

## **Registration Authority**

Handbook FirmaCerta for Windows

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



Pag. 1 di 79

#### 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

UNI EN ISO 9001:2015 - Certificato N. 223776 | UNI EN ISO 27001:2013 - Certificato N. IT280490



– This page is intentionally left blank –



## **INDEX**

Inc	ndex								
Re	vision	History	7						
1	Intro	roduction							
	1.1	Document Purpose and field of application							
	1.2	Definitions and Acronyms used in this document							
2	Insta	allation	10						
3	Grap	bhic interface							
4	Maiı	n Functions							
4	4.1	Signature:							
	4.1.1	Signature	13						
	4.1.2	Countersign							
	1.1	Sign and time stamp							
	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	4.2	Graphometric Signature	17						
	4.2.1	Sign Document							
	4.2.2	Signatures Template							



	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	Арр	endix A: How to sign and countersign	
	5.1	How to sign a document	
	5.1.1	Sign in CAdES - XAdES	
	5.1.2	Sign in PAdES	
	5.2	How to Countersign	35
6	Арр	endix B: How to timestamp a file	
	6.1	Configuration of Timestamp Parameters	
	6.2	How to Sign and Timestamp	
	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	Арр	endix 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	Арр	endix 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 Ap	pendix F: Command Line	
9.1	Commands and Parameters	49
9.2	Examples:	49
10 A	ppendix G: Advanced Features	
10.1	Signature of more document	50
10.2	Multiple Document Timestamp	50
10.3	Sign and Timestamp more documents	51
11 A	ppendix H: Certificate Renewal	
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 A	ppendix I: Setting up Remote Signature	
12.1	Introduction to Namirial Otp app	57
12.1	.1 How to open it	57
12.1	.2 Namirial OTP configuration	
12.1	.3 Android	
12.1	.4 iOS	
12.2	Enabling Namirial SignEngine Service	59
12.3	How to sign a document	60
12.3	3.1 Username	61
12.3	8.2 Remote Device selection	
12.3	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	2.6.1 OTP activation	66				
13	web Authentication	68				
14	Appendice J: Bit4id – Linux	68				
14.1	Change PIN	69				
14.2	2 Unlock PIN	70				
14.3	Change PUK	70				
15	Appendice K: Bit4id – MacOS	71				
15.1	Change PIN	72				
15.2	2 Unlock PIN	72				
15.3	Change PUK	73				
Refere	ences					
Tables	ables Index74					
Figure	es Index	74				



## **REVISION HISTORY**

VERSION	<version></version>
Date	01/02/2019
Reasons	First document issue with new funcionality
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.

🛃 Firma Certa	– 🗆 🗙					
Selezione cartella di installazione	metan					
Firma Certa verrà installato nella cartella seguente.						
Per utilizzare questa cartella, scegliere Avanti. Per scegliere un'altra cart oppure scegliere Sfoglia.	ella, specificarne una					
<u>C</u> artella:						
C:\Program Files (x86)\FirmaCerta\	Sfoglia					
	Spazio richiesto su disco					
Installazione di Firma Certa per l'utente corrente o per tutti gli utenti:						
Tutti gli utenti						
O Utente corrente						
Annulla < Inc	lietro Avanti >					

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.

🕼 Firma Certa	– 🗆 X
Conferma installazione	(wretan
È possibile installare Firma Certa nel sistema in uso.	
Scegliere Avanti per iniziare l'installazione.	
Annulla	< Indietro Avanti >

Figure 3 - Installation confirmation

Wait until installation has been completed.

🕼 Firma Certa	– 🗆 X
Installazione completata	wetan
Firma Certa è stato installato.	
Scegliere Chiudi per uscire.	
Utilizzare Windows Update per verificare l'esistenza di aggior	namenti critici per .NET Framework.
Annulla	< Indietro Chiudi

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;

FIRMA CERTA								_¤×
SIGN	SIGN AND TIMESTAMP	VERIFY	TIMESTAMP	DEVICE MANAGER	GRAPHOMETRIC SIGNATURE	UTILITY	HELP	
The dyn	amic solution to and compar	o manage profe nies' privacy	Namirial ssionals'	GraphoSie	gn	Manage dig that requ for handw	True Service Provider itally documents irre a paper pass ritten signatures	Ver. 4.3.1.3
		Namir	ial GDPR			Digitally	as on paper	

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.

Change PIN				
Insert old and new PIN				
Old PIN				
	ମେ			
New PIN				
	୶			
Confirm PIN				
	OK Cancel			

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
63
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
<u>ද</u>
New PUK
<u>କ</u>
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.

Result Details	Result Details	
✓ The signature certificate is trusted	Туре	
Valid from 20/07/2017 09:29:00 to 19/07/2020 00:00:00	Description	Signature certificate
Check date 14/01/2019 09:25:25 The <u>certificates list</u> used to verify is signed by AgID	Validity	from 20/07/2017 09:29:00 to 19/07
✓ The certificate is valid and legal	Issuer	
The certificate complies with the regulation UE n. 910/2014	Country Certification authority	п
The certificate is mantained from CA for at least 20 years	Organization	Namirial S.p.A./02046570426
The private key is stored in a secure device	Organization unit	Certification Authority
✓ OCSP verify : certificate enabled	Certification authority	Namirial CA Firma Qualificata
Check date 14/01/2019 09:25:25		

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).

PIN	Firma Certa	
O Incert smart card PIN	1 The device is v	vorking properly.
	Description	. Maria
	Description	value
	TYPE	Bit4Id
	ID	7000003000165083
	ATR	3BFF1800008131FE55006B02090403010101434E5310318065
OK Cancel	DLL	bit4xpki.dll (dnmDefault)
		ОК

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 <u>Appendix H</u>).

#### 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).

1 1 1		
_	-	
_		

Click with the left mouse button (or right) to save the Once the field has been selected, the following window first field of the template



pag. 2 of 3; size 210x297 mm Area (X:456, Y:350, Width:267, Height:161) Figure 19 - Marker in the template will appear.

