1000416108997

OK Cancel

Figure 120 - Select OTP device

Click on the button **Send SMS** to receive to the mobile number provided during the registration an SMS containing the OTP code to be entered in the OTP box



Remote service

Insert credentials of remote service:

Virtual device
RHI7736422357495

Pin
[]

OTP [] Type 8381

Send SMS

Settings OK Cancel

Figure 121 - Sending SMS OTP

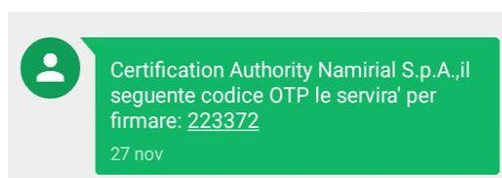


Figure 122 - SMS received

At the end of the operation the following message will occur.

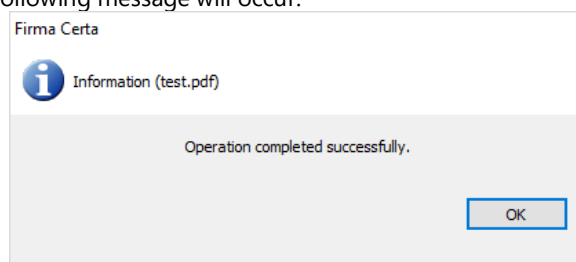


Figure 123 - Confirmation message



12.5 MOBILE OTP PROCEDURE: NAMIRIAL OTP

Enter the PIN received by digital blind envelope.

Click on the icon in the blue box to select the OTP device, then click OK

This screen shows the type of OTP (in this case GENERATOR)

Figure 124 - Select OTP device

Open Namirial OTP application and enter the code in the OTP box

Figure 125 - OTP Generator

At the end of the operation the following message will occur.

Figure 126 - Confirmation message



12.6 OTP HARDWARE PROCEDURE

12.6.1 OTP ACTIVATION

Log on to [User Private Area](#), using the credentials Username and Password received by e-mail at the e-mail address provided during the registration.

PRIVATE AREA CREDENTIALS RECOVERY: In case of loss of the username and / or password, you can proceed to the recovery by clicking on "I don't remember the username" or "I don't remember the password" and following the instructions. If the problem will persist the credentials may be requested sending an e-mail to: helpdesk@firmacerta.it providing the signature holder's tax code.

At the first access the portal will recognize if the OTP device is not active yet.

Generate the code with the OTP pressing the button on the device, then add the code generated in the OTP code field and press **Activate OTP**.



Figure 127 – Activation Otp

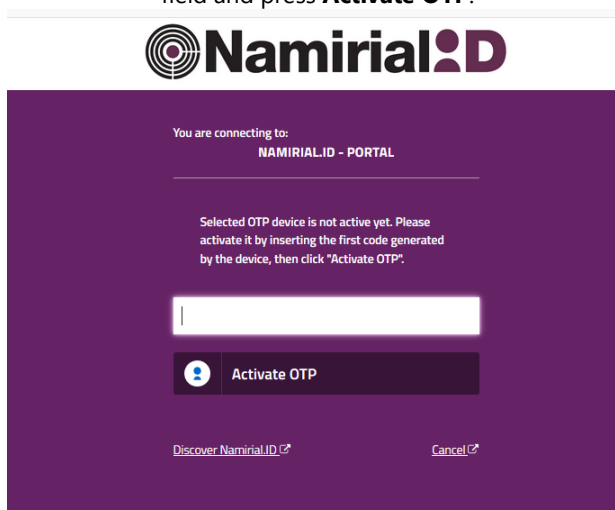
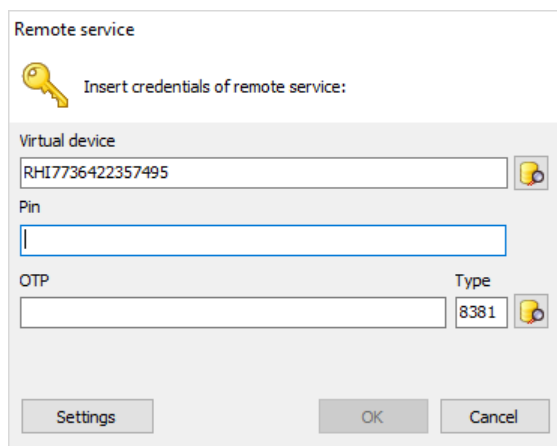


Figure 128 - Private user Area

Enter the device PIN received by digital blind envelope.

