

Registration Authority

Handbook FirmaCerta for MacOS

Category	TSP-Digital Signature	Document ID	NAM-User Guide MacOS	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	_____



Namirial S.p.A.

Registered office, management and administration 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
Tax Code/Company Register of Ancona n. 02046570426 - VAT no. IT02046570426 Share Capital € 6.500.000,00 fully paid-up
Tel. 07163494 s.a. - Fax 199.418016 - info@namirial.com - www.namirial.com



– This page is intentionally left blank –



INDEX

Index	3
Revision History	6
1 Introduction	7
1.1 Document purpose and application range.....	7
1.2 Definition and acronyms used in the document.....	8
2 Installation.....	9
3 Graphic Interface	11
4 Main Functions.....	11
4.1 Signature.....	11
4.2 Sign and Timestamp.....	12
4.3 Countersign.....	12
4.4 Timestamp.....	12
4.5 Verify.....	12
4.6 View.....	12
5 Tools.....	13
5.1 Show Certificates in Signature Device	13
5.2 Check Signature Device	14
5.3 Change PIN	14
5.4 Unlock PIN.....	15
5.5 Change PUK.....	15
5.6 Renew Certificates.....	16
5.7 Options	16
5.7.1 General	16



5.7.2	File.....	17
5.7.3	Verify	17
5.7.4	TimeStamp	18
5.7.5	Updates	18
6	Appendix:	19
6.1	Appendix A: How to sign a document.....	19
6.1.1	Select signature format.....	19
6.1.2	Select signature motivation (Only PDF FILE)	20
6.1.3	Confirmation of signature process	20
6.2	Appendix B: How to countersign a document.....	22
6.2.1	Confirmation of signature process.....	22
6.3	Appendix C: Timestamp parameters configuration	24
6.3.1	Appendix C1: How to timestamp a file	25
6.3.2	Appendix C2: How to sign and put the timestamp in a document	28
6.4	Appendix D: how to verify a file	31
6.5	Appendix E: certificate renewal.....	32
6.5.1	Proxy configuration	32
6.5.2	Smartcard and token renewal	33
6.6	Appendix F: Remote signature guide.....	35
6.6.1	How to sign a file	35
6.6.2	Virtual OTP procedure: Namirial OTP	37
6.6.3	Sms OTP procedure.....	41
6.6.4	Hardware OTP procedure.....	42
6.7	Appendix H: Bit4id – MacOS.....	44
6.7.1	Change PIN	45
6.7.2	Unlock PIN.....	45



6.7.3	Change PUK	46
References	47
Tables Index	48
Figures Index	48



REVISION HISTORY

VERSION	1.0
Date	01/02/2019
Reasons	First document issuance
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.

Firma Certa 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 APPLICATION RANGE

This document, identified by the code shown in the title, describes the steps to follow to install the Client Firma Certa and bit4id drivers for the recognition of the certificates; it also describes the functions of the Client Firma Certa 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, Firma Certa during the verification operation of the document will fail.



1.2 DEFINITION AND ACRONYMS USED IN THE DOCUMENT

TERM	DEFINITION
Digital signature	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 a 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 it with another to determine the temporal order. The practical application is called timestamping. A marked file extension has temporally .m7m
PDF: (Portable Document Format)	Graphic file format developed by Adobe Systems. This standard is normally used to make available representative documents, printed pages of books, magazines, brochures, catalogues, 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 to read PDF documents.
Smart Card	Is a hardware device similar to a credit card that has potential for processing and storing high-security data.
Token USB	Is a usb key that includes a similar chip to that of a smart card put directly into a USB port: thus it has the same smart card functions with the same chip, drivers and bundled software but do not require a reader having a direct connection 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 the 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.
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.
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.

Table 1 - Definitions and Acronyms



2 INSTALLATION

Download the software from the following site www.firmacerta.it, section *Download > Software Firmacerta*, > Versione Desktop per Mac ([LINK](#)).

Then, start FirmaCerta.dmg file and:

1. Drag the file FirmaCerta into the folder **Applicazioni**;
2. Start the packet *hid-switch-signed.pkg*
3. Start the packet *bit4id-middleware-user-signed.pkg* (once the installation of this packet will be completed it will be necessary to restart the system).



Figure 1 - Firmacerta Installation

Note: For devices with serial number 2203... 2204... please install [SafeDive](#).

Attention: At the first start of FirmaCerta software a warning message will be shown to the user to inform that: "FirmaCerta software belongs to a non-identified developer". This message appears for all the application that does not belong to Apple Store.

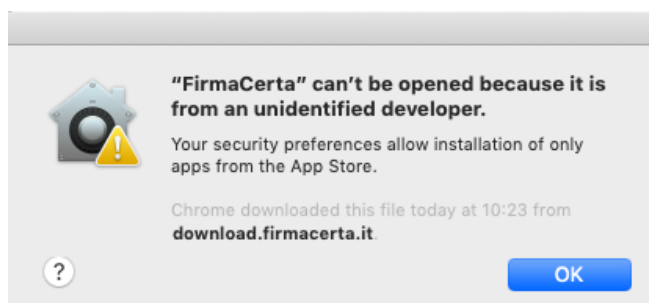


Figure 2 - Warning: unidentified developer



To choose to ignore the security setting opening in any case the app:

1. In Finder > Applications, find the app to open. *Please, don't use Launchpad for this operation because Launchpad does not allow accessing to the quick menu.*
2. Click on the icon of the app pressing the **Ctrl** key (alternatively, click using the right button), then choose **Open** from the quick menu.
3. Clicking on Open you will confirm to open anyway the app that will be saved as an exception in the security settings, so in the future the user will be able to open it with a double click on the app itself, as an authorized application.

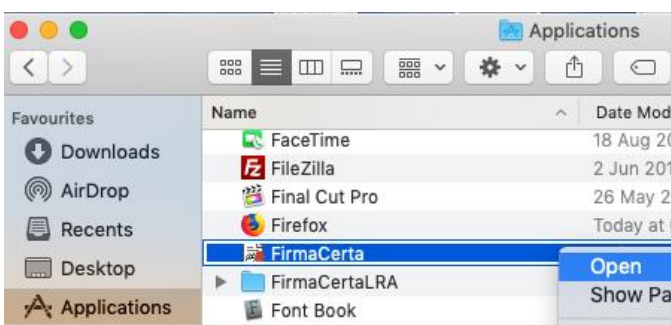


Figure 3 - firmacerta installation solution 1a

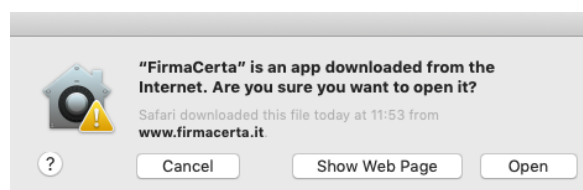


Figure 4 - firmacerta installation solution 1b

Note:

The user can authorize an exception for an app previously locked, clicking on the button **“Open Anyway”** from the panel General in preferences panel **“Security & Privacy”**.

To open this panel choose from the menu **Apple > System Preferences...** and click on **“Security & Privacy”**, then click on **General**.

Once you have tried to open the app this button is available for one hour approximately

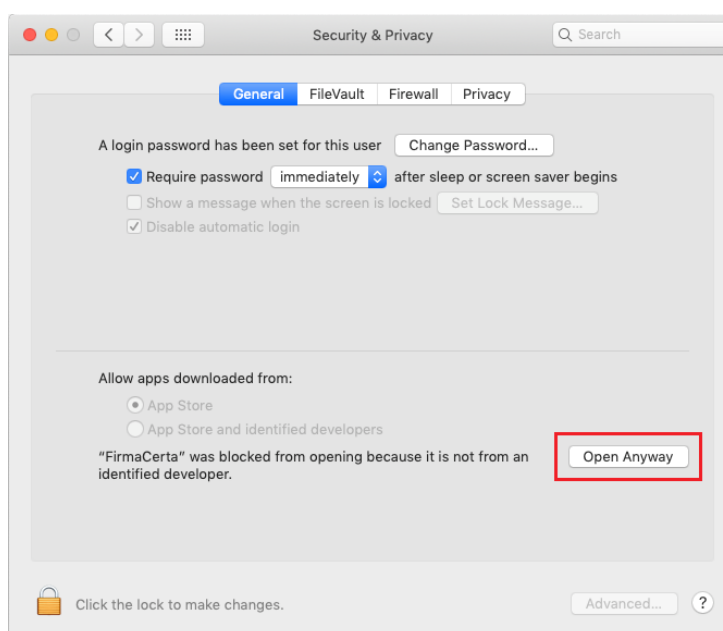


Figure 5 - firmacerta installation 2nd solution



3 GRAPHIC INTERFACE

FirmaCerta graphic interface is simple and intuitive.

The menu is made up of the main functions of the software:

- Digitally sign any files;
- Affix Timestamp;
- View and Verify digitally signed files;



Figure 6 - Firmacerta Graphic Interface

For further informations about the principal functions see [Chapter 4](#)

In the task bar is possible to manage the software settings and the use of specific functions as:

- Activate signature device
- Show signature device certificates
- Check signature device
- Certificates renewal



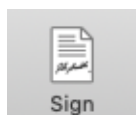
Figure 7 - Firmacerta: Tools Bar

For further software settings and specific functions use see [Chapter 5](#)

4 MAIN FUNCTIONS

4.1 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 software window and clicking on the icon "Sign".

From the tools bar **File > Add File** it will be possible to search for the file you want to sign, inside the folders of your computer.

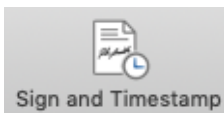
From Software: Clicking on the icon Sign you can search for the file you want to sign, inside the folders of your computer.

Once you press "Sign" the software will ask you to choose the directory 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 F: Remote Signature](#)



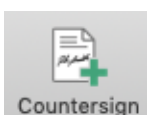
4.2 SIGN AND TIMESTAMP



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 for the signed file. Once you press "Sign and Timestamp" and entering the PIN code the software will require to enter the credentials "Username" and "Password" to use the timestamps.

See the whole procedure for Sign and Timestamp a document [Appendix C2: How to Sign and Timestamp a document](#)

4.3 COUNTERSIGN



With this function 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 B: How to countersign](#)

4.4 TIMESTAMP



After selecting a file, with this feature you can temporally mark the same file giving a certain date/time to the document, opposable against third party.

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 C1: How to TimeStamp a file](#)

4.5 VERIFY

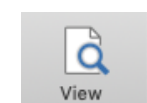


The function allows verifying and displaying the signature/signatures status on the document.

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 is possible to open the window **Details** to show the main features of the certificate (Type, Issuer Entity, Owner, Certificate validity)

See the whole procedure to check a document [Appendix D: How to verify and view a file](#)

4.6 VIEW



This function allows you to view digitally signed documents in .p7m format



5 TOOLS

5.1 SHOW CERTIFICATES IN SIGNATURE DEVICE

In the left column the two certificates are valued: **Authentication** (TAX Code) and **Subscription** (Name and Surname).

In the right column the **Result** of the verification is shown and in **Details** it is deepened.

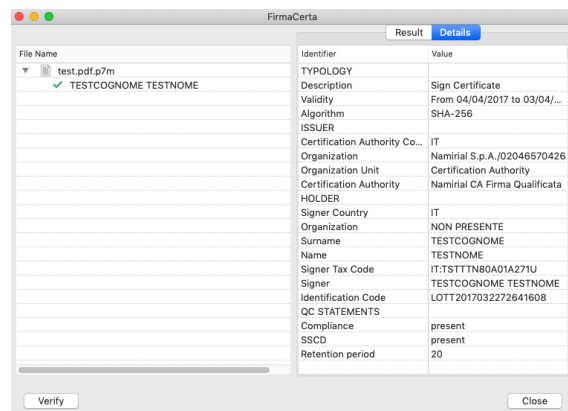
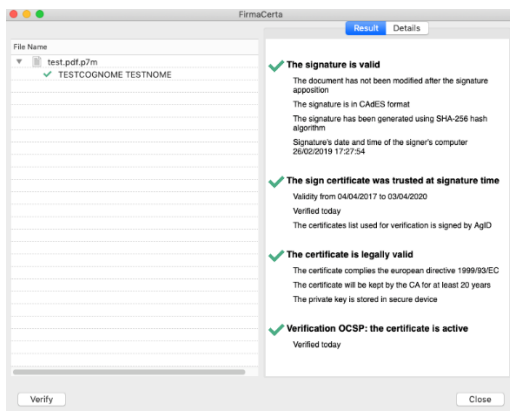
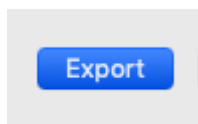


Figure 8 - Show Certificates in signature device



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

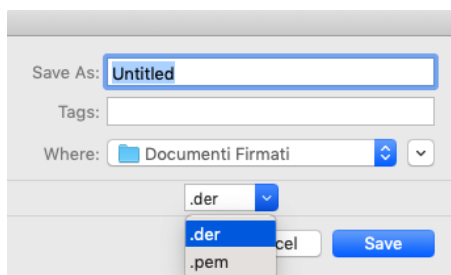


Figure 9 - Export Certificates

.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.

