



Document Digital Signature

Supplier handbook - Software Configuration for Digital Signature and
Timestamp to certificate-based signature

Marzo 2016

2One
Global Procurement

enel

Document objectives and structure



- The document aims to support suppliers during the following phases:
 - › configuration of the program used to digitally signed a document;
 - › add a Digital Signature on a document;
 - › add a Timestamp^(*) to certificate-based signature on a document.

- For each of the above steps, the document shows the **operational steps** and the related system screenshots for some of the most used software to Digital Sign documents and to add a Timestamp^(*) to certificate-based signature.

For detailed documentation please look at the user manual of the used software

- Please remind that Enel requires to both digital sign and add a timestamp on a document **in the same moment** with the following allowed format **.pdf** or **p7m**.

(*) Please remind that the timestamp service is subject to fees defined by the used provider

Acrobat 8 (or later) program utilization



Acrobat 8 program utilization



Initial settings (1/6)

- The first step to use Acrobat 8 for the digital signature is the connection between the signature device (i.e. token USB) and the personal computer.
- Next step is to install the specific software (driver) that will enable the personal computer to dialog with the signature device
- At this stage you can proceed with the configuration of the signature handler (digital ID accounts) and parameters of Timestamp^(*) and, at the end, adding the Digital Signature and the Timestamp^(*) on the document (slide 5-14)

For detailed documentation please look at the following link:

- › <https://helpx.adobe.com/it/acrobat/using/certificate-based-signatures.html>

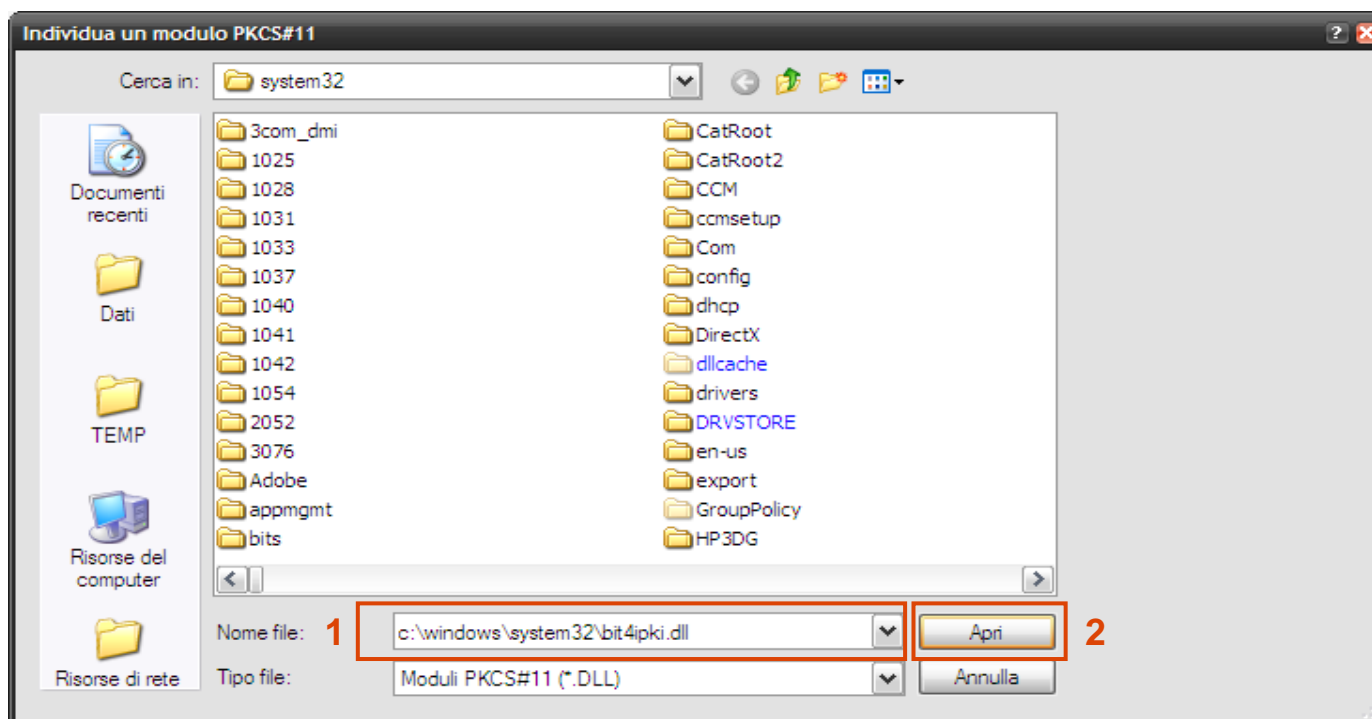
() Please remind that the timestamp service is subject to fees defined by the used provider*

Acrobat 8 program utilization

Initial settings (2/6)



From menu click on **Advanced** > **Security settings** and, after selecting “Modules and tokens PKCS#11”, click on **Add module**. Look for the path where libraries are shown (if the Operating System is a 32bit, libraries are in the directory C:\Windows\System32). Select the library **bit4ipki.dll** (1) and click on **Open** (2).