Template X
Signature field settings:
Signature field name
Holder's signature
Use empty signature field created in document: (set name only if different from field name)
×
Create background OK Cancel



#### 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.



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 tamplate 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



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)

Chiave di ricero	a			
Maiuscole/n	ninuscole 📄	Parola intera	Numero mass	simo di campi firma
		0		0
Coordinata X	Coordinata Y	Larghezza ca	mpo firma. Alte	ezza campo firma
390	677		266	160

#### 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 tempalte for other

Figure 22 - Search keywords



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.

# FIRMA CERTA > UTILITY CRYPT DECRYPT GENERAL OPTIONS PROXY AND CONNECTIONS SIGNATURE OPTIONS VERIFY OPTIONS GRAPHOMETRIC TIMESTAMP OPTIONS (CRYPT DECRYPT GENERAL OPTIONS PROXY AND CONNECTIONS SIGNATURE OPTIONS VERIFY OPTIONS GRAPHOMETRIC SIGN OPTIONS TIMESTAMP OPTIONS (CRYPT DECRYPT GENERAL OPTIONS PROXY AND CONNECTIONS SIGNATURE OPTIONS VERIFY OPTIONS GRAPHOMETRIC SIGN OPTIONS (CRAPHOMETRIC SIGN OPTIONS) (CRAPHOMETR

## 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 <u>Appendix D</u>).

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.

🚔 Options	×
General File manager Logo pdf Verify Connection URL Timestamp	• • •

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

<ul> <li>Sign pdf files in original format (PAdES)</li> <li>Not require the additional signature information</li> <li>Not show signature logo in pdf document</li> <li>Open pdf after sign</li> </ul>
<ul> <li>Sign xml files in original format (XAdES)</li> <li>Save signed files in source folder</li> <li>Overwrite file if exists in target folder</li> <li>Not require confirmation before sign</li> <li>Not notify successful operations</li> </ul>



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.
<ul> <li>Do not request additional signature informations:</li> </ul>	Optional informations will not be displayed in the signed document;
<ul> <li>Do not show the signature logo in PDF documents:</li> </ul>	Setting this preference before signing and then viewing the digitally signed PDF file, the signature logo with signer's information will not be reported.
	<b>NB:</b> You can customise the logo through the corresponding setting <b>Logo pdf</b> , 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.

<u>Attiva dispositivo di firma</u>
Visualizza certificati contenuti nel dispositivo di firma
Verifica dispositivo di firma
Cambio PIN
Sblocca dispositivo di firma
<u>Visualizza logo pdf</u>

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.
- o 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).

Download upgrade

http://download.firmacerta.it/ca-docs/easyupgrade/

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.

Options			×	
Verify Connecti	on URL Timesta	mp Graphometric sign	nature Web service	
Service		Description	Url	
Namirial Sign	Namirial SignEngine		https://fra.namirialtsp.com/	
<			>	
Enabled/Disab	led Delete	e Change	: Url Upgrade	
Not share this o softwares	ptions with other "firm	na certa"	OK Cancel	

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.

JRL Timestamp	Graphometric signature Web service Information	• •
	Namirial Trust Service Provider	
Ver. 4.3.1.3		
Namirial S.p.A.		
eIDAS Qualified	Trust Service Provider	
www.firmacerta	<u>.it</u>	
System informat	tion:	
Windows 10 Pro	(64 bit)	
00330-50000-00	0000-AAOEM	
F09A-7D09		
wv10 stand-alor	ne, current-user	
	Add Namirial to trusted identities	
	Reset last reader cache	
	Reset last reader cache Reset "do not show again" messages	
Language	Reset last reader cache Reset "do not show again" messages	
Language	Reset last reader cache Reset "do not show again" messages	
Language English	Reset last reader cache Reset "do not show again" messages	Cancel

#### 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.

Proxy server Authentication mode	Port	
None None		~
Username	Password	
		63
Use Internet Explorer configuration	n	Options
Connection timeout     0   milliseconds		
Figure 30 - Options: Config	ure 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.



General File manager Logo pdf Verify Connection UR	L (Timestamp
-Default logo	
Width Height	
93 93	
Hide background	
Logo for pdf signature	
Set tranparency	
From Argento To Bianco	~
Show text on signature logo Not prompt text customization Embed text font (PDF/A compatibility)	Smartcard settings
Show logo pdf	

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.

FIRMA CERTA >	UTILITY > GRAPH	OMETRIC SIGN	OPTIONS	_DX
	OPTIONS	ACTIVATION	DISCLOSURE	
0				Ver. 4.3.1.3

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 <u>www.firmagrafometrica.it</u> section "Dispositivi Utilizzabili").

	Detect digitize	er		
External digitizer			Id	
Wacom STU-530		~		0
Embedded digitizer or connected a	s secondary mor	nitor		
Model:				
🧶 Generic		~ 🕞		
Show document in secondary moni	tor	5	Wonitor 2 [S22F350]	~
Execute sequentially all signatu	ires in the docum	ient		
Show secondary monitor on the	e main screen			
Show document in primary monitor	before sign			
Show document in primary monitor	after sign			
Activate document controller on ex	kternal digitizer			
Activate mouse control during sign	ature			
Unlock mouse on primary monitor d	during signature			
Sign with color ink:			🗾 Blue	$\sim$
Graphometric signature "light" (with	hout biometric da	ata)		
Not add timestamp in signature				
Not print graphometric signature signature	tamp			
Acquire signature in terminal serve	r mode		Advanced	
Capture photo and add in signatur	e		Advanced	
Install certificates for "medium" signati	ure			

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:

	Options	
Select the Request License option and press <b>Next</b> ;	<ul> <li>Request license</li> <li>Activate license</li> <li>View license</li> <li>Retrieve license</li> <li>Move license</li> </ul>	
	Device selection	
Press <b>Next</b> ;	Select device that you want to ac	tivate to graphometric signature and press "Next $>$ "
	📓 Graphometric signature - License [ver.	1.2.9.5] — 🗆 🗙
	License request	
	License subject Billing information	
	Surname and name	Tax code
Fill the fields with the license holder's	TEST COGNOME TEST NOME	TSTTTN89H08I608Q
data and press <b>Send</b> .	Company	
	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 singer 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.