.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 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.



5.2 CHECK SIGNATURE DEVICE

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

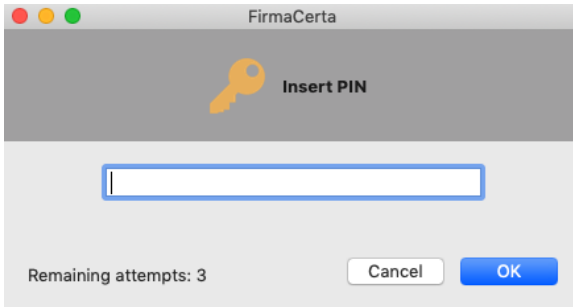


Figure 10 - insert PIN for check signature device

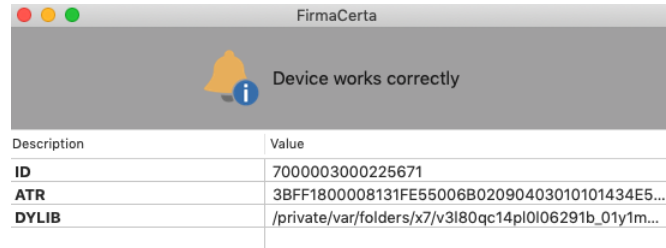


Figure 11 - Result Check Device

5.3 CHANGE PIN

It allows editing the current PIN code through the insertion of a new PIN (insertion and verification).

Note:

- For remote digital signature holders is possible to modify the PIN code by accessing to the user [Private Area](#) > User > Digital signature > Management.
- It's possible to Change PIN also with the Middleware Bit4id as mentioned in the [Appendix H](#)

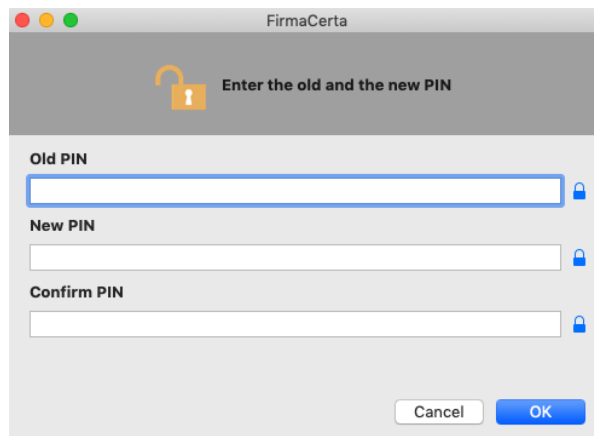


Figure 12 - Change PIN



5.4 UNLOCK PIN

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

It's possible to Unlock PIN also with the Middleware Bit4id as mentioned in the [Appendix H](#)

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 be permanently locked and it will be necessary to request a new signature device.

The screenshot shows a macOS-style dialog box titled 'FirmaCerta'. The main content area has a grey background with a white border. At the top, there's a header with a lock icon and the text 'Enter the PUK and the new PIN'. Below this, there are three input fields: 'PUK', 'New PIN', and 'Confirm PIN'. Each field has a small lock icon to its right. At the bottom right, there are two buttons: 'Cancel' and 'OK'.

Figure 13 - Unlock PIN

5.5 CHANGE PUK

It allows editing the current PUK code through the insertion of a new PUK (insertion and verification).

Note:

- For remote digital signature holders is possible to modify the PIN code by accessing to the user [Private Area](#)> User> Digital signature> Management.
- It's possible to Change PUK also with the Middleware Bit4id as mentioned in the [Appendix H](#)

The screenshot shows a macOS-style dialog box titled 'FirmaCerta'. The main content area has a grey background with a white border. At the top, there's a header with a lock icon and the text 'Enter the old and the new PUK'. Below this, there are three input fields: 'Old PUK', 'New PUK', and 'Confirm PUK'. Each field has a small lock icon to its right. At the bottom right, there are two buttons: 'Cancel' and 'OK'.

Figure 14 - Change PUK



5.6 RENEW CERTIFICATES

Function required to renew the digital signature certificates for further three years. See the **guide** with all the basic information to renew the certificates at the [Appendix H](#).

ATTENTION:

1. If the user has not been unlocked by RAO the renewal cannot be completed;
2. It's impossible renew the certificates twice.

5.7 OPTIONS

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

5.7.1 GENERAL

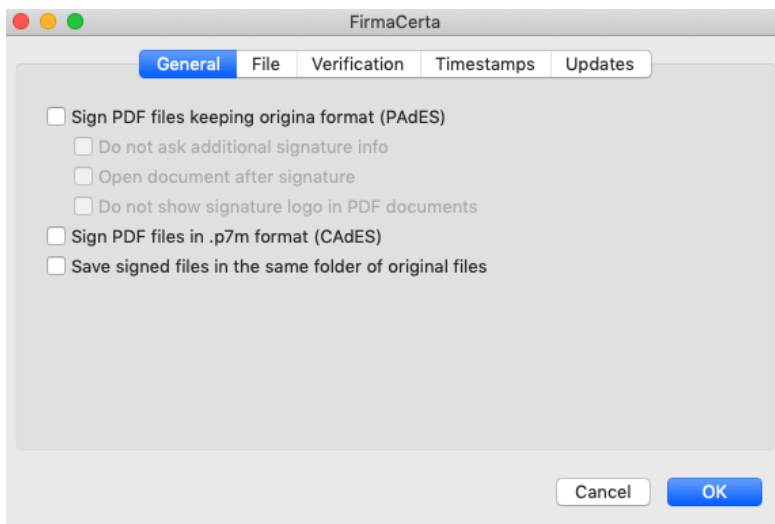


Figure 15 - Options: General

<p>Signature of pdf files maintaining the format (PAdES):</p>	<p>.pdf files will be automatically signed in PAdES format without allowing the user to choose between .p7m or .pdf format</p> <p>It keeps the original signed file format (otherwise converted into .p7m format), giving the users with no specific digital signature software the possibility of view the document.</p>
<ul style="list-style-type: none"> • Do not request additional signature information: 	<p>Optional information will not be displayed in the signed document;</p>
<ul style="list-style-type: none"> • Open the PDF after the signing process: 	<p>The PDF file will be opened with the default program by the computer after the application of the digital signature.</p>
<ul style="list-style-type: none"> • Do not show the signature logo in PDF documents: 	<p>Setting this preference before signing and then viewing the digitally signed PDF file, the signature logo with signer's information will not be reported.</p>



	Note: 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
Signature of pdf files into .p7m format (CADES):	.pdf files will be automatically signed in CADES format without allowing the user to choose between .p7m or .pdf format.
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;

5.7.2 FILE

In this section it is possible to code digitally signed files (.p7m), temporally marked files (.tsd, .tsr, .tst) and protected files (.p7e) in Base64 format.

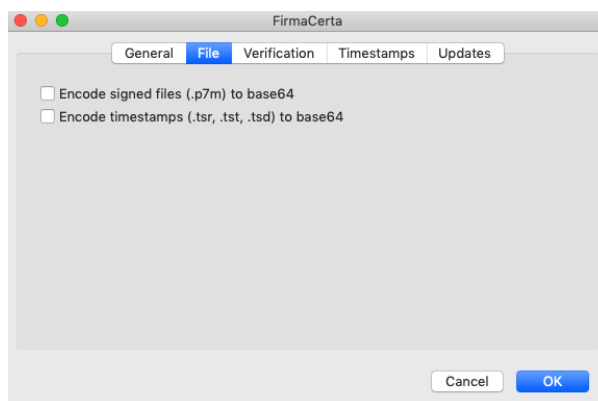


Figure 16 - Options: File

5.7.3 VERIFY

Function to verify and display at the same time the certificate status (active/revoked/suspended) and to check the file when the Verify function starts.

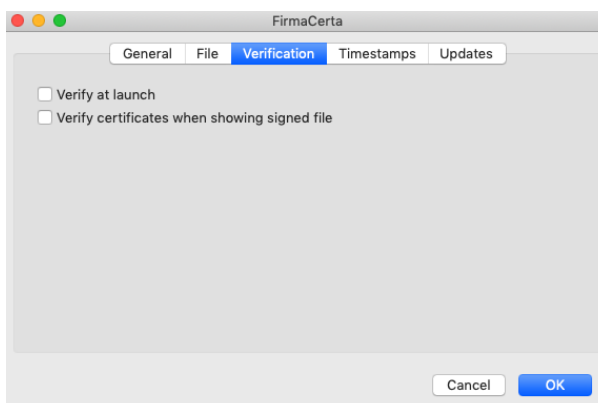


Figure 17 - Options: Verification



5.7.4 TIMESTAMP

This section allows saving the credentials **Username** and **Password** to use the timestamps (if the holder has ones) 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.

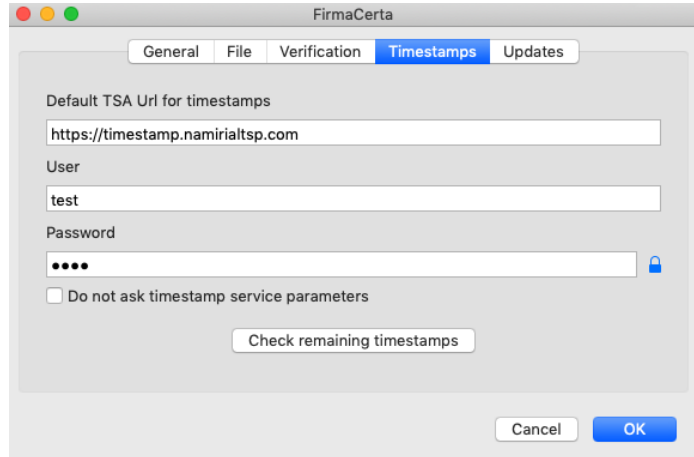


Figure 18 - Options: Timestamps

LINK to use the timestamping service

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

5.7.5 UPDATES

Function to enable/disable the updates check, you can choose if allow the updates to be installed automatically when available, in silent mode.

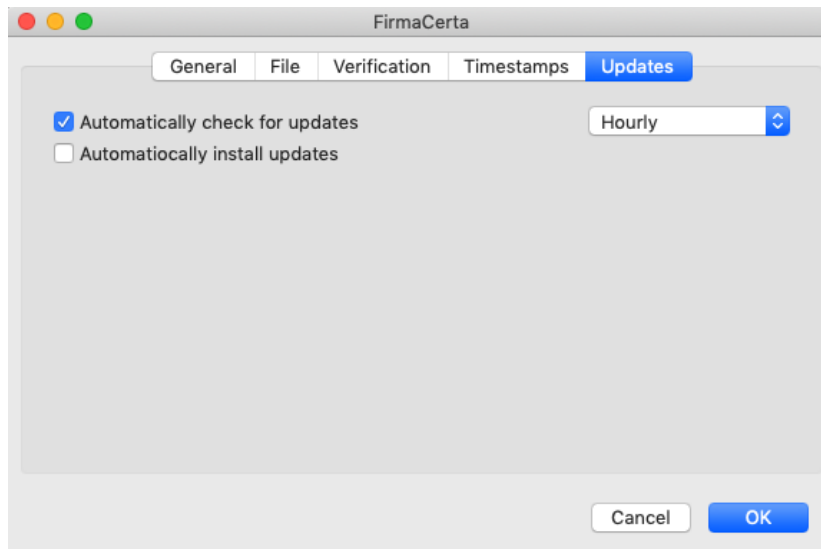


Figure 19 - Options: Updates



6 APPENDIX:

6.1 APPENDIX A: HOW TO SIGN A DOCUMENT

After loading the file to be signed and clicking on the **Signature** function the user will be asked to select a destination folder to save the signed document.