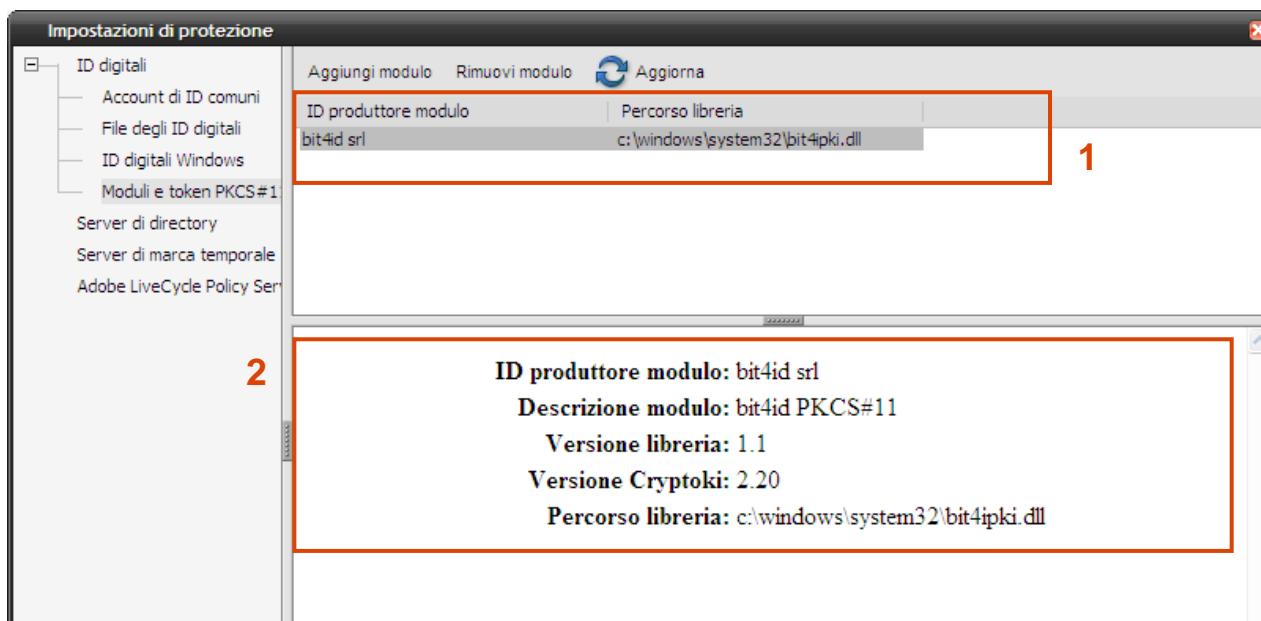


Acrobat 8 program utilization

Initial settings (3/6)



The next window shows the available security settings. The box (1) shows the module previously added (library bit4ipki.dll). The box (2) enables to view the module general information.

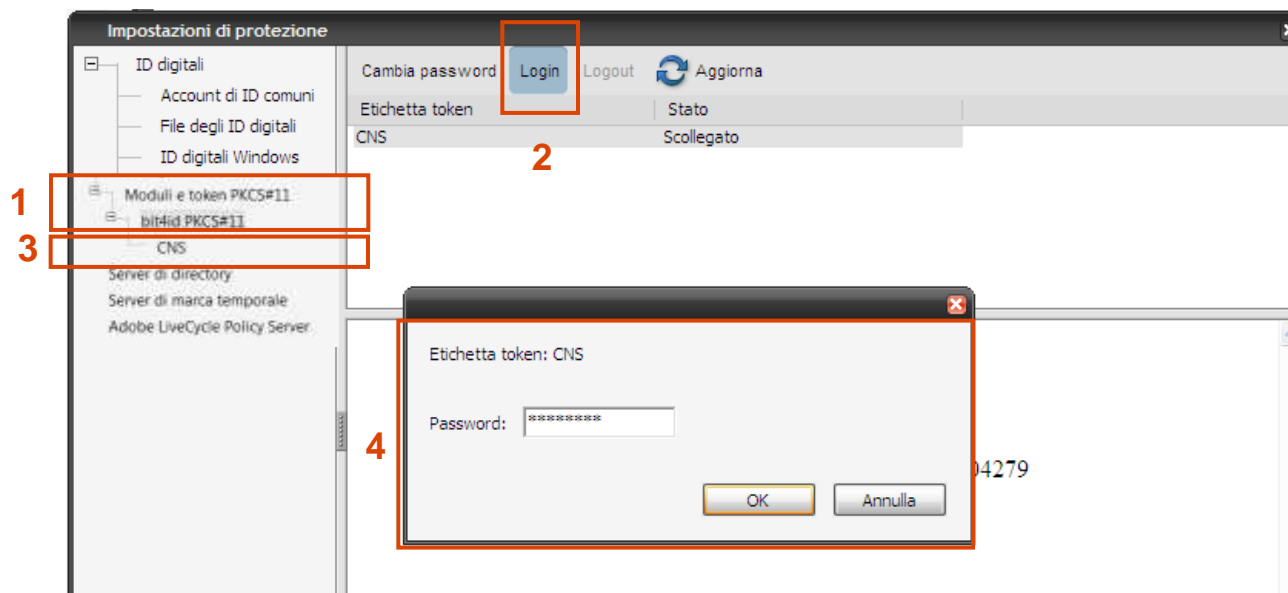


Acrobat 8 program utilization

Initial settings (4/6)



In order to insert token credentials, go through the modules tree on the left side window and click on “bit4id PKCS#11” (1), then click on “**Login**” (2) in the menu on the right side. Go through the modules tree again till finding the **CNS** (3) and once selected insert the token pin and click on **OK** (4).