Click on the icon in the red box to select the OTP device, then click OK



Remote service

Insert credentials of remote service:

Virtual device
RHI7736422357495

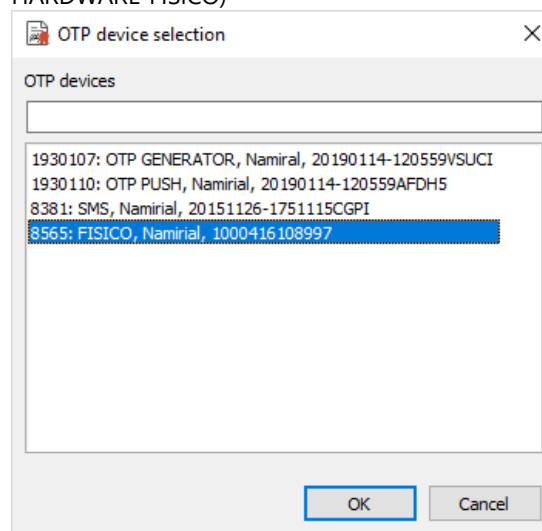
Pin
[Empty field]

OTP
[Empty field]

Type
8381

Settings OK Cancel

This screen shows the type of OTP (in this case
HARDWARE-FISICO)



OTP device selection

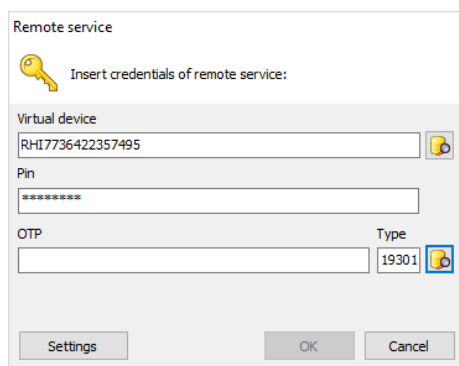
OTP devices

1930107: OTP GENERATOR, Namiral, 20190114-120559VSUCI
1930110: OTP PUSH, Namiral, 20190114-120559AFDH5
8381: SMS, Namiral, 20151126-1751115CGPI
8565: FISICO, Namiral, 1000416108997

OK Cancel

Figure 129 - Select OTP device

After generating the code thanks to the assigned device, enter it into the OTP field



Remote service

Insert credentials of remote service:

Virtual device
RHI7736422357495

Pin

OTP
[Empty field]

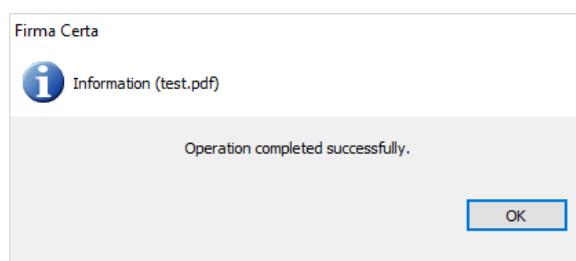
Type
19301

Settings OK Cancel



Figure 130 - OTP Body Raised

At the end of the operation the following message will occur.



Firma Certa

Information (test.pdf)

Operation completed successfully.

OK

Figure 131 - Confirmation message



13 WEB AUTHENTICATION

To import the certificates we kindly invite you to follow the guide published in our portal at the following link:
<http://download.firmacerta.it/pdf/manualeAutenticazioneWeb.pdf>

14 APPENDICE J: BIT4ID – LINUX

Download and install the Bit4id PKI Manager Driver Manager, at the following link:

- [File .deb: 64 bit](#) e [file .deb 32bit](#)
- [File .rpm 64bit](#) e [file rpm 32bit](#)

Open Show Applications and look for the Bit4id PKI Manager software.



Figure 132 - DashBoard Linux



The Bi4id software allows the user to use the Change PIN and the PIN unblock functions, for smartcard and token signature devices.