In the following example, a specific folder for digitally signed files has been previously created, then select Signed Documents and click on **Open**.

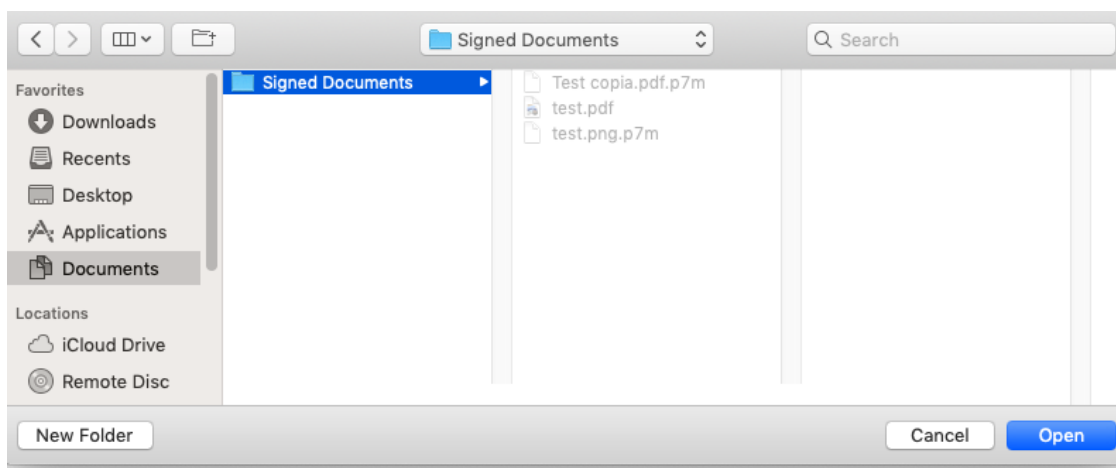


Figure 20 - Selection of the destination folder

6.1.1 SELECT SIGNATURE FORMAT

Select the CADES format to sign the file into .p7m format

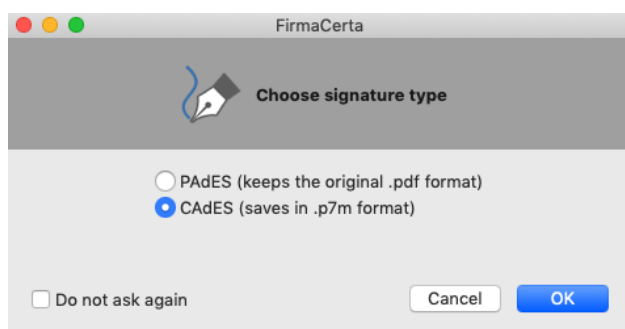


Figure 21 - Selection: CADES format

Select the PAdES format to sign the file into .pdf format

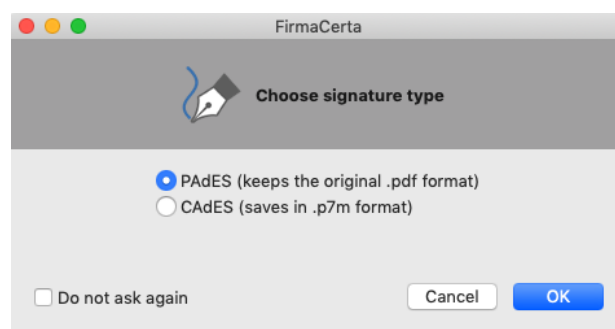


Figure 22 - Selection: PAdES format

Note: the choice of the signature format is available only for .pdf, for every other format the software will automatically apply the extension .p7m

Setting the preference **Do not ask anymore** it will be set automatically not to show the message anymore and it will be necessary to modify the settings from [Options](#) to have the possibility to view again the message.



6.1.2 SELECT SIGNATURE MOTIVATION (ONLY PDF FILE)

This function allows the user to add optional information as *motivation, location, contact information* before completing the signature of the document.

Note: This function is available only for .p7m documents. The use of this function is at the user's choice as an Optional Operation.

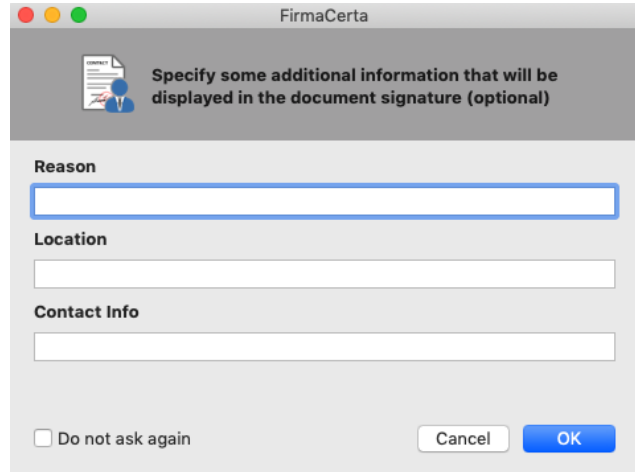


Figure 23 - Signature information

6.1.3 CONFIRMATION OF SIGNATURE PROCESS

Confirmation of the signature application.

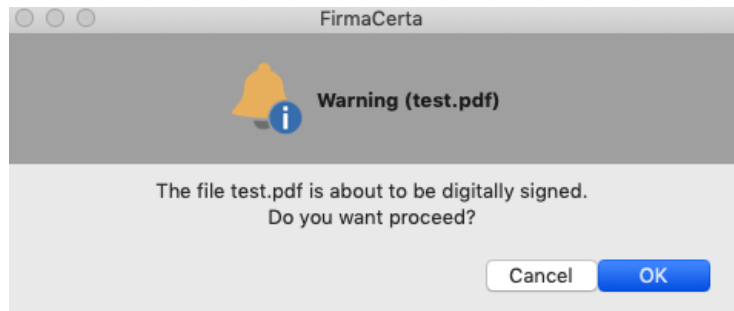


Figure 24 - Confirmation signature process

USB reader device/Token USB selection

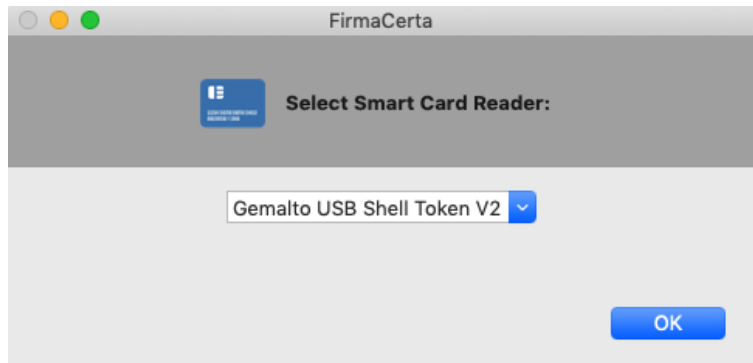


Figure 25 - Selection: signature device reader



Enter the PIN of the signature device and click on **OK**.

Note:

The Pin code has been given with the blind envelope

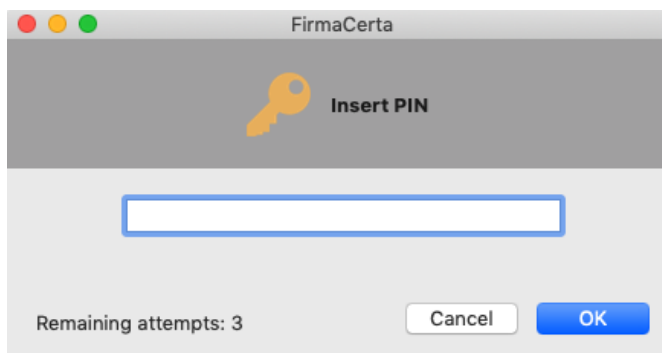


Figure 26 - Insert PIN

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

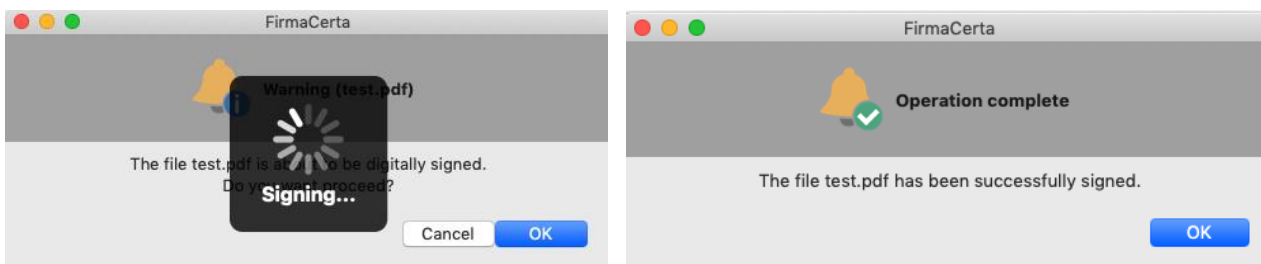


Figure 27 - Signature Process conclusion



6.2 APPENDIX B: HOW TO COUNTERSIGN A DOCUMENT

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

After loading the file digitally signed that you want to countersign, click on the button "Countersign".
In the following example, a specific folder for digitally signed files has been previously created, then select Signed Documents and click on **Open**.

Note: the countersign operation is possible only for digitally signed file in .p7m format

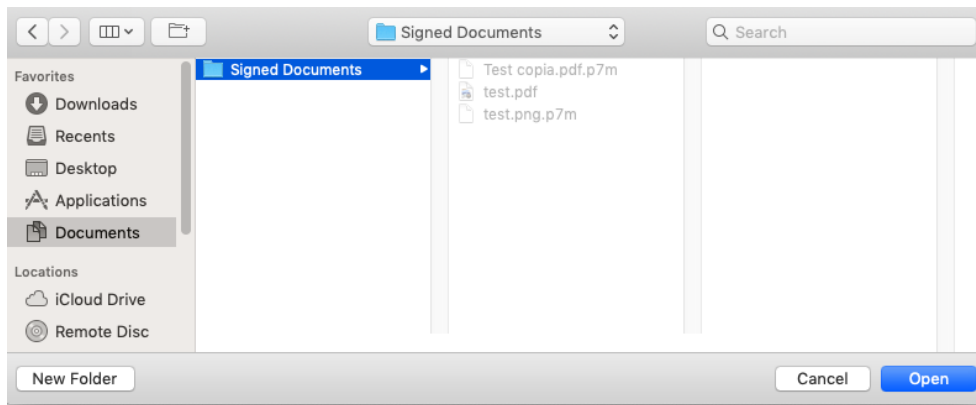


Figure 28 - Selection of the destination folder

6.2.1 CONFIRMATION OF SIGNATURE PROCESS

Confirmation of the signature application.

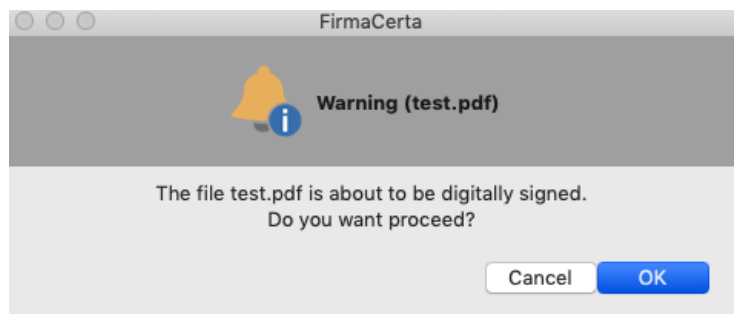


Figure 29 - Confirmation Process



USB reader device/Token USB selection

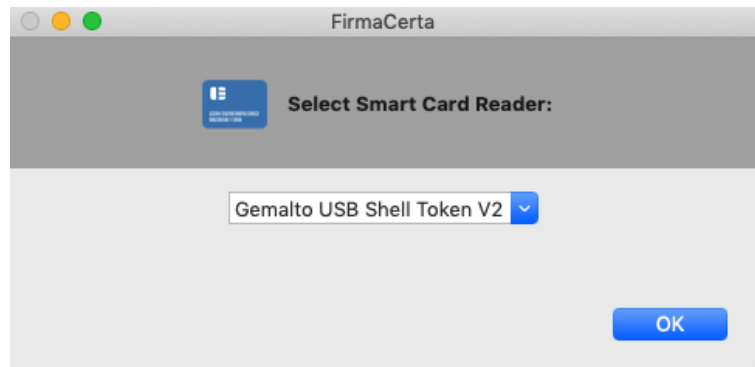


Figure 30 - Select signature device reader

Enter the PIN of the signature device and click on **OK**.