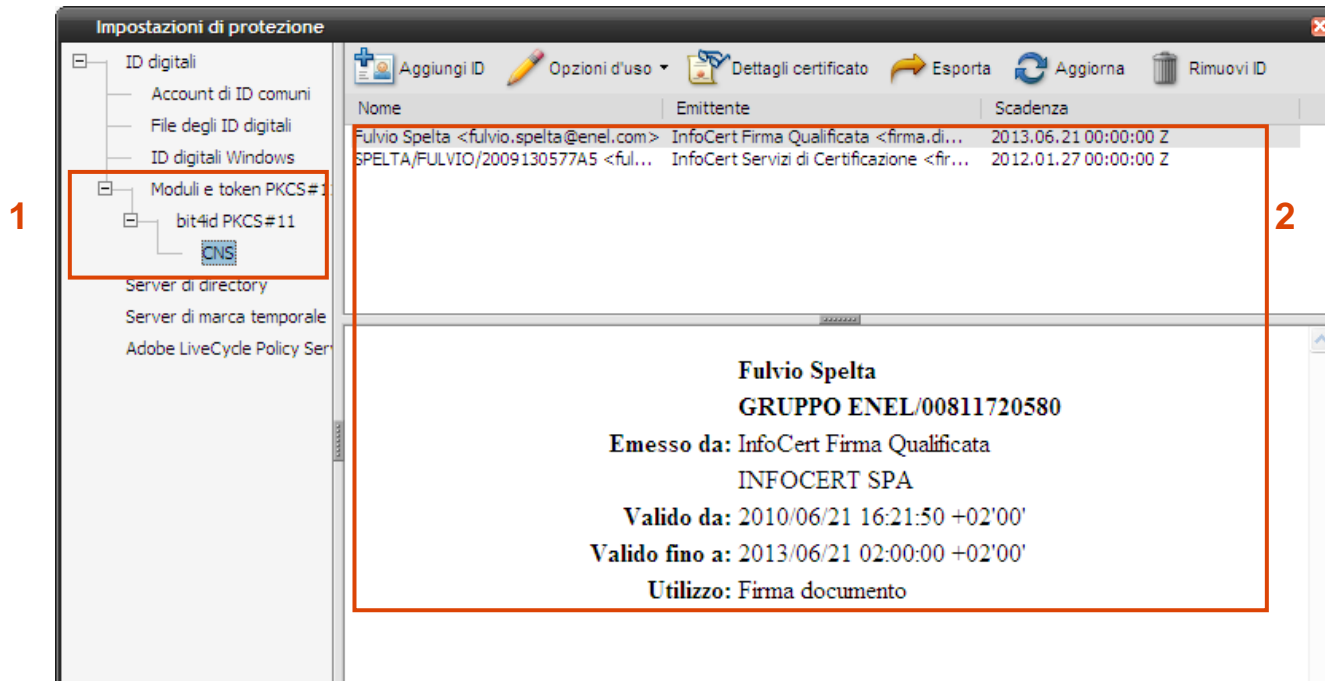


Acrobat 8 program utilization

Initial settings (5/6)



Re-open the modules tree and select again the CNS (1).
Verify the token id (certified) acquisition (2).



Acrobat 8 program utilization

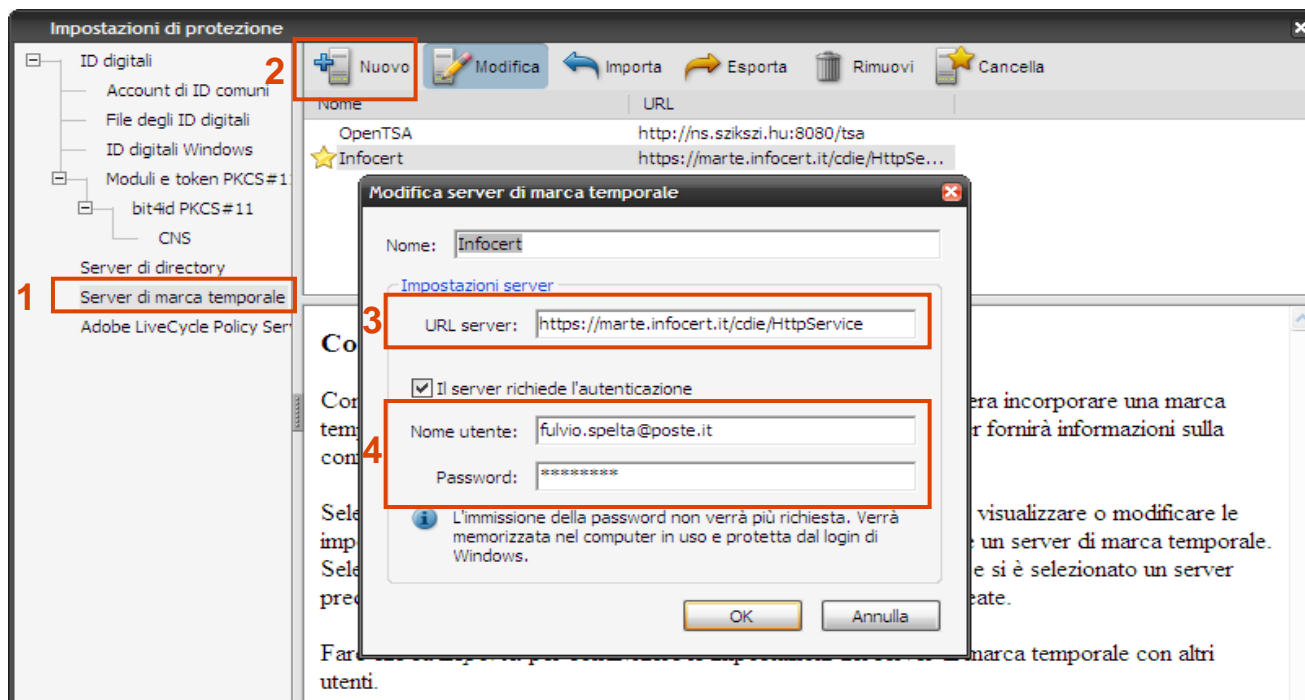
Initial settings (6/6)