The PUK change is a function that can only be activated with the **Ctrl + A** key combination

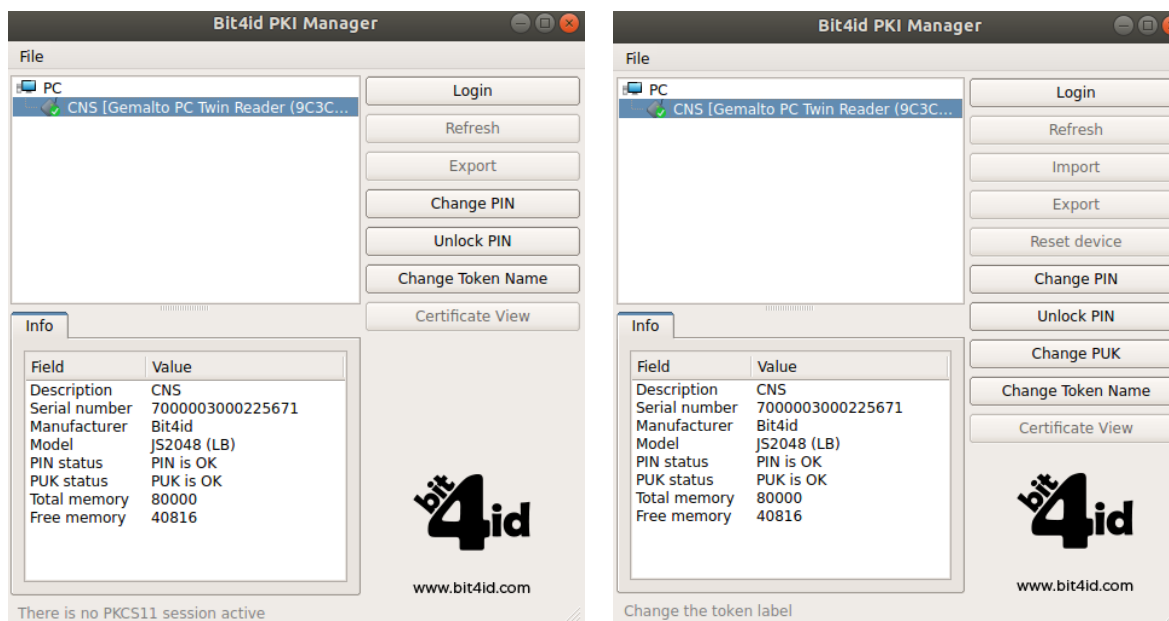


Figure 133 - Bit4id PKI Manager Advanced Functions

14.1 CHANGE PIN

Change the current PIN by entering a new PIN (insertion and verification).

ATTENTION: The Remote Signature's holder can change the PIN from the [Private User Area](#) in the section > User > Digital Signature > Management.

Figure 134 - Change PIN



14.2 UNLOCK PIN

Function required to unlock the PIN. Enter the PUK Code (8-digit numerical code) in the blind envelope.

ATTENTION: before the unlocking procedure it is necessary to have the blind envelope received after the device issuance.

After 3 incorrect attempts of the PUK Code the device will be permanently locked and it will be necessary to request a new signature device.

The 'Unlock PIN' dialog box has a title bar with a close button. It contains the following elements:

- PUK:** A text input field.
- PUK Status:** Displays 'PUK is OK'.
- New PIN:** A text input field.
- Min lenght: 4** and **Max lenght: 8:** Text labels indicating the required length for the new PIN.
- Repeat new PIN:** A text input field.
- OK** and **Cancel** buttons at the bottom right.

Figure 135 - Unlock PIN

14.3 CHANGE PUK

It allows modifying the current PUK assigned by Namirial through the insertion of a new PUK, chosen by the user (insertion and verification).

ATTENTION:

The Remote Signature's Holder can not be changed.

Namirial is not responsible for any improper use of this function. In case of loss of the puk code it will not be possible to recover it and it will be necessary to request a new signature device.