Firma Certa - Documents	
Subject information	
Tax code	
Surname and name	
City of birth	
Date of birth	
~	
	OK Cancel

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.

Options	
eneral File manager Logo pdf Verify Connection URL Timestamp	
Default TSA URL	
https://timestamp.namirialtsp.com	
Username	
Password	
	69
Not prompt timestamp credentials	
Check available timestamps	
Not share this options with other "firma certa" OK	Cance
tns://timestamp.namirialtsp.com	

http://timestamp.namirialtsp.com

LINK to the use timestamping service

Figure 38 - Options Time Stamp

#### **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**.

FIRMA CERTA > SIGN		_DX
SIGN	COUNTERSIGN	Ver. 43.13

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

Firma Certa
Attention (test.xml)
Do you want to make a xml signature (XAdES)? Press "Yes" to make a XAdES signature (.xml) Press "No" to make a CAdES signature (.p7m)
Yes No
Figure 41 - Selection of Cades-XAdES signature format



Select the destination folder of the signed file, then Proceed with the signature operation pressing Yes. click OK.

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

Cerca cartella	×
test.pdf Select targer folder:	
🗸 📃 Questo PC	^
> 📃 Desktop	
> 🔮 Documenti	
> 🕂 Download	
> 📰 Immagini	
> 🎝 Musica	
> 🧊 Oggetti 3D	
> 📑 Video	
> 🏪 Acer (C:)	
> 👝 Data (D:)	
> 🔐 Unità DVD RW (E:)	
> 🐂 Raccolte	~
Crea <u>n</u> uova cartella OK	Annulla
gure 42 - Select the destination	n folder

Atten	tion (test.pdf)	1				
	The file tes	t.pdf modifie is being di Do you war	d on 07/1 igital sign nt to prec	1/2018 10:3 ed. eed?	3:24	
				Yes		No
Figure 43 -	Sianature	Confirmat	ion			

click OK.

PIN Insert smart card PIN	Firma Certa
OK Cancel	Operation completed successfully.
Figure 44 - Enter the PIN code	Figure 45 - Operation completed

Enter the PIN of the digital signature device and Wait the processing time and press OK to complete the operation.

ОК

## 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



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.

erca cartella	×
est.pdf Select targer folder:	
🗸 💻 Questo PC	^
> 📃 Desktop	
> 🔮 Documenti	
> 🕂 Download	
> 📰 Immagini	
> 🎝 Musica	
> 🧊 Oggetti 3D	
> 📕 Video	
> 🏪 Acer (C:)	
> 👝 Data (D:)	
> 🔐 Unità DVD RW (E:)	
> 🐂 Raccolte	~
Crea <u>n</u> uova cartella OK Anr	nulla





Figure 48: Signature Confirmation

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

Select the signature reason (optional).



PIN	Signature information (test.pdf)
Insert smart card PIN	Insert some additional signature information (optional)
OK Cancel	Reason
	Contact info
	Do not show again OK Cancel

Figure 49: Enter the PIN Code

Figure 50: Signature information

Select the position of the logo using the green To confirm the operation press "Yes". marker





Wait the processing time and press OK to complete the

To customise the logo (optional), press OK.

	operation.
Logo customization (test.pdf)	Firma Certa
1 Insert logo text customization values (optional)	1 Information (test.pdf)
✓ Show date and time ✓ Auto generate text	Operation completed successfully.
Header	ОК
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 束	
Save values in smartcard	
Do not show again OK Cancel	
Figure 53: Customized Logo	Figure 54: Operation completed

## 5.2 HOW TO COUNTERSIGN



#### Figure 47 - Panel of Countersign

With this function it'is 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

click OK.

Select the Destination Folder of the signed file, then



Confirm if you want to overwrite the existing file and

Cerca cartella × Firma Certa test.pdf Select targer folder: Attention (test.pdf) 7 💻 Questo PC ٨ Target file C:\Users\m.bonvini\Desktop\test.pdf already exists. 📃 Desktop Overwrite? 🔮 Documenti > 뒞 Download 📰 Immagini Yes No 👌 Musica 🧊 Oggetti 3D 📑 Video > 🏪 Acer (C:) 🕳 Data (D:) Unità DVD RW (E:) 🐂 Raccolte Crea <u>n</u>uova cartella OK Annulla Figure 48 - Select the destination folder Figure 49 - Confirmation of overwriting

click Yes.

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

TEST COGNOME TEST NOME	Identifier	Value		
IEST COGNOME TEST NOME	Validità	dal 20/07/2017 al 18/07/2020		
	Algoritmo	SHA-256		
	Country Signer	Π		
	Last name	TEST COGNOME		
	First name	TEST NOME		
	<ul> <li>Tax code Signer</li> </ul>	IT:TSTTTN89H08I608Q		
	Signer	TEST COGNOME TEST NOME		
	Qualifier	LOTT2017072058507911		
	Country Certification authority	Π		
	Organization	Namirial S.p.A./02046570426		
	Organization unit	Certification Authority		
	Certification authority	Namirial CA Firma Qualificata		
	Marche temporali	0		
	•			
		01		

Figure 50 - Example screen: verification of the countersigned file


Proceed with the signature operation pressing Yes.