In the same window select **Timestamp^(*) server** (1), click on **New** (2) in the left side menu and configure parameters^(**): **URL Server:** *https://marte.infocert.it/cdie/HttpService* (3) **Username and password:** username and password through which the user purchased the timestamps (4). Click on OK to set the Time Stamp Server as default.

() Please remind that the timestamp service is subject to fees defined by the used provider*

*(**) Parameters refer to timestamp purchased from Infocert provider. In case of different type of timestamp the users has to ask for the right parameters to his provider*

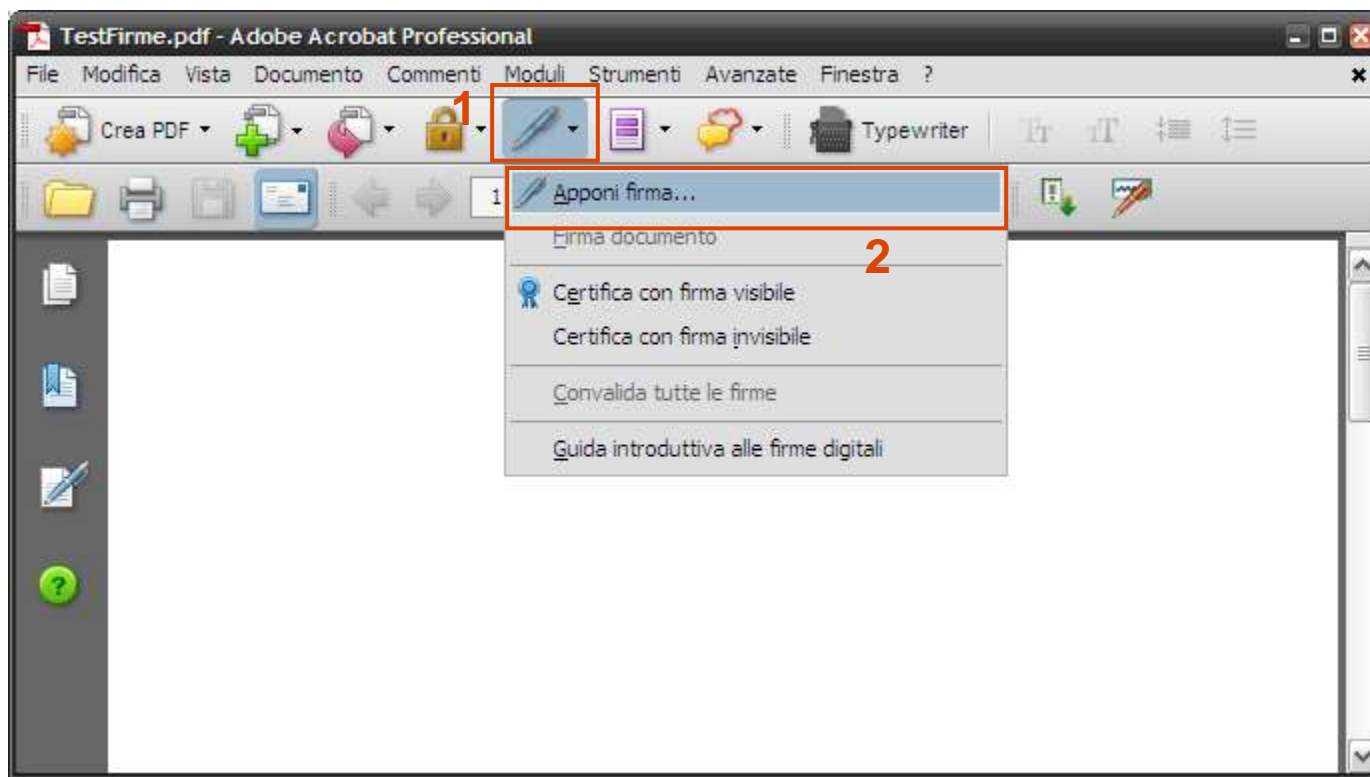


Acrobat 8 program utilization

Digital signature and timestamp (1/5)