Note:

The Pin code has been given with the blind envelope

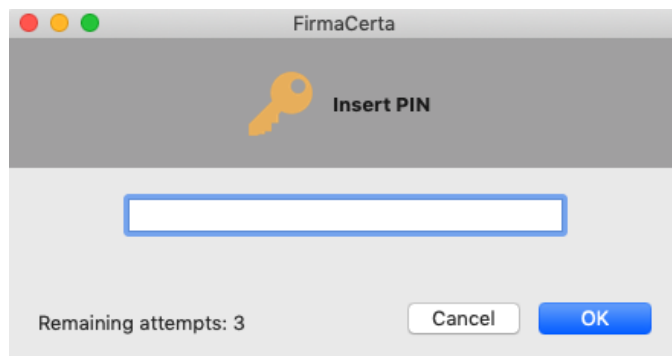


Figure 31 - Insert PIN

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

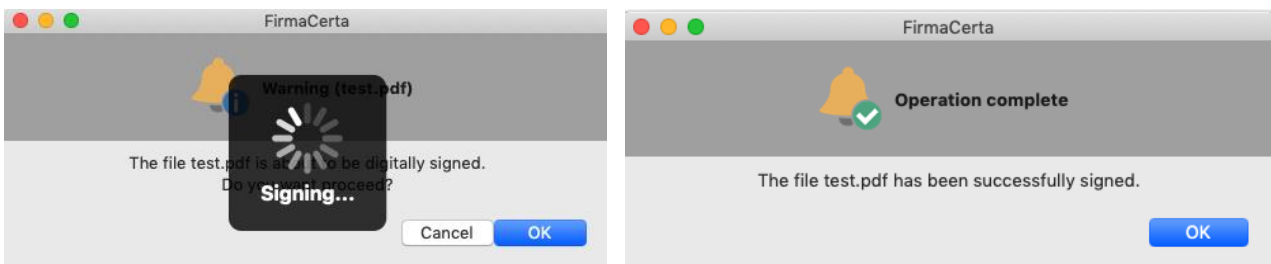


Figure 32 – Completion Signature Process



6.3 APPENDIX C: TIMESTAMP PARAMETERS CONFIGURATION

Before using the Timestamp Service you must configure FirmaCerta software.

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

Open FirmaCerta > Tools > Options > Timestamps

- Verify that the URL is <http://timestamp.namirialtsp.com> or <https://timestamp.namirialtsp.com>
- Enter **Username and Password** and click on **OK**.
- Setting the option "Do not ask timestamp service parameters", the data confirmation during the timestamp process will be not required.

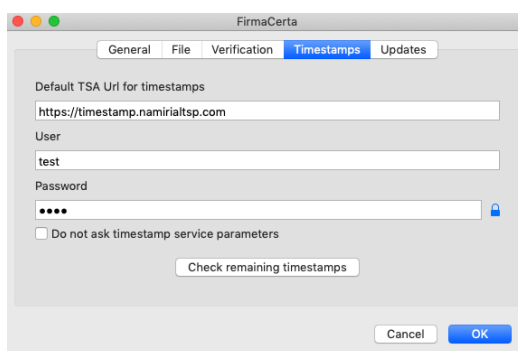


Figure 33 - Timestamps Configuration

- **Note:** 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).

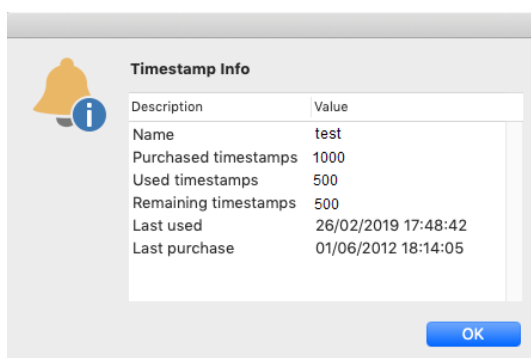


Figure 34 - Check available Timestamps



6.3.1 APPENDIX C1: HOW TO TIMESTAMP A FILE

After loading the file to be timestamped and clicking on the **Timestamp** function the user will be asked to select a destination folder to save the document.

*In the following example, a specific folder for digitally signed files has been previously created, then select Timestamp Documents and click on **Open**.*

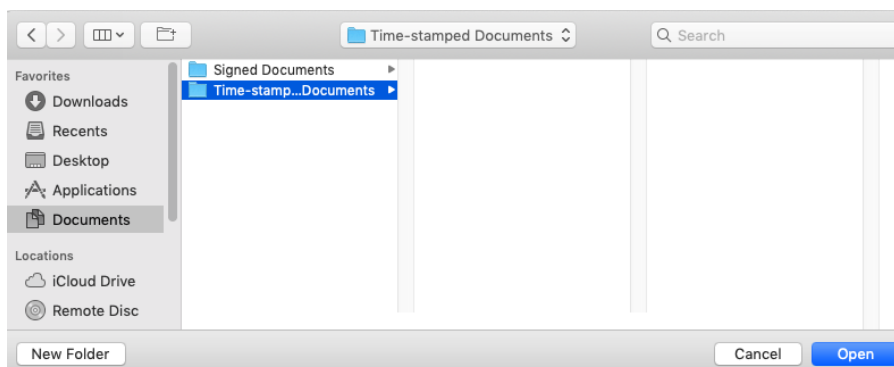


Figure 35 - Selection of the destination folder

Choose the format to mark the document.

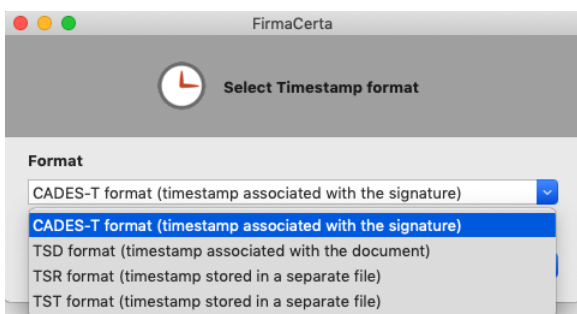


Figure 36 - Selection of Timestamps Format

.TSD (TimeStamp Document): is the **standard format** which contains both the time stamp and the original file to be timestamped, so it allows verifying the accuracy of the timestamp and the contents of the original file. The timestamp is associated with the document.

.TSR (TimeStamp Response): is similar to the format .TST but, in addition, with the response code from the TimeStamp server of the Certification Authority. The IT test, obtained thanks to the verification, it's only about the timestamp accuracy, while it's necessary to have the original file to verify the correspondence between this one and the .tsr file.

.TST (TimeStamp Token): is a file that containing the imprint of the document or file marked not the content of the document itself.

CADES-T o PADES-T: it proves that the signature has existed indeed, in a certain date/hour. The timestamp is associated with a singular signature and it's not separable.



Attention: if the document has been already signed and you want to put the timestamp in it, the software allows the choice of **CADES-T format** (for .p7m file) and **PADES-T format** (for .pdf file).

Example: timestamp of a .p7m file

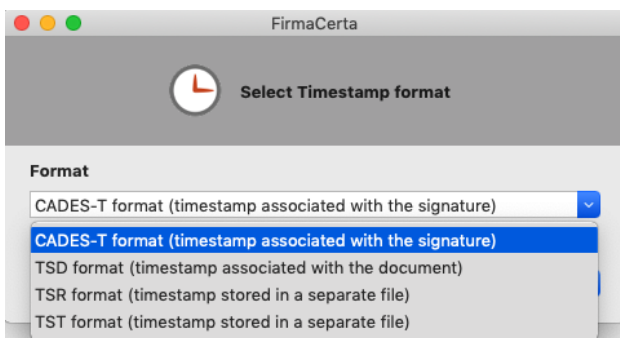


Figure 37 – Select Timestamp format for .p7m file

Example: timestamp of a .pdf file

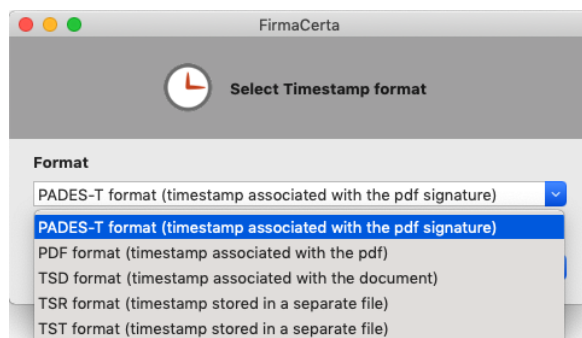


Figure 38 - Select Timestamp format for .pdf file

6.3.1.1 TIMESTAMP PARAMETERS CONFIGURATION

It's necessary to configure the parameters for the timestamp service.

Note:

- If the configuration of the timestamp has been done, the fields **URL**, **Username** and **Password** will be completed.
- Setting the option "**Do not ask access parameters anymore**", the data confirmation during the timestamp process will be not required, to set again this option it will be necessary to modify the settings from [Options Timestamps](#).

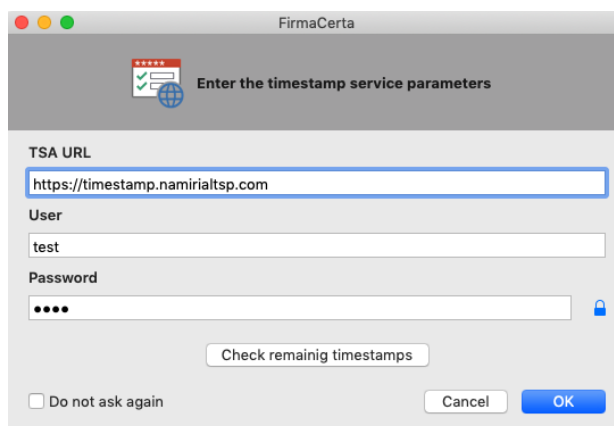


Figure 39 - Enter Timestamp Parameters



6.3.1.2 CONCLUSION OF THE TIMESTAMP PROCESS

Confirmation of the signature application.

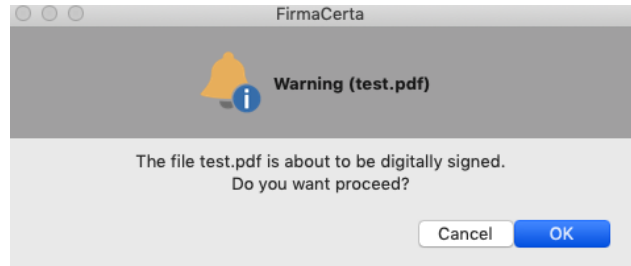


Figure 40 - Confirmation signature process

USB reader device/Token USB selection

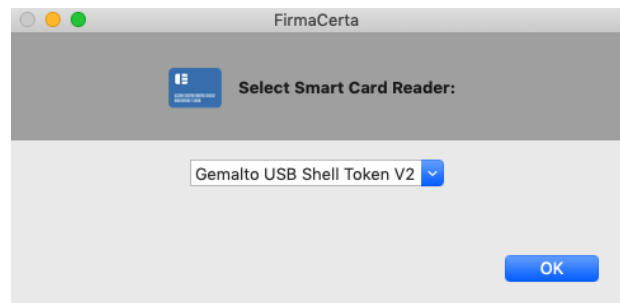


Figure 41 - Select Signature device reader

Enter the PIN of the signature device and click on **OK**.