Firma Certa
Attention (test.pdf)
The file test.pdf modified on 07/11/2018 10:33:24 is being digital signed. Do you want to preceed?
Yes No

Figure 51 - Signature Confirmation

### Enter the PIN of the Digital Signature device and Wait the processing time and press OK to complete the click OK.

# operation.

PIN	Firma Certa
Insert smart card PIN	1 Information (test.pdf)
	Operation completed successfully.
OK Cancel	ОК

Figure 52 - Enter the Pin Code

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 digitally signature. The timestamps can be purchased in our Shop. To configure the timestamp open FirmaCerta Software> Utility> Timestamp Options

FIRMA CERTA > U	JTILITY							
	CRYPT DECRYPT	GENERAL OPTIONS	PROXY AND CONNECTIONS	SIGNATURE OPTIONS	VERIFY OPTIONS	GRAPHOMETRIC SIGN OPTIONS	TIMESTAMP OPTIONS	
0							Ĩ.	Ver. 43.13

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.

Dptions	×
General File manager Logo pdf Verify Connection URL	Timestamp 🔹 🕨 💌
Default TSA URL	
https://timestamp.namirialtsp.com	
Username	
ab 1234567	
Password	
******	69
Not prompt timestamp credentials	
Check available timestamps	
Not share this options with other "firma certa" softwares	OK Cancel
Figure 55 - Timestamp Configuration	on Options

### **ATTENTION**:

- Clicking on the icon 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@sicurezzapostale.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)



Timestamp information	
Description	Value
Name	io
Purchased	10000000
Used	12176984
Remaining	87823016
Last use	14/01/2019 10:08:14
Last purchase	01/06/2012 18:14:05
	ОК

# 6.2 HOW TO SIGN AND TIMESTAMP

After selecting a file you can choose this function to sign and timestamp in one singlular 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 <u>NOT severable</u>.

To Sing and Timestamp proceed as in the following steps:

• Select Sign and Timestamp inside the software,

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

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

Cerca cartella	×
test.pdf Select targer folder:	
V 💻 Questo PC	^
> Desktop	
> 🔮 Documenti	
> 🕂 Download	
> 📰 Immagini	
> 🁌 Musica	
> 🧊 Oggetti 3D	
> 📑 Video	
> 🏪 Acer (C:)	
> 🔜 Data (D:)	
> 🔐 Unità DVD RW (E:)	
> 🐂 Raccolte	~
Crea nuova cartella OK Annul	la:

Figure 57 - Select the destination folder

Attention (test.pdf)      The file test.pdf modified on 07/11/2018 10:33:24         is being digital signed.         Do you want to preceed?      Yes No	Attention (test.pdf)	
The file test.pdf modified on 07/11/2018 10:33:24 is being digital signed. Do you want to preceed? Yes No		
Yes No	The file test.pdf modified on 07/11/2018 10:33:2 is being digital signed. Do you want to preceed?	4
	Yes	No

Figure 58 - Signature Confirmation

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



PIN	
	Insert smart card PIN
	OK Cancel
	Figure 59 - PIN Entry

OK.

Confirm the application of the timestamp, then click Wait the processing time and press OK to complete the operation.

Timestamping (test.pdf.p7m)	Firma Certa
Insert service credentials:	1 Information (test.pdf)
TSA URL	Operation completed successfully.
https://timestamp.namirialtsp.com	
Username	ОК
ab 1234567	
Password	
*******	
Check remaining timestamps	
Do not show again	
Figure 60 - Confirmation of the entered timestamp	Figure 61 - Operation completed

credentials

#### 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)



Follow the procedure described in point <u>Appendix A: How to sign a document</u>.

### 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.

Timestamping (test.pdf.p7m)		
Select timestamp format:		
Format		
CADES-T format (timestamp associated with the signature) $\qquad \qquad \lor$		
CADES-T format (timestamp associated with the signature) TSD format (timestamp associated with the document) TSR format (timestamp inserted in a separate file) TST format (timestamp inserted in a separate file)		

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 clickWait the processing time and press OK to complete the<br/>operation.



Timestamping (test.pdf.p7m)	Firma Certa
Insert service credentials:	1 Information (test.pdf)
TSA URL	Operation completed successfully.
https://timestamp.namirialtsp.com	
Username	OK
ab 1234567	UK
Password	
*******	
Check remaining timestamps	
Do not show again	
Figure 67 - Confirms configuration timestamp	Figure 68 - Operation completed

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



lettera.p7m.tsd File con marca temporale 🚺 1,32 MB

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 seperate the timestamp

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

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

😹 Verify	Timestamping
Split timestamp and document	Select timestamp format:
Namirial TSA 2 (2019-1)	Format
> - 🙀 test.pdf.pdf.p7m > - 🙀 test.pdf.pdf	TST format (timestamp inserted in a separate file) $$
	TSR format (timestamp inserted in a separate file)
	rst format (unlestantp inserted in a separate file)
	OK Cancel

Figure 71 - Timestamp Separation



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.



marchetemporali.pdf.p7m File P7M 695 KB



marchetemporali.pdf.tsr Marca temporale 4,03 KB

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.

FIRMA CERTA								
SIGN	SIGN AND TIMESTAMP	VERIFY	TIMESTAMP	DEVICE MANAGER	GRAPHOMETRIC SIGNATURE	UTILITY	HELP	
								Ver. 43.1.3

Figure 74 - FirmaCerta Panel Verify

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

Verify	>	~
<ul> <li>Itest.pdf.p7m</li> <li>Itest.pdf</li> <li>Itest.pdf</li> </ul>	Result       Details         ✓       File test.pdf.p7m         C:\Users\m.bonvini\Desktop\test.pdf.p7m         All certificates are trusted         ✓       TEST COGNOME TEST NOME         The signature certificate is trusted (details)         ✓       TEST COGNOME TEST NOME         The signature certificate is trusted (details)         ✓       TEST COGNOME TEST NOME         The signature certificate is trusted (details)	
Verify 14/01/2019 V 10:39:28 💌 Check date	Close	