From the toolbar, click on button **Sign** (1) and then on **Place Signature** (2) to open the digital signature management screenshots



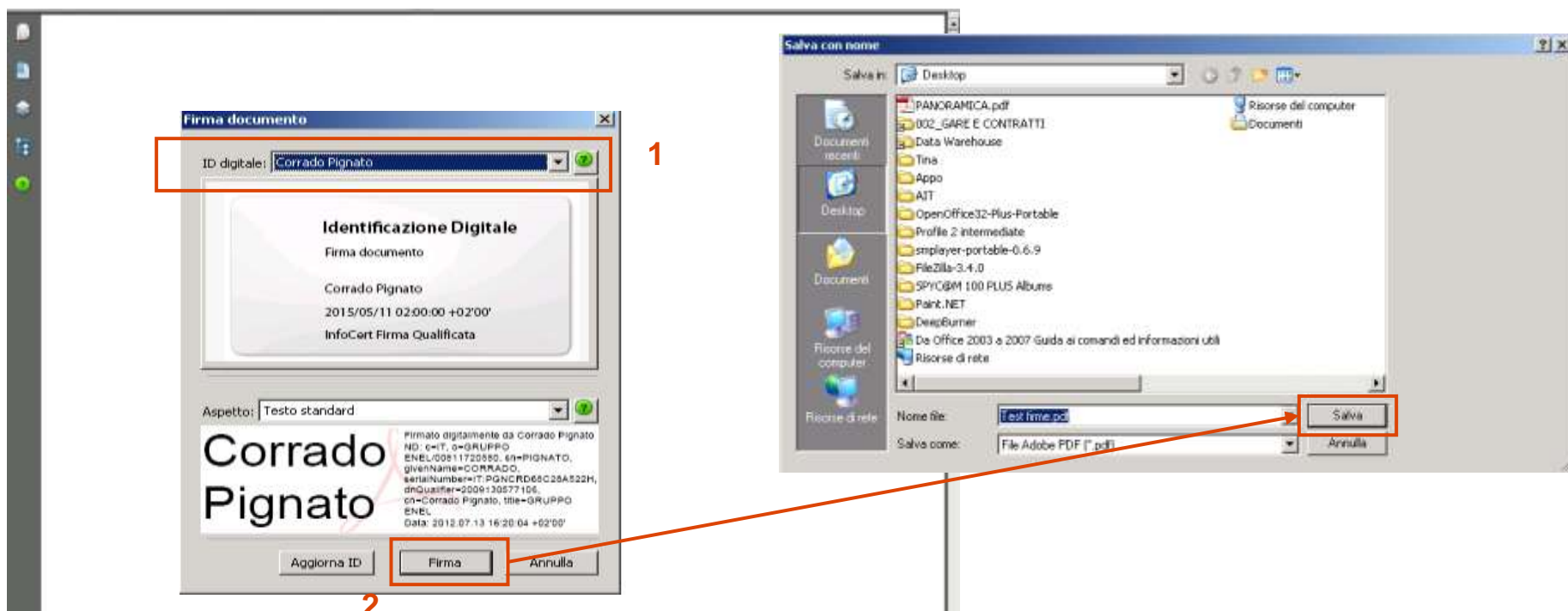
Acrobat 8 program utilization

Digital signature and timestamp (2/5)



The coming pop up enables to post the signature on the document, after selecting the document area where the signature have to be inserted and the certificate to be used (1) then click on **Sign** (2).

Fill in the name of the signed file and click on **Save** (3)