Note:

The Pin code has been given with the blind envelope

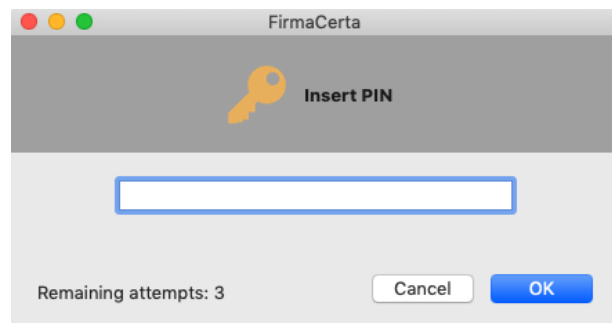


Figure 42 - Insert PIN

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

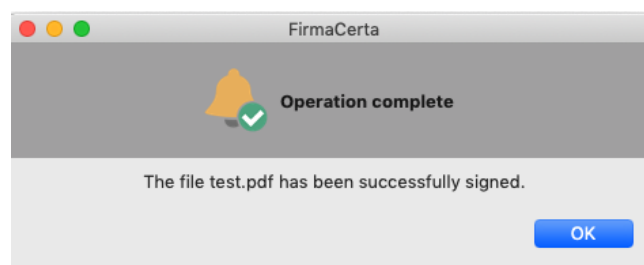


Figure 43 - Signature Process Complete



6.3.2 APPENDIX C2: HOW TO SIGN AND PUT THE TIMESTAMP IN A DOCUMENT

After loading the file choose this function to sign and put the timestamp in one singular operation.

Once signed and timestamped the file, the format will be **CADES-T** (ex. filename.pdf.P7M).

With a CADES-T format (default format) or PAdES-T (format available only for PDF document) the timestamp is associated with a singular signature and is *not separable*.

After loading the file and choosing the function **Sign and Timestamp**, the user will be required to select a destination folder to save the file.

In the following example, a specific folder for digitally signed files has been previously created, then select *Timestamped Documents* and click on **Open**.

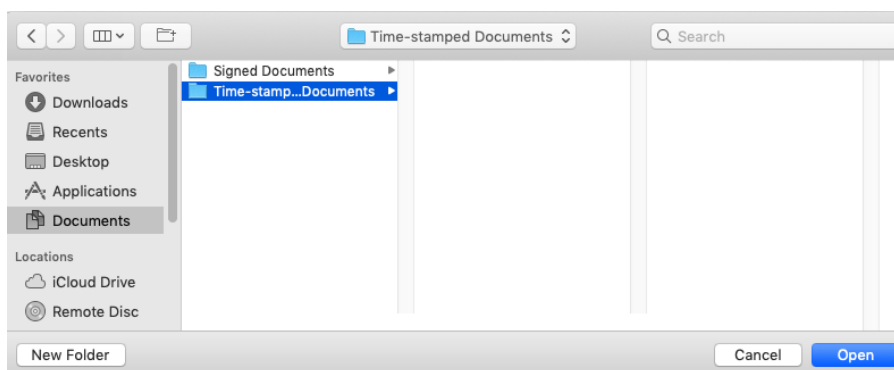


Figure 44 - Selection of the destination folder

6.3.2.1 SELECT SIGNATURE FORMAT

Select the CADES format to sign the file into .p7m format

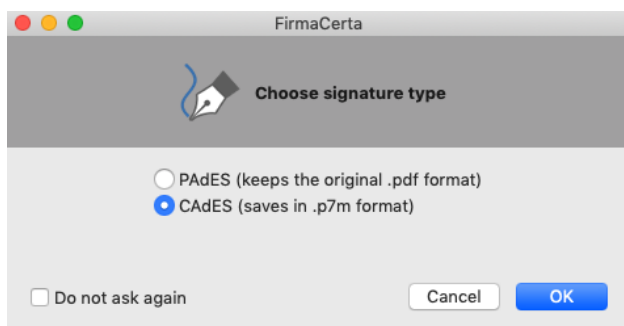


Figure 45 - CADES format selection

Select the PAdES format to sign the file into .pdf format

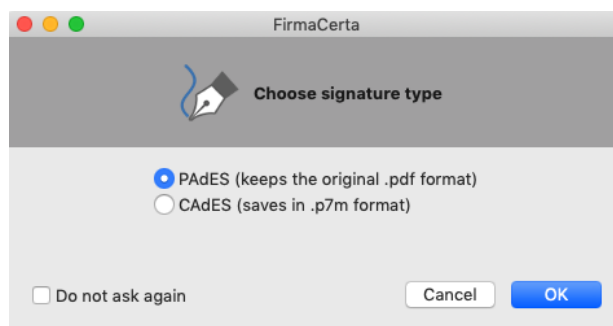


Figure 46 - PAdES format selection

Note: the choice of the signature format is available only for .pdf, for every other format the software will automatically applied the extension .p7m

Marking the preference **Do not ask anymore** it will be set automatically, and to remove it will be necessary to modify the settings from [Options](#).



6.3.2.2 SELECT SIGNATURE MOTIVATION (ONLY PDF FILE)

This function allows the user to add optional informations as *motivation, location, contact informations* before completing the signature of the document.

Note: This function is available only for .pdf documents. The use of this function is at the user's choice as an Optional Operation.

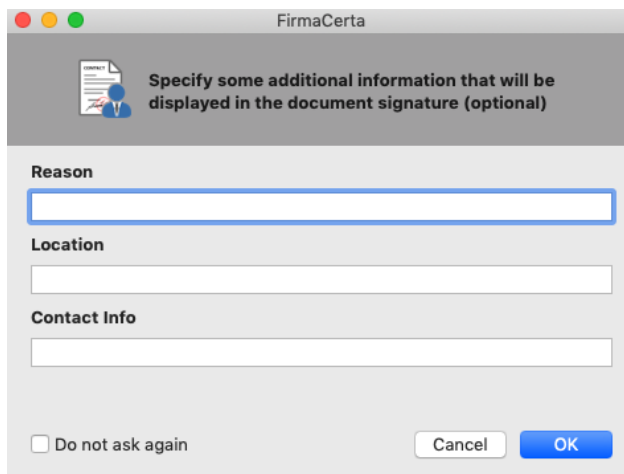


Figure 47 - Signature information

6.3.2.3 TIMESTAMP PARAMETERS CONFIGURATION

It's necessary to configure the parameters for the timestamp service.

Note:

- If the configuration of the timestamp has been done, the fields **URL**, **Username** and **Password** will be completed.
- Setting the option "**Do not ask access parameters anymore**", the data confirmation during the timestamp process will be not required, *to set again this option it will be necessary to modify the settings from [Option Timestamps](#).*

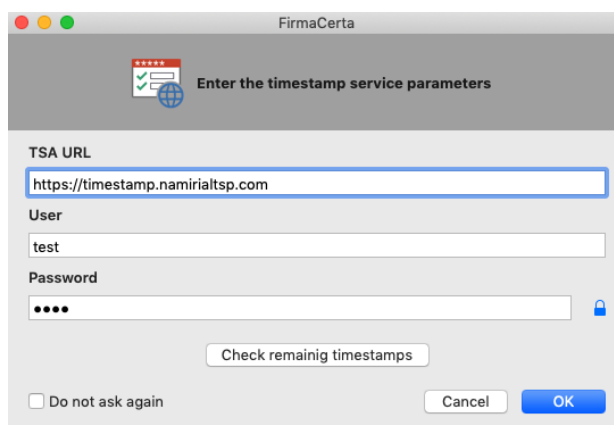


Figure 48 - Timestamps Parameters



6.3.2.4 CONCLUSION OF SIGNATURE AND TIMESTAMP PROCESS

Confirmation of the signature application.

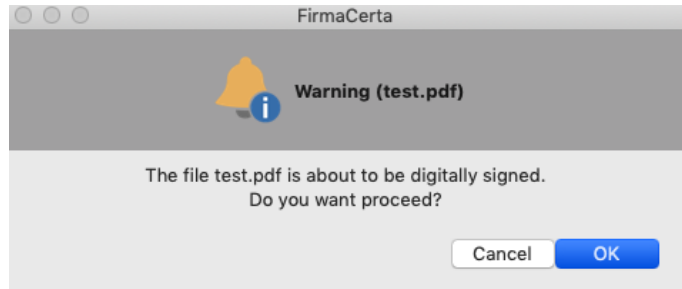


Figure 49 – Confirmation Signature Process

USB reader device/Token USB selection

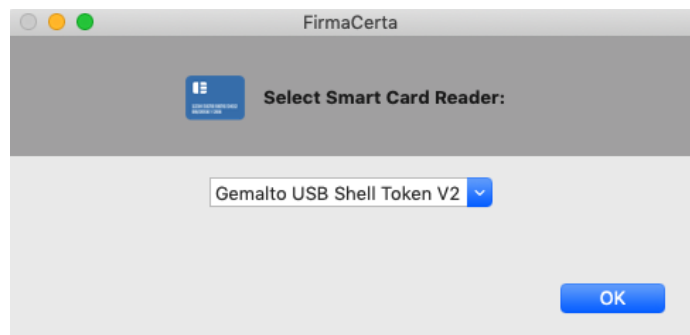


Figure 50 - Select signature device reader

Enter the PIN of the signature device and click on **OK**.

Note:

The Pin code has been given with the blind envelope

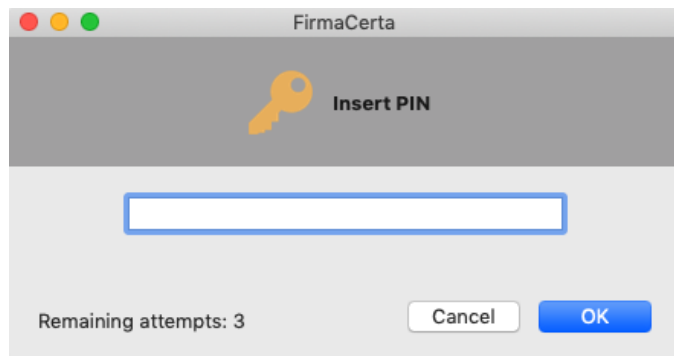


Figure 51 - Insert PIN

Attendere il tempo di elaborazione e premere **OK** per concludere il processo di firma.

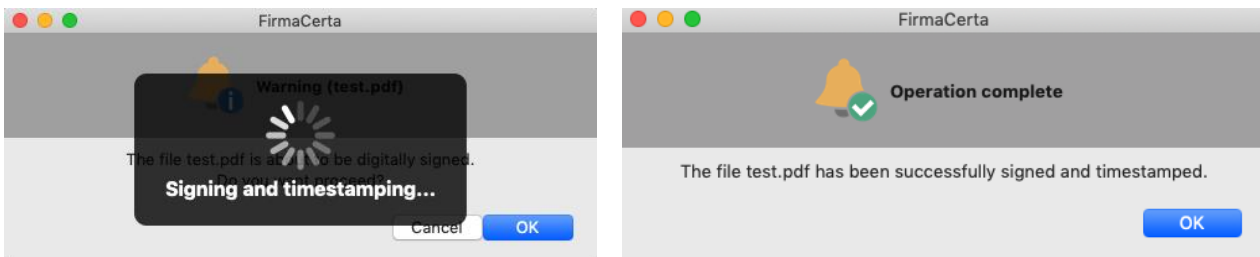


Figure 52 - Conclusion Signature Process



6.4 APPENDIX D: HOW TO VERIFY A FILE

After loading the file to be verified and clicking on the function **Verify** a summary window will be opened.

Note:

if the message ***the signature certificate has not been verified*** appears, it means that the verification has not been started automatically (to activate automatically the verification at the file opening it will be necessary to modify, manually, in the [Verification Options](#)) otherwise the verification of the signatures must be manually start by clicking on button **Verify**.