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 automaticcally 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;



esult Details	Result Details	
/ The desidence is set	Туре	
V The signature is valid	Description	Signature certificate
This document has not been changed after signature	Validity	from 20/07/2017 09:29:00 to 19/0.
The signature format is CAdES and respects the resolution CNIPA 45/2009	Algorithm	SHA-256
The signature hash algorithm is SHA-256	Issuer	
Signing time from computer clock : 14/01/2019 10:15:38	Country Certification authority	Π
	Organization	Namirial S.p.A./02046570426
The signature certificate is trusted	Organization unit	Certification Authority
Valid from 20/07/2017 09:29:00 to 19/07/2020 00:00:00	Certification authority	Namirial CA Firma Qualificata
Check date 14/01/2019 10:39:28	Subject	
The <u>certificates list</u> used to verify is signed by AgID	Country Signer	Π
/ The contificate is walld and logal	Last name	TEST COGNOME
	First name	TEST NOME
The certificate complies with the regulation UE n. 910/2014	Tax code Signer	IT:TSTTTN89H08I608Q
The certificate is mantained from CA for at least 20 years	Signer	TEST COGNOME TEST NOME
The private key is stored in a secure device	Qualifier	LOTT2017072058507911
OCSP verify : certificate enabled	QC Statements	
Check deta 14/01/2010 10:20:20	Compliance	found
CHECK UBLE 17/01/2019 10:39:20	SSCD	found
	Retention period	20
1		

# 7.1 HOW TO AUTOMATICALLY SET THE LAUNCH OF VERIFICATION OF SIGNATURES

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

📓 Options	×
General File manager Logo pdf Verify Connection URL (Timestamp	< ▶ ▼
Verify at startup  Fnabled cache for CRL verification	
Activate cache for TSL verify (expiry: 7 days)	
☑ Verify certificates when signed document is open	
Not share this options with other "firma certa" OK	Cancel

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:



### **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.



Proteggi documenti





Comparing C	Result       Details         ✓ The authentication certificate is trusted         Valid from 20/07/2017 09:29:00 to 19/07/2020 00:000         Check date 14/01/2019 11:26:25         The certificates ist used to verify is signed by AgID         ✓ OCSP verify : certificate enabled         Check date 14/01/2019 11:26:25
Verify 14/01/2019 V 11:26:25 🗘 Check date	

۱ 🛃	test1.pdf - /	Adobe A	crobat R	ead	-			×
<u>F</u> ile	<u>M</u> odifica	<u>V</u> ista	Fin <u>e</u> stra	2				
Ho	ome	Strum	enti	?	÷.	Α	cce	edi
	ୁ କ		$\bowtie$	Q	1	/ 1		27,8
Ľ						^		<b>[</b> ]
	TEST							1
								₽
								Þ
•							•	Ð
								č0
								4
								~
k						~		l⇒

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:

Xtten:	tione	
	Accesso al documento non cons	entito
		ОК

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>
- UrITSA = <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:

🗟 Options 🛛 🗙	Deptions >
General File manager Logo pdf Verify Connection URL Timestamp  Sign pdf files in original format (PAGES) Not require the additional signature information Not show signature logo in off dog ment	General File manager Logo pdf Verify Connection URL Timestamp  Default TSA URL https://timestamp.namirialtsp.com Username lah1233657
Open pdf after sign Gign xml files in original format (XAdES) Sign xml files in source folder	Password
Overwrite file if exists in target folder Not require confirmation before sign Not notify successful operations	Check available timestamps           Not share this options with other "firma certa"         OK         Cancel
igure 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.

Timestamping (test.pdf)
Select timestamp format:
Format
TSD format (timestamp associated with the document) $\qquad \qquad \lor$
OK Cancel

# 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:

Options	X Doptions X
General File manager Logo pdf Verify Connection URL Timestamp	General File manager Logo pdf Verify Connection URL Timestamp
	Default TSA URL
Sign pdf files in original format (PAdES)	https://timestamp.namirialtsp.com
Not require the additional signature information	Username
Not show signature logo in pdf document	ab1234567
Open pdf after sign	Password
	*******
Sign xmi tiles in original format (XAdES) ✓ Save signed files in source folder	Not prompt timestamp credentials
Overwrite file if exists in target folder	Check available timestamps
✓ Not require confirmation before sign	
Not notify successful operations	Not share this options with other "firma certa" OK Cancel

Figure 87 - Configuration for sign and timestamp multiple documents

Figure 88 - Configuration Timestamp Option

The software will	request to	enter the P	IN code once.

PIN	
Insert smart card PIN	
	OK Cancel

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.

🚳 FirmaCerta Device Manager 4.0.3 Win	_		×
Read and confirm			
The owner declares to be fully aware that the renewal of the Certificate is carried out by Namirial under the forth in General Terms and Conditions (Mod.NAM CA01_ENG), available on the website at the following address https://docs.namirialtsp.com/documents/EN_Mod.NAMCA01.pdf	terms and	conditions	; set
The Holder agrees to have fully read and understood the meaning of and expressly accept provisions contain of the General Terms and Conditions (Mod.NAM CA01_ENG): Art. 2 (Structure of the Contract); Art. 3 (Subject Contract); Art. 5 (Hardware e software required); Art. 6 (Validity and renewal of Certificates); Art. 7 (Revo Certificates); Art. 8 (Duration of the Contract); Art. 9 (Fee and invoicing); Art. 10 (Obligations and liabilit (Warranties); Art. 12 (Obligations and liability of the Certification Service Provider); Art. 13 (Express Ten (Termination by Holder and information in accordance with Directive 2011/83/EU); Art. 15 (Miscellaneous); Art 17 (Jurisdiction); Art. 18 (Amendments to the Contract) and Art. 19 (Termination of the activity of the Certifica	ed in the fo ; Art. 4 (Fo cation and y of the Ho mination Cl . 16 (Gover tion Service	ollowing art ormation of Suspensio older); Art ause); Art ning law); Provider).	ticles f the n of . 11 . 14 Art.
×	Close		.:
Figure 90 - Restrictive clauses			

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

🛞 FirmaCerta Device Manager 4.0.3 Win	-		×
<u>Actions</u> <u>I</u> ools <u>H</u> elp			
Language EN V	$\boldsymbol{\mathcal{K}}$	9	)
Use proxy			
Proxy configuration			
System proxy			
O Manual proxy configuration			
host: namproxy.namirial.it port: 9090 🜩			
Username:			
password:			
	Save X C	ancel / Clos	e:
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**.