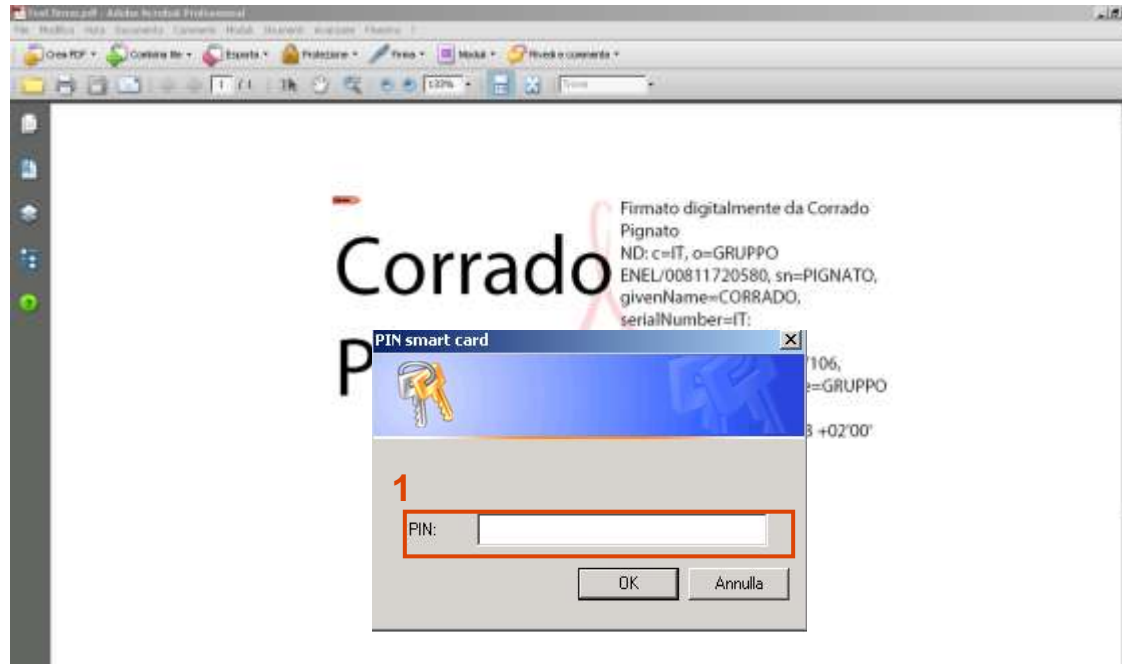


Acrobat 8 program utilization

Digital signature and timestamp (3/5)



The signature appears in the previously selected area and the system requires to insert the **Smart Card PIN** (1).



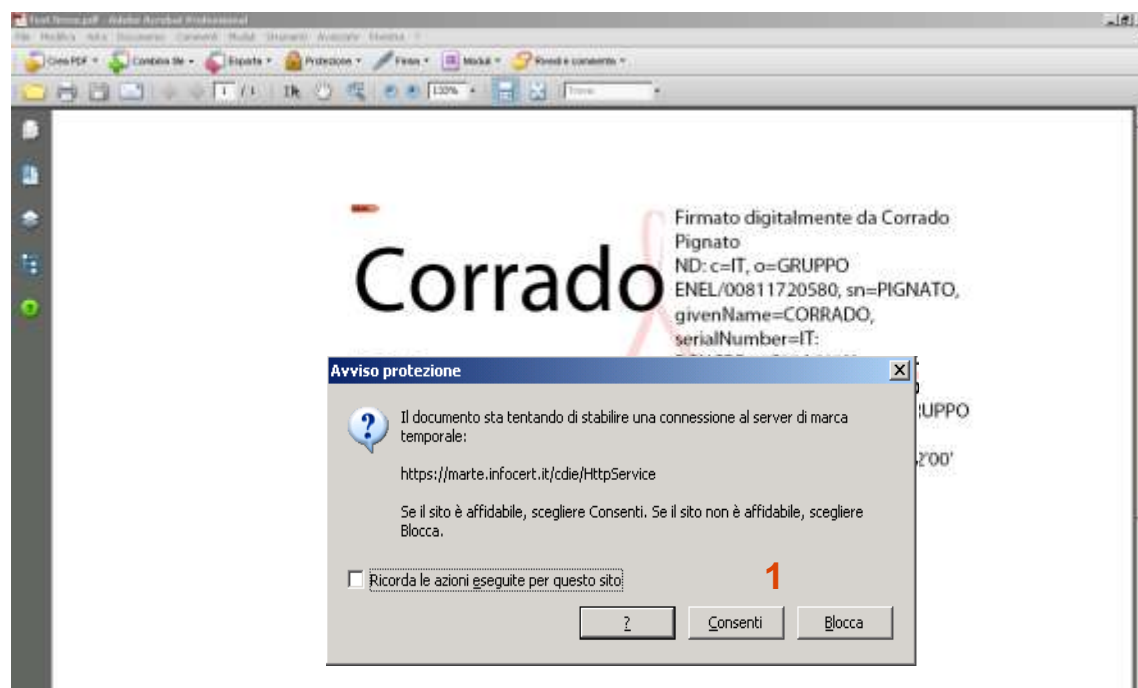
Acrobat 8 program utilization

Digital signature and timestamp (4/5)



Once completed the document signature, the system goes on with the timestamp^(*) application. To confirm the log on to the serve to apply the time stamp to the document click on **Allow** (1) . The program will use user name and password previously set in the configuration step.

() Please remind that the timestamp service is subject to fees defined by the used provider*