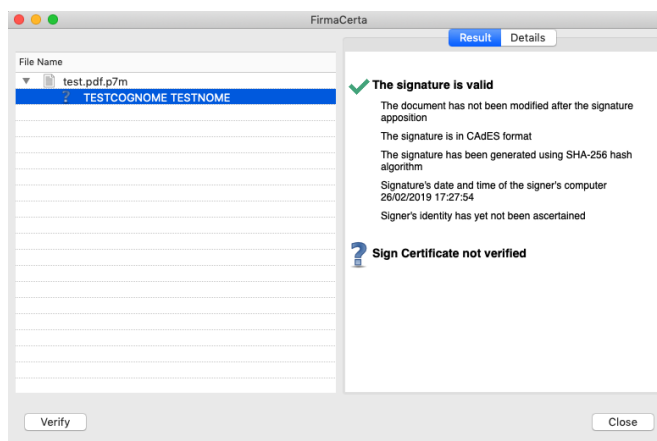


Figure 53 - Verification

Example: In this case the signed file is test.png.p7m and it has been signed by the user TESTCOGNOME TESTNOME.

In the left column it's possible to find the digitally signed file and the signer.

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;

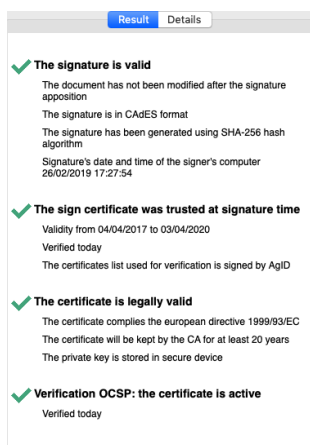


Figure 54 - Verify Result

Identifier	Value
TYPOLOGY	
Description	Sign Certificate
Validity	From 04/04/2017 to 03/04/20...
Algorithm	SHA-256
ISSUER	
Certification Authority Co...	IT
Organization	Namirial S.p.A./02046570426
Organization Unit	Certification Authority
Certification Authority	Namirial CA Firma Qualificata
HOLDER	
Signer Country	IT
Organization	NON PRESENTE
Surname	TESTCOGNOME
Name	TESTNOME
Signer Tax Code	IT-TSTTTN80A01A271U
Signer	TESTCOGNOME TESTNOME
Identification Code	LOTT2017032272641608
QC STATEMENTS	
Compliance	present
SSCD	present
Retention period	20

Figure 55 - Verify Details



6.5 APPENDIX E: CERTIFICATE RENEWAL

Before proceeding ensure to have been installed the signature software **FirmaCerta** properly updated.
If you are using a Proxy, please ask your network administrator the parameters configuration.

6.5.1 PROXY CONFIGURATION

Open Firmacerta software and click on the tools bar: Tools> Certificate Renewal, confirm the terms and click **Next**.

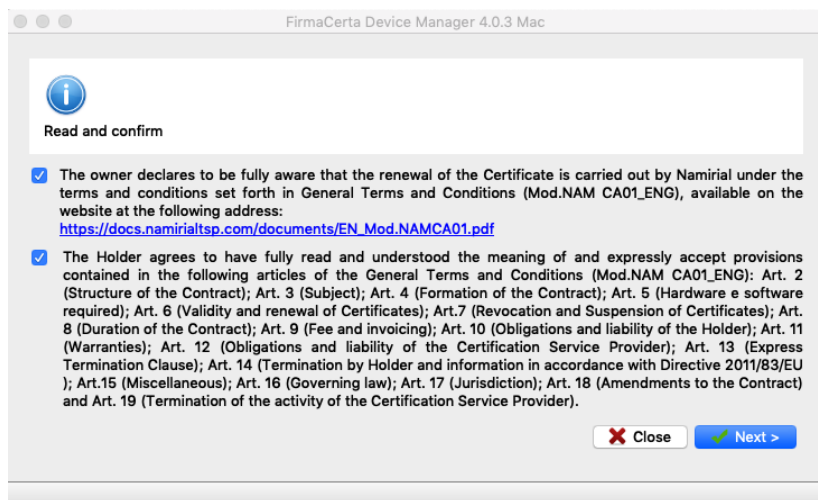


Figure 56 - Terms and Conditions

Select **Firmacerta DeviceManager > Preferences** and proceed with the proxy configuration (for the parameters contact your network administrator) Then click on **SAVE**.

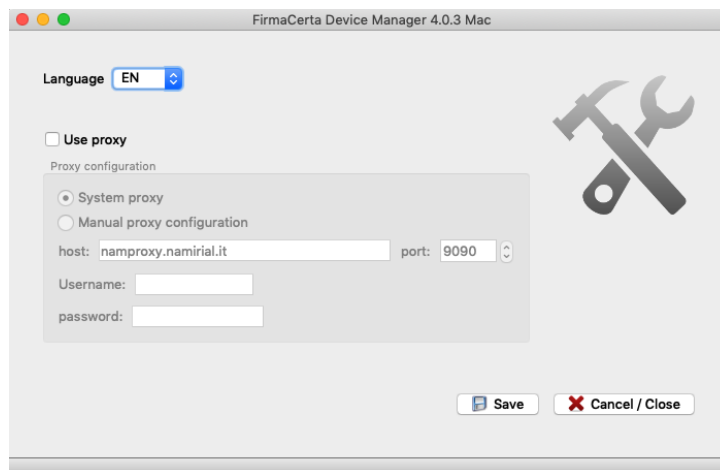


Figure 57 - Proxy Configuration



6.5.2 SMARTCARD AND TOKEN RENEWAL

Open FirmaCerta with the signature device connected to the computer, then click on *Tools > Certificates Renewal*. Read and confirm the restrictive terms and click **NEXT**

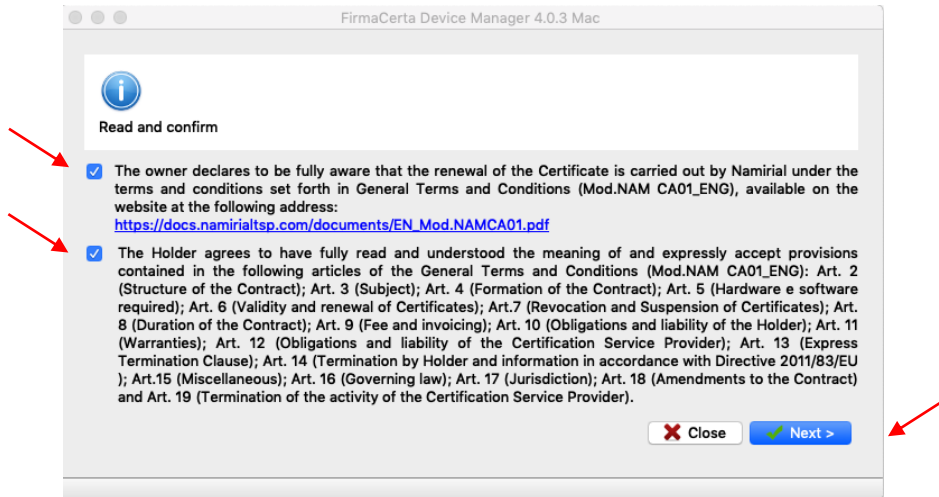


Figure 58 - Terms and Conditions

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

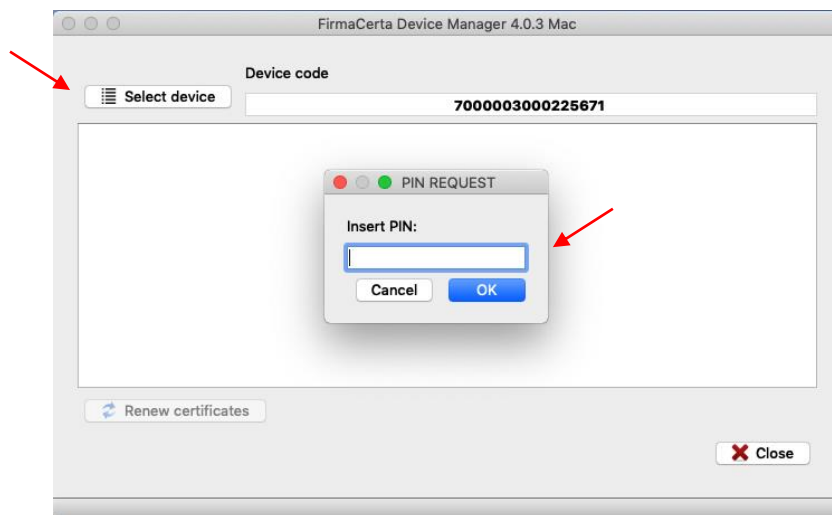


Figure 59 - Select Signature Device and insert PIN



The Tool Device Manager 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.

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

Press Yes if you want to view the contract, press No if you want't.

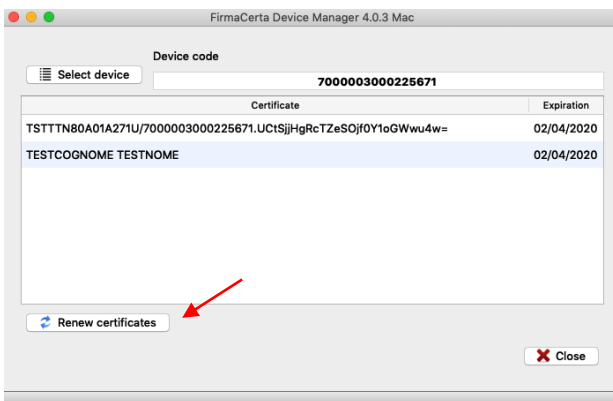


Figure 60 - Renew Certificates

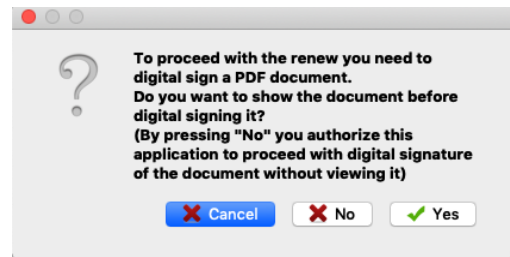


Figure 61 - request to view the contract before signing it

ATTENTION: If you have selected to view the PDF document the program will show you the certificate renewal contract. To complete the whole process the user must apply the signature by clicking on the file shown. Wait to complete the renewal process and end the operation pressing **OK**.

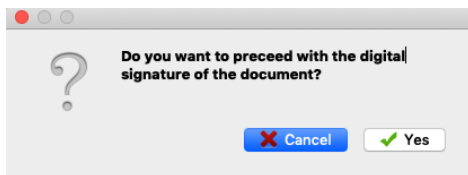


Figure 62 - Confirm signature process

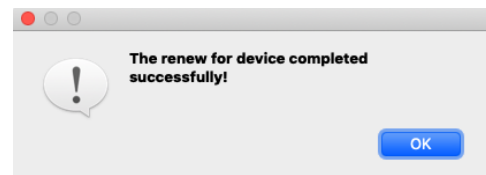


Figure 63 - Renew Signature Device Complete



6.6 APPENDIX F: REMOTE SIGNATURE GUIDE

6.6.1 HOW TO SIGN A FILE

After loading the file to be signed and clicking on the function **Sign** function the user will be asked to select a destination folder to save the signed document.