🐼 FirmaCerta Device Manager 4.0.3 Win	_		×
Read and confirm			
The owner declares to be fully aware that the renewal of the Certificate is carried out by Namirial under the terms a	nd conditio	ns set for	th in
General Terms and Conditions (Mod.NAM CA01_ENG), available on the website at the following address: https://docs.namirialtsp.com/documents/EN_Mod.NAMCA01.pdf			
Image: The Holder agrees to have fully read and understood the meaning of and expressly accept provisions contained in the General Terms and Conditions (Mod.NAM CA01_ENG): Art. 2 (Structure of the Contract); Art. 3 (Subject); Art. 4 (Formatic (Hardware e software required): Art. 6 (Validity and repewal of Certificates): Art. 7 (Revocation and Suspension of Certificates): Art. 8 (Subject): Art. 8 (Subject): Art. 7 (Revocation and Suspension of Certificates): Art. 7 (Revocation and Suspension of Certificates): Art. 7 (Revocation and Suspension of Certificates): Art. 8 (Subject): Art. 8 (Subject): Art. 9 (Sub	e following n of the Co ates): Art.	articles of ontract); A 8 (Duratio	f the Art. 5 on of
the Contract); Art. 9 (Fee and invoicing); Art. 10 (Obligations and liability of the Holder); Art. 11 (Warranties); Art. 12 ( the Certification Service Provider); Art. 13 (Express Termination Clause); Art. 14 (Termination by Holder and inform	Obligations ation in ac	and liabili	ty of with
Directive 2011/33/EU ); Art.15 (Miscellaneous); Art. 16 (Governing law); Art. 17 (Jurisdiction); Art. 18 (Amendments to (Termination of the activity of the Certification Service Provider).	the Contrac	t) and Ar	t. 19
×	Close	🗸 Next	t >
Fiaure 92 - Restrictive clauses			

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

Select device	ode	7000030	00165083	
	PI     Insert     [	N REQUEST ? PIN: OK Ca	X ncel	
🥏 Renew certificates				





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 it or not.

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

) FirmaCerta Device Manager 4.0.2 V	lín	-		>
tions <u>T</u> ools <u>H</u> elp				
Device code				
im spect device	7000003000165083		Evolutio	
TSTTTN89H08l608Q/700000300016	5083.9BRf3wqvEDQCtrup8xnN5leE1Rc=		18/07/20	20
TEST COGNOME TEST NOME			18/07/20	20
	1			
2 Renew certificates				
			X Close	





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: <u>https://portal.namirialtsp.com</u> Click on LOGIN and insert username and password previously received via email at the time the digital signature certificate has been issued.

Namirial 2D	Certificate management 📕 Italiano 💥 English 📗 Românesc
Atti	va SPID con Namirial <b>2D</b>
	REGISTERED LOG in
	I don't remember the user name I don't remember the password

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 <u>helpdesk@firmacerta.it</u> specyfing 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.

©Namirial <sup>®</sup> D	•					ቆ
Cmstest Portalitest		Home The home page user				
💄 User	~	Data	associated with	The servic	e of digital signature	Functionality or services to activate
倄 Home		Name	Value	Name	Value	Renew certificates
Se Profile		Email box	TEST@FIRMACERTA.IT	Number certificates	1	
Frome	·	Phone number	(+39) 3331234567			
OTP		Home digital (PEC)	FIRMACERTA@SICUREZZAPOST			
📝 Digital signature	^	User name	C.PORTALTEST			
Signature						
Valid signature						
	-11		1. 6		ist updates	
Management		06/12/2018 Portal acce	ss also for certificate holders			
			Figure 99 -	Private User De	ashboard	



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

Selecting the certificate and click on the **RENEW** button the panel will open: <u>Procedure to renew the subscription certificate</u> <u>autonomously</u>, 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 Columns							
Device code	Expiration date	State	Renewable				
220100009002609	27/02/2019	Active	Renewed				
220100009002609	27/02/2019	Active	Renewed				
220100009002609	28/03/2019	Active	By request				
220100009002609	28/03/2019	Active	By request				
RHI2760138582183	30/03/2019	Active	To renew				
Active Pause Revocation & Change PIN CRenewed							

Figure 100 - Certificate Management

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

Procedure renewal in the autonomy of	of the certificate of subscription		
Below, you will be issued the new cert affix a digital signature to the remote	tificate in place of the one expiring. The missir using the certificate to be renewed. The new o	ng days to expire will be added to the new that will vertificate will retain the code device and PIN.	be usable immediately. In order to proceed you must
	led		
PIN			
SMS - 326484	Download contract signed	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 104 - Making tap the green button (Add OTP)

Add Virtual OTP	
Select OTP name	3
App activation cod	Ø
CANCEL	ADD

Figure 105 - Enter code and label allocation

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

# 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:



Cancel	Add OTP	Add
Select OT	Pname	
<u> </u>		
App activ	ation code (SMS)	
		0

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**.