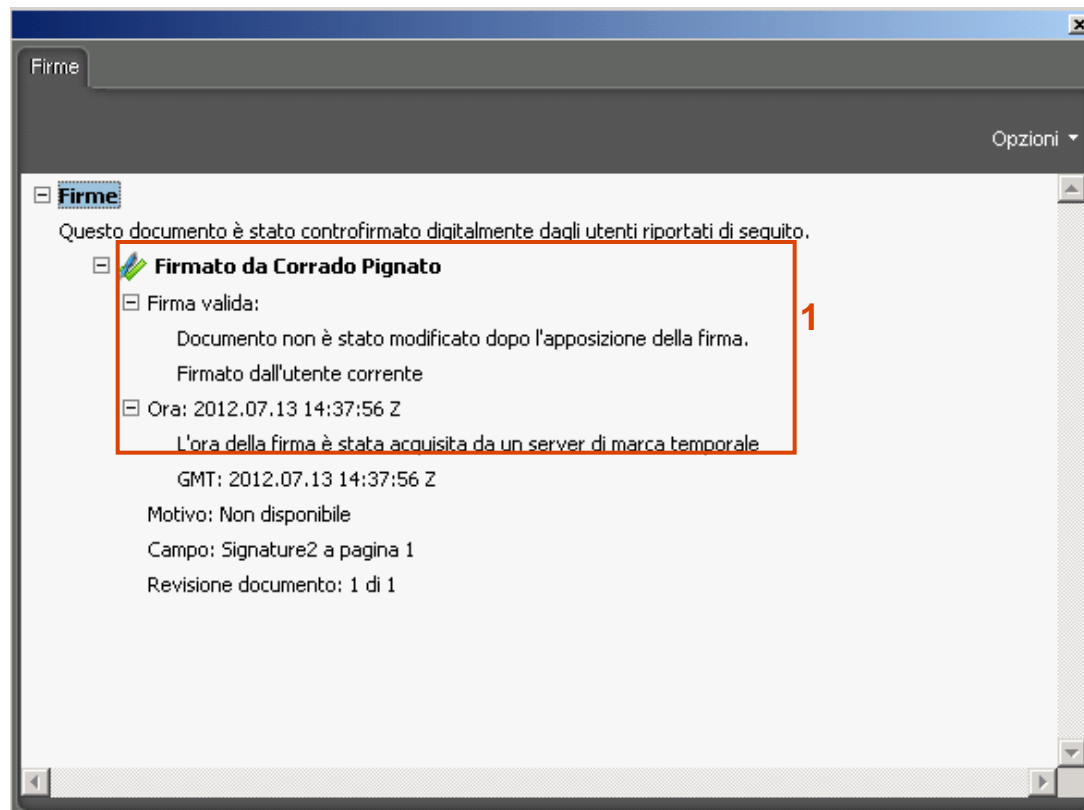


Acrobat 8 program utilization

Digital signature and timestamp (5/5)



Open the signature panel to verify the **digital signature validity** and the **correct timestamp^(*) application (1)**



() Please remind that the timestamp service is subject to fees defined by the used provider*

Dike 5.3.0 (or later)

program

utilization



Dike 5.3.0 program utilization



Initial settings (1/3)

- First step to setup Dike 5.3.0 for the digital sign is to link the signature device (i.e. Token USB) and the personal computer
- Then go on with the specific software setup (driver) that will enable the computer to dialog with the signature device
- At this point, configure the directory where files and parameters for Digital Signature and Timestamp^(*) will be stored and finally certify and sign documents (slide 17-22)

For detailed documentation please look at the following link:

- › <https://www.firma.infocert.it/installazione/>
- › https://help.infocert.it/firma/guide-firma/?_ga=1.72319060.672499180.1429689758

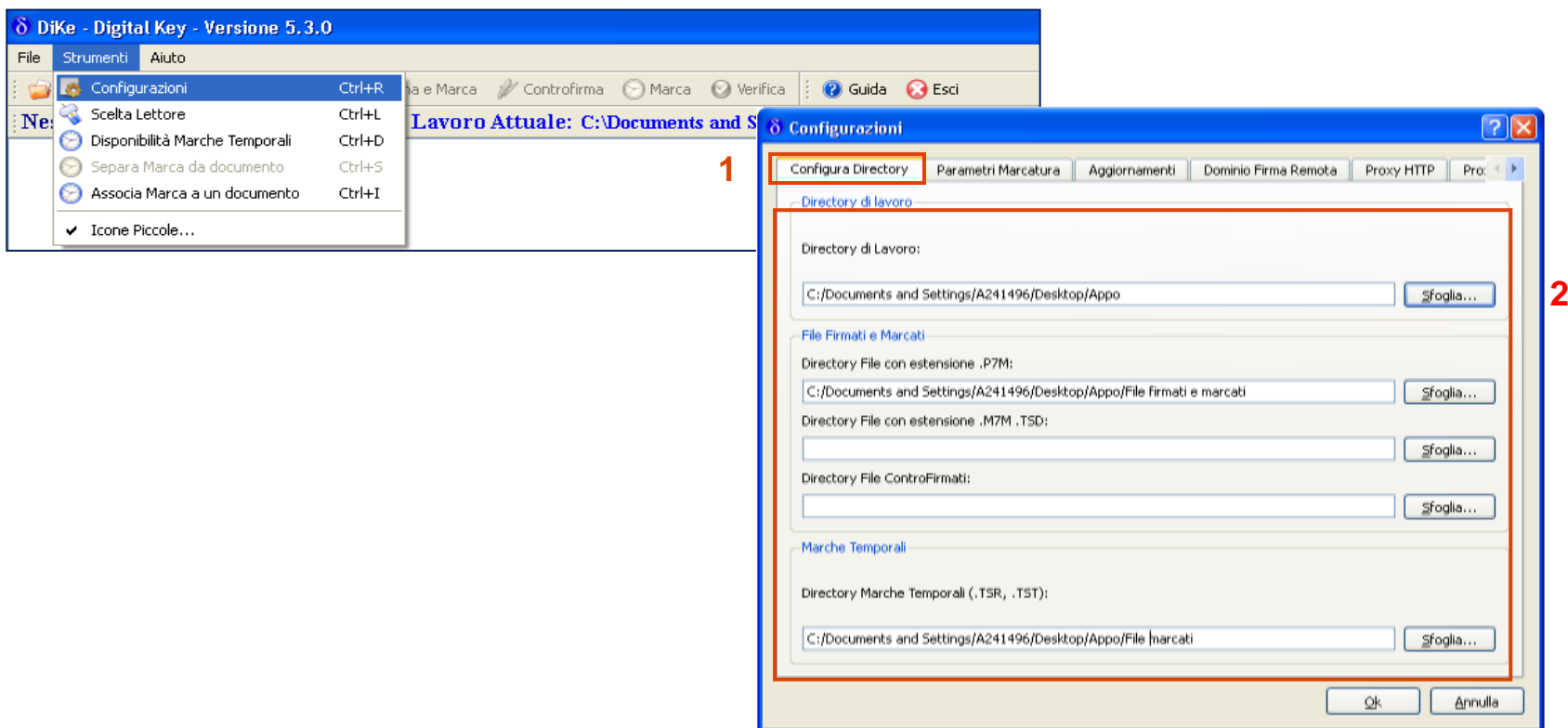
() Please remind that the timestamp service is subject to fees defined by the used provider*