The 'Change PUK' dialog box has a title bar with a close button. It contains the following elements:

- Old PUK:** A text input field.
- PUK Status:** Displays 'PUK is OK'.
- New PUK:** A text input field.
- Min lenght: 4** and **Max lenght: 8:** Text labels indicating the required length for the new PUK.
- Repeat new PUK:** A text input field.
- OK** and **Cancel** buttons at the bottom right.

Figure 136 - Change PUK



15 APPENDICE K: BIT4ID – MACOS

Download and install the Bit4id PKI Manager Driver Manager, at the following [link](#):

Open **Finder > Applications**, otherwise click on **Launchpad** and search for the **PIN Manager** software in the list of applications.

Open **Finder > Applications > PIN Manager**

Click on **Launchpad** and search for the **PIN Manager** software in the list of applications

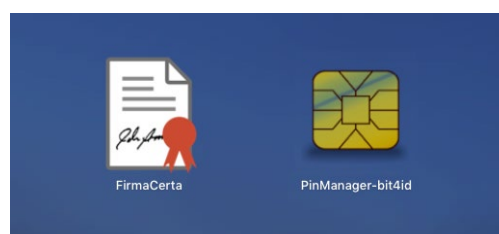
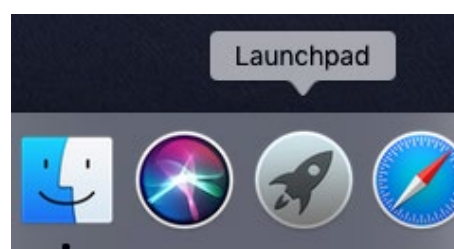
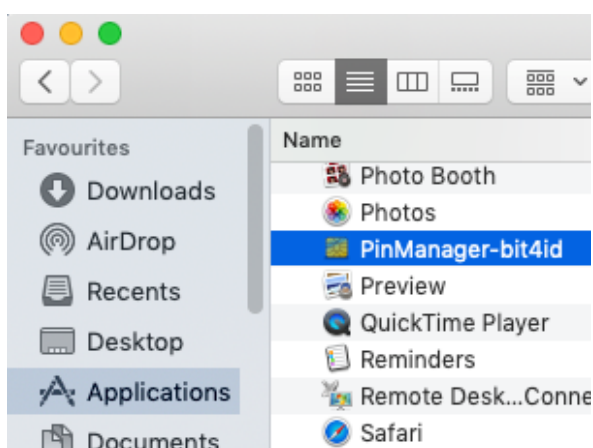


Figure 137 - PIN Manager Opening

The Bi4id software allows the use of the Change PIN and Unlock Pin functions.

The PUK change is a function that can only be activated with the key combination of **CMD + A**

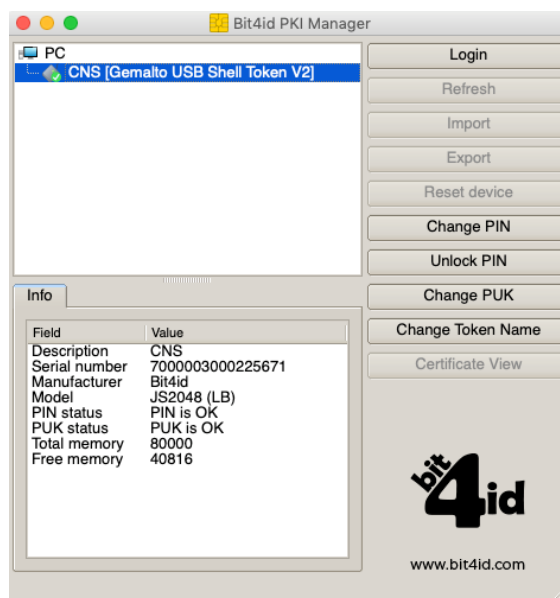


Figure 138 - Bit4id PKI Manager Advanced Functions



15.1 CHANGE PIN

Change the current PIN by entering a new PIN (insertion and verification).

ATTENTION: The Remote Signature's Holder can change the PIN from the [Private User Area](#) in the section > User > Digital Signature > Management.

Change PIN

Old PIN

PIN Status PIN is OK

New PIN

Min lenght: 4
Max lenght: 8

Repeat new PIN

OK Cancel

Figure 139 - Change PIN

15.2 UNLOCK PIN

Function required to unlock the PIN. Enter the PUK Code (8-digit numerical code) in the blind envelope.