*In the following example, a specific folder for digitally signed files has been previously created, then select Signed Documents and click on **Open**.*

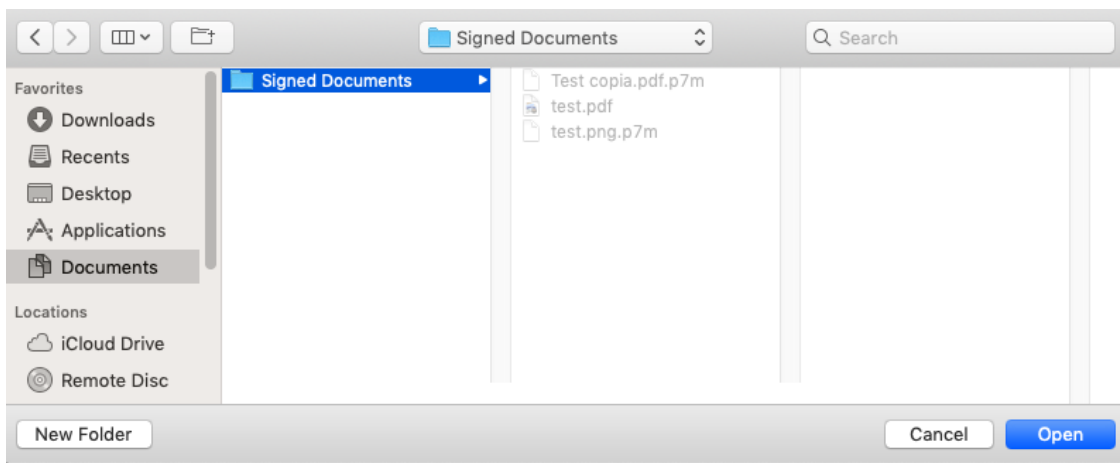


Figure 64 - Selection of the destination folder

6.6.1.1 SELECT SIGNATURE FORMAT

Select the CADES format to sign the file into .p7m format

Select the PAdES format to sign the file into .pdf format

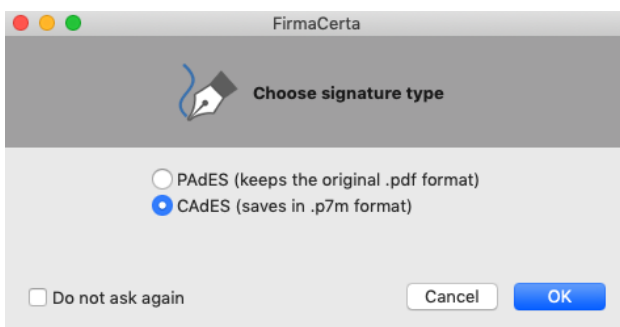


Figure 65 - Selection: CADES format

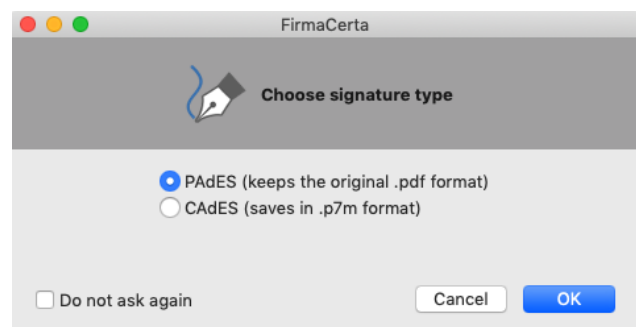


Figure 66 - Selection: PAdES format

Note: the choice of the signature format is available only for .pdf, for every other format the software will automatically applied the extension .p7m

Mark the preference **Do not ask anymore** it will be set automatically not to show the message anymore and it will be necessary to modify the settings from [Options](#)



6.6.1.2 SELECT SIGNATURE MOTIVATION (ONLY PDF FILE)

This function allows the user to add optional informations as *motivation, location, contact informations* before completing the signature of the document.

Note: This function is available only for .p7m documents. The use of this function is at the user's choice as an Optional Operation.

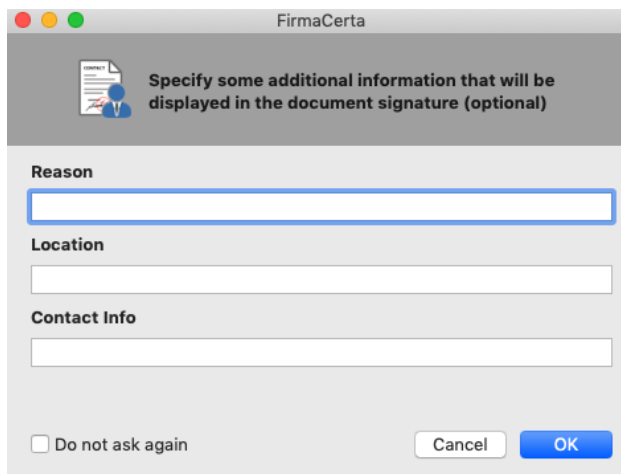


Figure 67 - Signature information

6.6.1.3 CONCLUSION OF THE SIGNATURE PROCESS

Confirmation of the signature application.

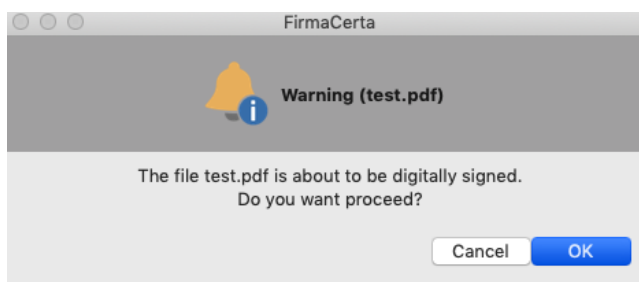


Figure 68 - Confirmation signature process

Select from the drop-down menu **Remote Signature**

Note: the choice between the devices will be available only if a usb reader or a token usb will be connected to the PC.

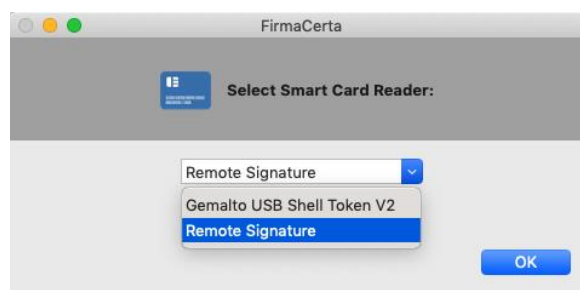


Figure 69 - Select signature device reader

To complete the signature process follow the instructions based on the type of OTP assigned during the registration:

- [Virtual OTP procedure](#)
- [SMS OTP procedure](#)
- [HARDWARE OTP procedure](#)



6.6.2 VIRTUAL OTP PROCEDURE: NAMIRIAL OTP

6.6.2.1 INTRODUCTION TO NAMIRIAL OTP MOBILEAPPLICATION

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.

This type of password is 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.

6.6.2.2 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.

6.6.2.3 NAMIRIAL OTP ACTIVATION

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.

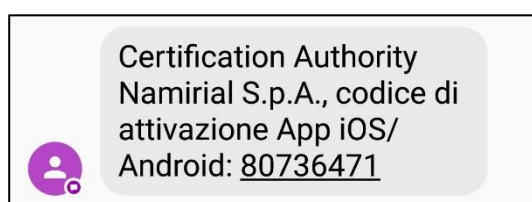


Figura 1 - SMS attivazione APP



6.6.2.4 ANDROID

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



Figure 70 - Namirial OTP interface



Figure 71 - add OTP

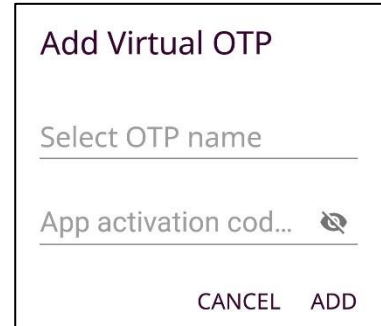


Figure 72 - Activation OTP

6.6.2.5 IOS

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



Figure 73 - Add OTP

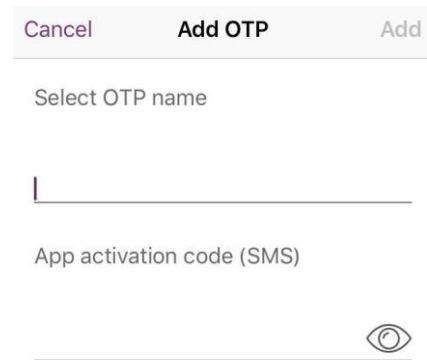



Figure 74 - Activation OTP



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.

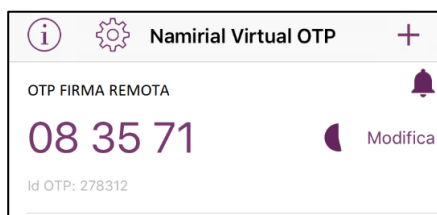


Figure 75 – Virtual OTP Generator

6.6.2.6 REMOTE SIGNATURE PARAMETERS CONFIGURATION

To recover the remote signature certificate data is necessary to enter the **Username** assigned during the service enrollment.

CREDENTIALS RECOVERY: In case of loss of the username, please access to the private area <https://portal.namirialtsp.com> and click on "I don't remember the username" and following the instructions. If the problem will persist the credentials may be requested sending an-mail to: helpdesk@firmacerta.it providing the signature holder's tax code.

Clicking on the key **Recover**, the fields **virtual devices** e **OTP type** will be automatically filled.

Figure 76 - remote signature parameters: username

Figure 77 - remote signature parameters: devices recovery



Enter the PIN in the PIN field received by digital blind envelope or paper blind envelope
Open the mobile app and enter the code shown on the display in the OTP field
Complete the process clicking on **OK**.

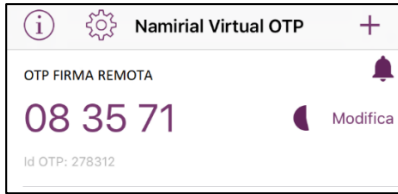


Figure 78 - Virtual OTP Generator

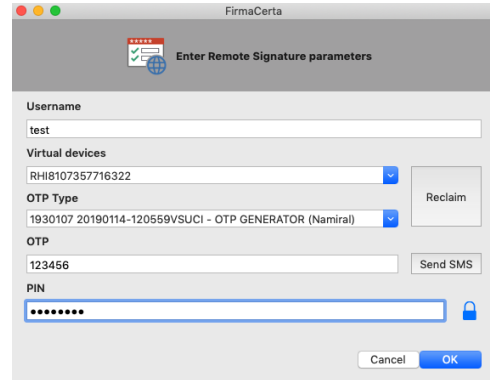
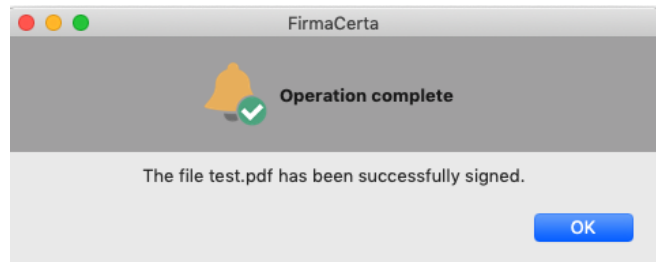


Figure 79 - remote signature parameters: pin

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



Figure 80 - Conclusion Signature Process





6.6.3 SMS OTP PROCEDURE

6.6.3.1 REMOTE SIGNATURE PARAMETERS CONFIGURATION

To recover the remote signature certificate data is necessary to enter the **Username** assigned during the service enrollment.

CREDENTIALS RECOVERY: In case of loss of the username, please access to the private area <https://portal.namirialtsp.com> and click on "I don't remember the username" and following the instructions.

If the problem will persist the credentials may be requested sending an-mail to: helpdesk@firmacerta.it providing the signature holder's tax code.

Clicking on the key **Reclaim**, the fields **virtual devices** e **OTP type** will be automatically filled.

The dialog box 'FirmaCerta - Enter Remote Signature parameters' has the following fields: Username (text input with 'test'), Virtual devices (dropdown menu), OTP Type (dropdown menu), OTP (text input), and PIN (text input with a lock icon). There are 'Reclaim', 'Send SMS', 'Cancel', and 'OK' buttons.

Figura 2 - Parametri Firma Remota: inserimento username

The dialog box 'FirmaCerta - Enter Remote Signature parameters' has the following fields: Username (text input with 'test'), Virtual devices (dropdown menu with 'RH18107357716322'), OTP Type (dropdown menu with '8381 20151126-1751115CGPI - SMS (Namirial)'), OTP (text input), and PIN (text input with a lock icon). There are 'Reclaim', 'Send SMS', 'Cancel', and 'OK' buttons.

Figura 3 Parametri Firma Remota: recupero dati

Enter the PIN in the PIN field received by digital blind envelope or paper blind envelope
Click on send SMS and enter the code received in the OTP field
Complete the process clicking on **OK**.

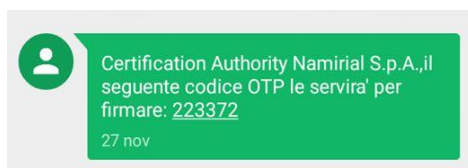


Figura 4 - SMS OTP

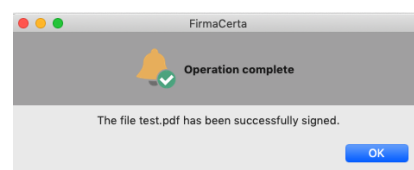
The dialog box 'FirmaCerta - Enter Remote Signature parameters' has the following fields: Username (text input with 'test'), Virtual devices (dropdown menu with 'RH18107357716322'), OTP Type (dropdown menu with '8381 20151126-1751115CGPI - SMS (Namirial)'), OTP (text input with '123456'), and PIN (text input with '*****' and a lock icon). There are 'Reclaim', 'Send SMS', 'Cancel', and 'OK' buttons.