B Options	×	Options		×
General File manager Logo pdf Verify Connection	on URL Timestamp	URL Timestamp Graphomet	tric signature Web service In	formation • •
	✓ General			
Sign pdf files in original format (PAdES)	File manager	Service	Description	Url
Not require the additional signature information	Logo pdf	Namirial SignEngine	Remote signature	https://fra.namirialtsp.com/
Not show signature logo in pdf document	Verify			
Open pdf after sign	Connection			
Sign xml files in original format (XAdES)	URL			
Save signed files in source folder	Timestamp			
Overwrite file if exists in target folder	Graphometric signature			
Not require confirmation before sign	Web service			
Not notify successful operations	Information			
			Delate Chancel H	5
Not share this options with other "firma certa"		Not share this options with oth	er "firma certa"	
softwares	OK Cancel	softwares		OK Cancel

Figure 109 - Enabling SignEngine Service



# **12.3 HOW TO SIGN A DOCUMENT**

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

FIRMA CERTA >	FIRMA		_DX
	FIRMA	CONTROFIRMA	
ଚ			2

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

format (only for PDF files)

Press No for a CAdES signature with .p7m forma	Press <b>No</b> for a CAdES signature with .p7m format
Firma Certa	Firma Certa
Attention (test.xml)	Attention (test.pdf)
Do you want to make a xml signature (XAdES)? Press "Yes" to make a XAdES signature (.xml) Press "No" to make a CAdES signature (.p7m)	Do you want to make a pdf signature (PAdES)? Press "Yes" to make a PAdES signature (.pdf) Press "No" to make a CAdES signature (.p7m)
Yes No	Yes No
Do not show	Do not show
Figure 111	- Choosing signature format



Select the destination folder for the signed file and, finally, click **OK**.

Proceed with the signature operation by pressing Yes.

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



Firma Certa

Content of the file test.pdf modified on 07/11/2018 10:33:24
is being digital signed.
Do you want to preceed?

Yes No

Figure 113 - Signature Confirmation

Figure 112 - Selecting the destination folder

### 12.3.1 USERNAME

Click on Settings to enter the username:

Remote service	Remote service
Insert credentials of remote service:	Insert user for access to the private area
Virtual device	
	ab 1234567
Settings OK Cancel	OK Cancel

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: <u>https://portal.namirialtsp.com</u>

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: <u>helpdesk@firmacerta.it</u>



# 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

Remote service		
🤍 Insert credentia	als of remote service:	
Virtual device		
		<b></b>
Settings	OK	Cancel

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

📓 Virtual device selection		×
Virtual devices		
RHI7736422357495 (valid from 22	2/10/2018 to 20/10/2021)	
	ОКС	ancel

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)				
1 Insert s	Insert some additional signature information (optional)			
Reason				
1				
Location				
Contact info				
Do not show	again	ОК	Cancel	

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 <u>Regards</u>, <u>Namirial</u> S.p.A. Email: <u>helpdesk@firmacerta.it</u> Web: <u>www.firmacerta.it</u>

#### 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.

emote service  Insert credentials of remote service:  irtual device  XH17736422357495 in  ITP Type 8381		I NIS S
Insert credentials of remote service:	ote service	📓 ОТ
irtual device RH17736422357495 in TP Type 8381  Settings OK Cancel	Insert credentials of remote service:	OTP de
RH17736422357495	al device	
in Type 8381 C	7736422357495	8381:
TTP Type 8381		8565:
Settings OK Cancel		
Settings OK Cancel	Type	
Settings OK Cancel		
Settings OK Cancel		
	Settings OK Car	ncel

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

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

OTP device selection		)
OTP devices		
l		
8381: SMS, Namirial, 20151126-	-1751115CGPI	
8565: FISICO, Namirial, 100041	6108997	
	OK	Cancel
	UK	Concer

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	redentials of remote service:
Virtual device RHI7736422357	7495
Pin *******	
OTP	Type 8381
Settings	OK Cancel
	Figure 121 - Sending SMS OTP

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

Firma Certa	
1 Information (test.pdf)	
Operation completed successfully.	
	OK
Figure 123 - Confirmation n	nessage

Remote service

Virtual device RHI7736422357495

> Send SMS Settings

Pin

OTP

Insert credentials of remote service:



# **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 is shows the type of OTP (in this case GENERATOR)

OTP device selection	
OTP devices	
1930107: OTP GENERATOR, Na 1930110: OTP PUSH, Namirial,	amiral, 20190114-120559VSUCI 20190114-120559AFDH5
	OK Cancel

Figure 124 - Select OTP device

6

Type 8381 🔂

Cancel

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

ОК

Remote service	ां २००२ Namirial Virtual OTP	+
Insert credentials of remote service:	OTP FIRMA REMOTA	, the second sec
RHI7736422357495	08 35 71	Modifica
Pin *******	Id OTP: 278312	
OTP Type [19301]		
Settings OK Cancel		

Figure 125 - OTP Generator

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





# **12.6 OTP HARDWARE PROCEDURE**

### **12.6.1 OTP ACTIVATION**

Log on to <u>User Private Area</u>, using the credentials Username and Password receiveid 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-mail to: <u>helpdesk@firmacerta.it</u> providing the signature holder's tax code.



Enter the device PIN received by digital blind envelope.

Click on the icon in the red box to select the OTP device, then click  $\ensuremath{\mathsf{OK}}$ 



	This screen shows the type of OTP (in this case HARDWARE-FISICO)
Remote service	DTP device selection X
Insert credentials of remote service:	OTP devices
Virtual device RHI7736422357495 Pin I OTP Type 8381 8381 Settings OK Cancel	1930107: OTP GENERATOR, Namiral, 20190114-120559VSUCI         1930110: OTP PUSH, Namirial, 20190114-120559AFDH5         8381: SMS, Namirial, 20151126-1751115CGPI         8565: FISICO, Namirial, 1000416108997         OK
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 RH17736422357495	
********           OTP         Type           19301         C	
Settings OK Cancel	



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

Firma Certa
Information (test.pdf)
Operation completed successfully.
ОК
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: <a href="http://download.firmacerta.it/pdf/manualeAutenticazioneWeb.pdf">http://download.firmacerta.it/pdf/manualeAutenticazioneWeb.pdf</a>

# **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 <u>Private User Area</u> in the section > User > Digital Signature > Management.