ATTENTION: before the unlocking procedure it is necessary to have the blind envelope received after the device issuance.

After 3 incorrect attempts of the PUK Code the device will be permanently locked and it will be necessary to request a new signature device.

Unlock PIN

PUK

PUK Status PUK is OK

New PIN

Min lenght: 4
Max lenght: 8

Repeat new PIN

OK Cancel

Figure 140 - Unlock PIN



15.3 CHANGE PUK

It allows to modify the current PUK assigned by Namirial through the insertion of a new PUK chosen by the user (insertion and verification).

ATTENTION:

The Remote Signature's Holder can not be changed.

Namirial is not responsible for any improper use of this function. In case of loss of the puk code it will not be possible to recover it and it will be necessary to request a new signature device.

Change PUK

Old PUK

PUK Status PUK is OK

New PUK

Min lenght: 4
Max lenght: 8

Repeat new PUK

OK Cancel

Figure 141 - Change PUK

REFERENCES

NUMBER	DESCRIPTION
[I]	<...>
[II]	<...>



TABLES INDEX

Table 1 - Definitions and Acronyms.....	9
---	---

FIGURES INDEX

Figure 1 - Wizard firmacerta	10
Figure 2 -Select the destination folder.....	10
Figure 3 -Installation confirmation.....	11
Figure 4 - Successful installation message.....	11
Figure 5 - FirmaCerta Graphical Interface	12
Figure 6 - Sub-menu of signature	12
Figure 7 - Introduction of the signature's function.....	13
Figure 8 - Introduction of countersignature function.....	13
Figure 9 -Introduction function signature and Brand	13
Figure 10 - Introduction verification function	13
Figure 11 - Introduction of Brand function.....	14
Figure 12 - The Device Management Panel	14
Figure 13 - Function Code Change	14
Figure 14 - PIN Unlocking function.....	15
Figure 15 - Puk change function.....	15
Figure 16 - Displays of Certified function.....	16
Figure 17 - Verification function device.....	17
Figure 18 - Introduction of certificates renewal's function	17
Figure 19 - Marker in the template.....	18
Figure 20 - Background Signature.....	19
Figure 21 - General Signature Properties	19



Figure 22 - Search keywords.....	20
Figure 23 - Utility Panel.....	21
Figure 24 - Introduction to Protect FirmaCerta	21
Figure 25 - Panel General Options	22
Figure 26 - Options: File Management.....	23
Figure 27 - Options: URL	23
Figure 28 - Options Web Services	23
Figure 29 - Options Information	24
Figure 30 - Options: Configure Proxy.....	24
Figure 31 - Signature Options Panel	25
Figure 32 - Options: PDF Logo.....	26
Figure 33 - Options: Verification Options.....	26
Figure 34 - Graphometric Signing Options Panel.....	27
Figure 35 - Options Signature graphometric.....	27
Figure 36 - Graphometric Options: License Activation.....	28
Figure 37 - Graphometric Options: Information Privacy.....	29
Figure 38 - Options Time Stamp.....	29
Figure 39 - Panel: Support.....	30
Figure 40 - Signature Panel.....	31
Figure 41 - Selection of Cades-XAdES signature format	31
Figure 42 - Select the destination folder	32
Figure 43 - Signature Confirmation	32
Figure 44 - Enter the PIN code.....	32
Figure 45 - Operation completed	32
Figure 46 - Selection of Cades-Pades signature format.....	33