Figura 5 - inserimento PIN firma remota

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



Figura 6 - operazione completata





6.6.4 HARDWARE OTP PROCEDURE

6.6.4.1 OTP ACTIVATION

Access to the [Private user Area](#), entering the credentials Username and Password received via email at the email address provided during the registration.

CREDENTIALS RECOVERY: In case of loss of the username/password, please access to the private area <https://portal.namirialtsp.com> and click 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-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 7 – hardware otp activation



Figure 8 – hardware otp insertion



6.6.4.2 REMOTE SIGNATURE PARAMETERS CONFIGURATION

To recover the remote signature certificate data is necessary to enter the **Username** assigned during the service enrollment.

CREDENTIALS RECOVERY: In case of loss of the username, please access to the private area <https://portal.namirialtsp.com> and click on "I don't remember the username" and following the instructions. If the problem will persist the credentials may be requested sending an-mail to: helpdesk@firmacerta.it providing the signature holder's tax code.

Clicking on the key **Recover**, the fields **virtual devices** e **OTP type** will be automatically filled.

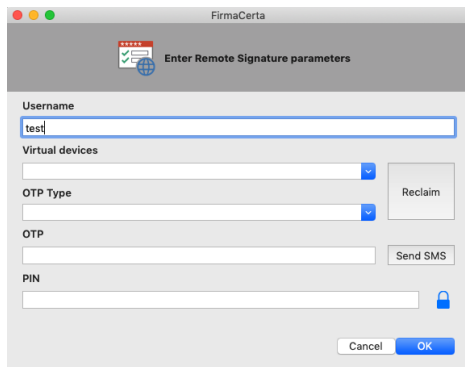


Figura 9 - Parametri Firma Remota: inserimento username

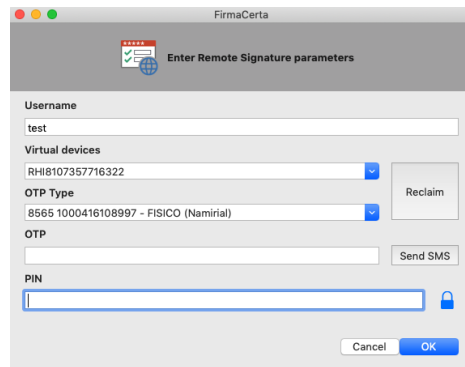


Figura 10 - Parametri Firma Remota: recupera dati

Enter the PIN in the PIN field received by digital blind envelope or paper blind envelope
Generate the otp code using the hardware device assigned and **enter it in the OTP field**
Complete the process clicking on **OK**.



Figure 11 - hardware otp

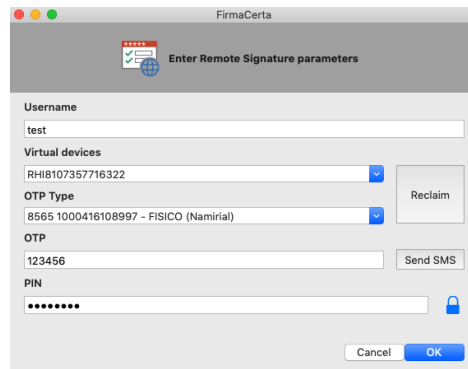
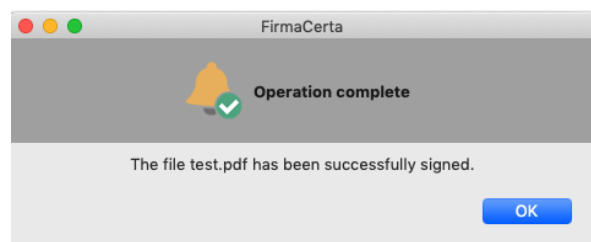


Figure 12 - PIN insertion

Attendere il tempo di elaborazione e premere **OK** per concludere il processo di firma.



Figura 13 - operazione completata





6.7 APPENDIX H: 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

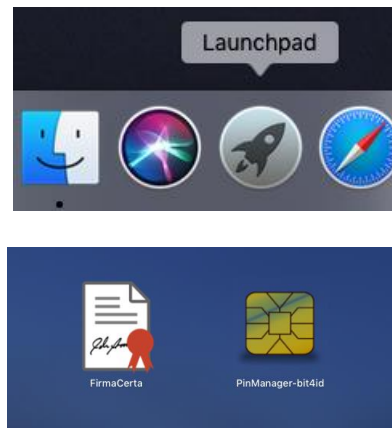
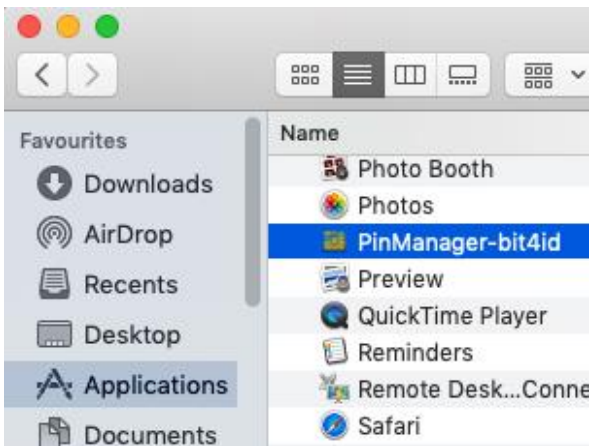


Figure 14 - PIN Manager: Opening

The Bi4id software allows the function Change PIN and Unlock Pin.

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

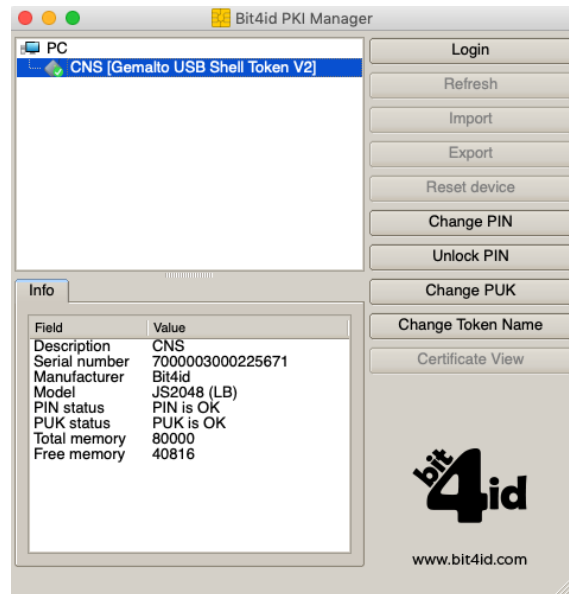
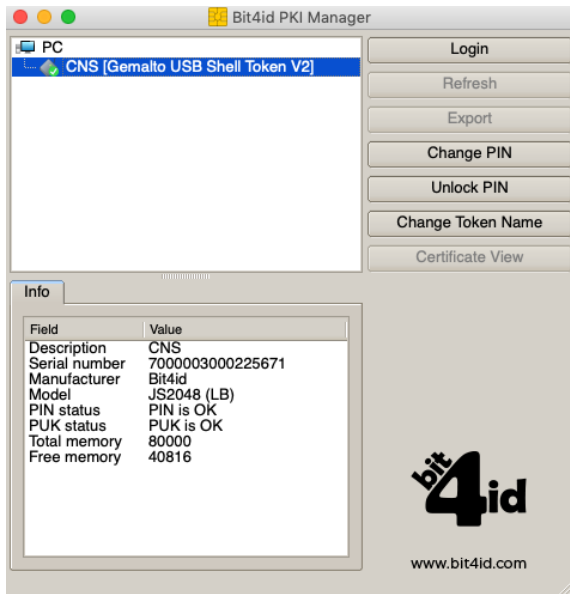


Figure 15 - Bit4id PKI Manager Advanced Functions



6.7.1 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 16 – pin change function

6.7.2 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

Figura 17 – Unlock PIN



6.7.3 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: 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.

Change PUK

Old PUK

PUK Status PUK is OK

New PUK

Min lenght: 4
Max lenght: 8

Repeat new PUK

OK Cancel

Figura 18 – Change PUK



REFERENCES

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



TABLES INDEX

Table 1 - Definitions and Acronyms	8
--	---

FIGURES INDEX

Figure 1 - Firmacerta Installation	9
Figure 2 - Warning: unidentified developer	9
Figure 3 - firmacerta installation solution 1a	10
Figure 4 - firmacerta installation solution 1b	10
Figure 5 - firmacerta installation 2nd solution	10
Figure 6 - Firmacerta Graphic Interface	11
Figure 7 - Firmacerta: Tools Bar	11
Figure 8 - Show Certificates in signature device	13
Figure 9 - Export Certificates	13
Figure 10 - insert PIN for check signature device	14
Figure 11 - Result Check Device	14
Figure 12 - Change PIN	14
Figure 13 - Unlock PIN	15
Figure 14 - Change PUK	15
Figure 15 - Options: General	16
Figure 16 - Options: File	17
Figure 17 - Options: Verification	17
Figure 18 - Options: Timestamps	18
Figure 19 - Options: Updates	18
Figure 20 - Selection of the destination folder	19
Figure 21 - Selection: CADES format	19



Figure 22 - Selection: PAdES format.....	19
Figure 23 - Signature information	20
Figure 24 - Confirmation signature process.....	20
Figure 25 - Selection: signature device reader.....	20
Figure 26 - Insert PIN	21
Figure 27 - Signature Process conclusion	21
Figure 28 - Selection of the destination folder	22
Figure 29 - Confirmation Process	22
Figure 30 - Select signature device reader	23
Figure 31 - Insert PIN	23
Figure 32 - Completion Signature Process.....	23
Figure 33 - Timestamps Configuration.....	24
Figure 34 - Check available Timestamps	24
Figure 35 - Selection of the destination folder	25
Figure 36 - Selection of Timestamps Format.....	25
Figure 37 - Select Timestamp format for .p7m file.....	26
Figure 38 - Select Timestamp format for .pdf file.....	26
Figure 39 - Enter Timestamp Parameters	26
Figure 40 - Confirmation signature process.....	27
Figure 41 - Select Signature device reader	27
Figure 42 - Insert PIN	27
Figure 43 - Signature Process Complete	27
Figure 44 - Selection of the destination folder	28
Figure 45 - CAdES format selection	28
Figure 46 - PAdES format selection	28



Figure 47 - Signature information	29
Figure 48 - Timestamps Parameters	29
Figure 49 – Confirmation Signature Process	30
Figure 50 - Select signature device reader	30
Figure 51 - Insert PIN	30
Figure 52 - Conclusion Signature Process.....	30
Figure 53 - Verification.....	31
Figure 54 - Verify Result.....	31
Figure 55 - Verify Details	31
Figure 56 - Terms and Conditions	32
Figure 57 - Proxy Configuration	32
Figure 58 - Terms and Conditions	33
Figure 59 - Select Signature Device and insert PIN.....	33
Figure 60 - Renew Certificates	34
Figure 61 - request to view the contract before signing it	34
Figure 62 - Confirm signature process	34
Figure 63 - Renew Signature Device Complete	34
Figure 64 - Selection of the destination folder	35
Figure 65 - Selection: CADES format.....	35
Figure 66 - Selection: PAdES format.....	35
Figure 67 - Signature information	36
Figure 68 - Confirmation signature process.....	36
Figure 69 - Select signature device reader	36
Figure 70 - Namirial OTP interface.....	38
Figure 71 - add OTP.....	38



Figure 72 - Activation OTP.....	38
Figure 73 - Add OTP.....	38
Figure 74 - Activation OTP.....	38
Figure 75 – Virtual OTP Generator.....	39
Figure 76 - remote signature parameters: username.....	39
Figure 77 - remote signature parameters: devices recovery.....	39
Figure 78 - Virtual OTP Generator.....	40
Figure 79 - remote signature parameters: pin.....	40
Figure 80 - Conclusion Signature Process.....	40