	Change PIN	8
Old PIN		
PIN Status	PIN is OK	
New PIN		
	Min lenght: 4 Max lenght: 8	
Repeat new PIN		
	ОК	Cancel
	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. <u>After 3 incorrect attempts of the PUK Code</u> the device will be permanently locked and it will be necessary to request a new signature device.

	Unlock PIN	8
PUK	[	
PUK Status	PUK is OK	
New PIN		
	Min lenght: 4	
	Max lenght: 8	
Repeat new PIN		
	ОК	Cancel
	Figure 135 - Unlock PIN	1

# 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.

Change PUK 😣		
Old PUK		]
PUK Status	PUK is OK	-
New PUK		]
	Min lenght: 4 Max lenght: 8	
Repeat new PUK		]
	ОК	Cancel

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** 







# **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 <u>Private User Area</u> in the section > User > Digital Signature > Management.

• •	🔁 Change PIN	
Old PIN	1	
PIN Status	PIN is OK	
New PIN		
	Min lenght: 4	
	Max lenght: 8	
Repeat new PIN		
	ОК	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. <u>After 3 incorrect attempts of the PUK Code</u> 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		]
	ОК	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	1	
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]	<>
[11]	<>



## **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	
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	
Figure 40 - Signature Panel	31
Figure 41 - Selection of Cades-XAdES signature format	31
Figure 42 - Select the destination folder	
Figure 43 - Signature Confirmation	
Figure 44 - Enter the PIN code	
Figure 45 - Operation completed	
Figure 46 - Selection of Cades-Pades signature format	



Figure 47 - Panel of Countersign	35
Figure 48 - Select the destination folder	
Figure 49 - Confirmation of overwriting	
Figure 50 - Example screen: verification of the countersigned file	
Figure 51 - Signature Confirmation	
Figure 52 - Enter the Pin Code	
Figure 53 - Operation completed	
Figure 54 - Utility Panel	
Figure 55 - Timestamp Configuration Options	
Figure 56 - Checking Timestamps	
Figure 57 - Select the destination folder	
Figure 58 - Signature Confirmation	
Figure 59 - PIN Entry	40
5	
Figure 60 - Confirmation of the entered timestamp credentials	40
Figure 60 - Confirmation of the entered timestamp credentials	40
Figure 60 - Confirmation of the entered timestamp credentials Figure 61 - Operation completed Figure 62 - Signature dashboard	40 40 40
Figure 60 - Confirmation of the entered timestamp credentials Figure 61 - Operation completed Figure 62 - Signature dashboard Figure 63 - Selecting the Cades signature format	40 40 40 40
Figure 60 - Confirmation of the entered timestamp credentials Figure 61 - Operation completed Figure 62 - Signature dashboard Figure 63 - Selecting the Cades signature format Figure 64 - FirmaCerta Panel Timestamp	40 40 40 41 41
Figure 60 - Confirmation of the entered timestamp credentials Figure 61 - Operation completed Figure 62 - Signature dashboard Figure 63 - Selecting the Cades signature format Figure 64 - FirmaCerta Panel Timestamp Figure 65 - Selecting time stamp format	40 40 40 40 41 42 42
Figure 60 - Confirmation of the entered timestamp credentials Figure 61 - Operation completed Figure 62 - Signature dashboard Figure 63 - Selecting the Cades signature format Figure 64 - FirmaCerta Panel Timestamp Figure 65 - Selecting time stamp format Figure 66 - Selection of destination folder	40 40 40 41 42 42 42 42
Figure 60 - Confirmation of the entered timestamp credentials   Figure 61 - Operation completed   Figure 62 - Signature dashboard   Figure 63 - Selecting the Cades signature format   Figure 64 - FirmaCerta Panel Timestamp   Figure 65 - Selecting time stamp format   Figure 66 - Selection of destination folder   Figure 67 - Confirms configuration timestamp	
Figure 60 - Confirmation of the entered timestamp credentials   Figure 61 - Operation completed   Figure 62 - Signature dashboard   Figure 63 - Selecting the Cades signature format   Figure 64 - FirmaCerta Panel Timestamp   Figure 65 - Selecting time stamp format   Figure 66 - Selection of destination folder   Figure 67 - Confirms configuration timestamp   Figure 68 - Operation completed	
Figure 60 - Confirmation of the entered timestamp credentials.   Figure 61 - Operation completed   Figure 62 - Signature dashboard   Figure 63 - Selecting the Cades signature format   Figure 64 - FirmaCerta Panel Timestamp   Figure 65 - Selecting time stamp format   Figure 66 - Selection of destination folder   Figure 67 - Confirms configuration timestamp   Figure 68 - Operation completed   Figure 69 - Example: file marked temporally	
Figure 60 - Confirmation of the entered timestamp credentials   Figure 61 - Operation completed	



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	
Figure 91 - Proxy Configuration	
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	
Figure 101 - Signature and renew Process	
Figure 102 - Example SMS with activation code	57
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	
Figure 106 - Start screen of Virtual OTP. Please tap on Add OTP	
Figure 107 - Enter code and label allocation	
Figure 108 - Screenshot OTP code generated from APP	
Figure 109 - Enabling SignEngine Service	
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	
Figure 123 - Confirmation message	
Figure 124 - Select OTP device	
Figure 125 - OTP Generator	
Figure 126 - Confirmation message	
Figure 127 – Activation Otp	
Figure 128 - Private user Area	
Figure 129 - Select OTP device	67
Figure 130 - OTP Body Raised	67
Figure 131 - Confirmation message	67
Figure 132 - DashBoard Linux	
Figure 133 - Bit4id PKI Manager Advanced Functions	
Figure 134 - Change PIN	
Figure 135 - Unlock PIN	
Figure 136 - Change PUK	
Figure 137 - PIN Manager Opening	
Figure 138 - Bit4id PKI Manager Advanced Functions	
Figure 139 - Change PIN	
Figure 140 - Unlock PIN	
Figure 141 - Change PUK	