Figure 47 - Panel of Countersign	35
Figure 48 - Select the destination folder	36
Figure 49 - Confirmation of overwriting.....	36
Figure 50 - Example screen: verification of the countersigned file.....	36
Figure 51 - Signature Confirmation	37
Figure 52 - Enter the Pin Code.....	37
Figure 53 - Operation completed.....	37
Figure 54 - Utility Panel.....	38
Figure 55 - Timestamp Configuration Options.....	38
Figure 56 - Checking Timestamps	39
Figure 57 - Select the destination folder	39
Figure 58 - Signature Confirmation	39
Figure 59 - PIN Entry	40
Figure 60 - Confirmation of the entered timestamp credentials.....	40
Figure 61 - Operation completed.....	40
Figure 62 - Signature dashboard	40
Figure 63 - Selecting the Cades signature format.....	41
Figure 64 - FirmaCerta Panel Timestamp	42
Figure 65 - Selecting time stamp format.....	42
Figure 66 - Selection of destination folder	42
Figure 67 - Confirms configuration timestamp.....	43
Figure 68 - Operation completed	43
Figure 69 - Example: file marked temporally.....	43
Figure 70 - FirmaCerta Panel Verify for separate the timestamp.....	44
Figure 71 - Timestamp Separation	44



Figure 72 - Select the format.....	44
Figure 73 - Example of timestamped files.....	44
Figure 74 - FirmaCerta Panel Verify	45
Figure 75 - Verification Screen.....	45
Figure 76 - Screen of Result Tab	46
Figure 77 - Screen of Details Tab.....	46
Figure 78 - Verification Settings.....	46
Figure 79 - Screen to view the signed file in verify option	46
Figure 80 - Verification with Sample Screen	48
Figure 81 - Access denied.....	48
Figure 82 - Configuration for automating Pades signature.....	50
Figure 83 - Configuration for automating Cades signature	50
Figure 84 - General Options for timestamp multiple documents.....	50
Figure 85 - Configuration Timestamp Option	50
Figure 86 - Select Timestamp Format.....	51
Figure 87 - Configuration for sign and timestamp multiple documents	51
Figure 88 - Configuration Timestamp Option	51
Figure 89 - Insert PIN	51
Figure 90 - Restrictive clauses	52
Figure 91 - Proxy Configuration.....	52
Figure 92 - Restrictive clauses	53
Figure 93 - Insert PIN	53
Figure 94 - Renew Certificates	54
Figure 95 - Request to view the contract before signing it.....	54
Figure 96 - Confirmation of affixing signature.....	54



Figure 97 - Renewal successfully completed	54
Figure 98 - Namirial Private User Area	55
Figure 99 - Private User Dashboard.....	55
Figure 100 - Certificate Management.....	56
Figure 101 - Signature and renew Process	56
Figure 102 - Example SMS with activation code	57
Figure 103 - Start screen of Virtual OTP. Please tap on the red button	58
Figure 104 - Making tap the green button (Add OTP)	58
Figure 105 - Enter code and label allocation	58
Figure 106 - Start screen of Virtual OTP. Please tap on Add OTP	58
Figure 107 - Enter code and label allocation	58
Figure 108 - Screenshot OTP code generated from APP.....	59
Figure 109 - Enabling SignEngine Service.....	59
Figure 110 - Signature Panel.....	60
Figure 111 - Choosing signature format.....	60
Figure 112 - Selecting the destination folder	61
Figure 113 - Signature Confirmation.....	61
Figure 114 - Remote Service Configuration	61
Figure 115 - Insert Username	61
Figure 116 - Selection of the remote virtual device.....	62
Figure 117 - Wizard Remote Service	62
Figure 118 - Signature information.....	63
Figure 119 - Example of Blind Envelope	63
Figure 120 - Select OTP device	64
Figure 121 - Sending SMS OTP.....	64



Figure 122 - SMS received	64
Figure 123 - Confirmation message	64
Figure 124 - Select OTP device	65
Figure 125 - OTP Generator	65
Figure 126 - Confirmation message	65
Figure 127 – Activation Otp.....	66
Figure 128 - Private user Area	66
Figure 129 - Select OTP device	67
Figure 130 - OTP Body Raised.....	67
Figure 131 - Confirmation message	67
Figure 132 - DashBoard Linux	68
Figure 133 - Bit4id PKI Manager Advanced Functions.....	69
Figure 134 - Change PIN	69
Figure 135 - Unlock PIN.....	70
Figure 136 - Change PUK	70
Figure 137 - PIN Manager Opening	71
Figure 138 - Bit4id PKI Manager Advanced Functions.....	71
Figure 139 - Change PIN	72
Figure 140 - Unlock PIN.....	72
Figure 141 - Change PUK	73