Dike 5.3.0 program utilization

Initial settings (2/3)



Once the program is open, it is necessary to set directories where different types of file has to be saved, by clicking on **Tools> Settings**, selecting the “**Directory Settings**” section (1) and then by inserting required information (2)

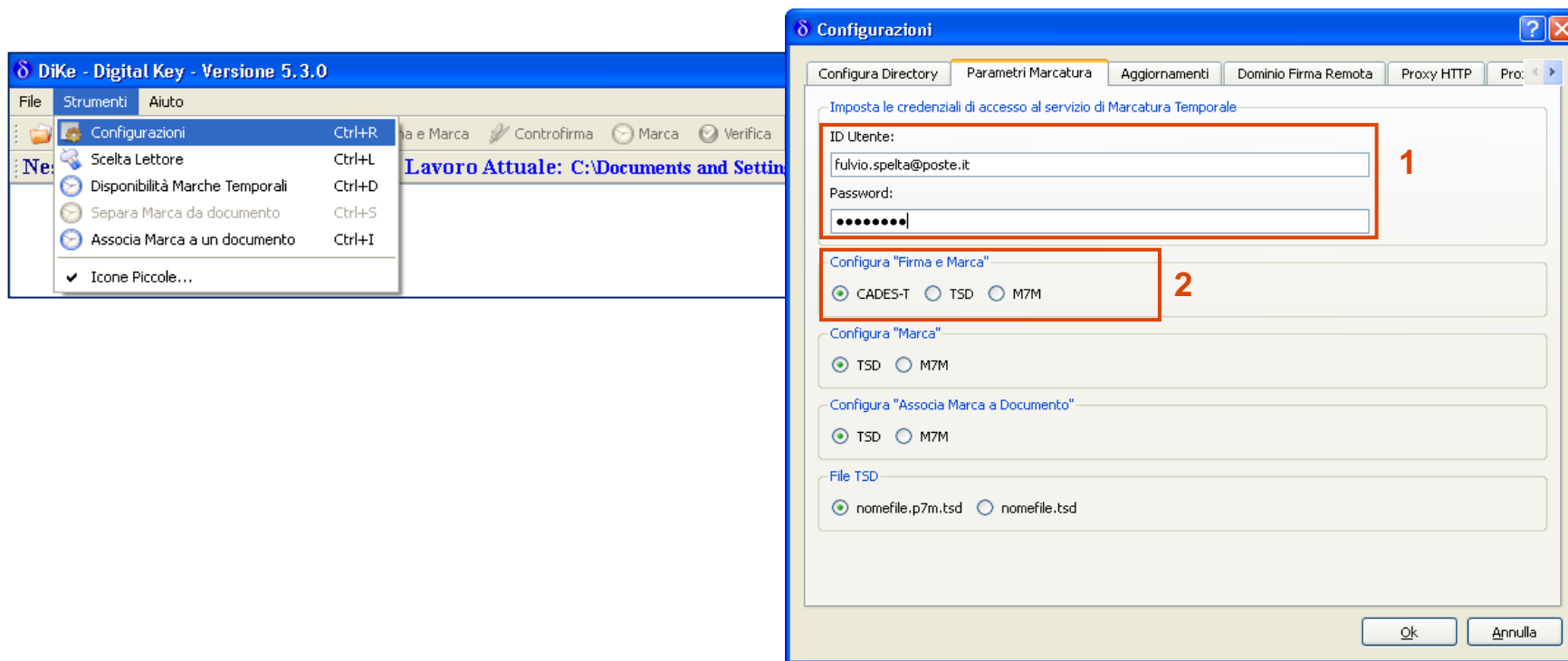


Dike 5.3.0 program utilization

Initial settings (3/3)



In the “**Marking Parameters**” section it is possible to set credentials to access to timestamp^(*) service by inserting **User ID and Password** (1) and by selecting “**CADES-T**” in the field **Set “Signature and Timestamp”** (2) in order to assure that the signed and marked file will keep the .p7m extension as required by Enel



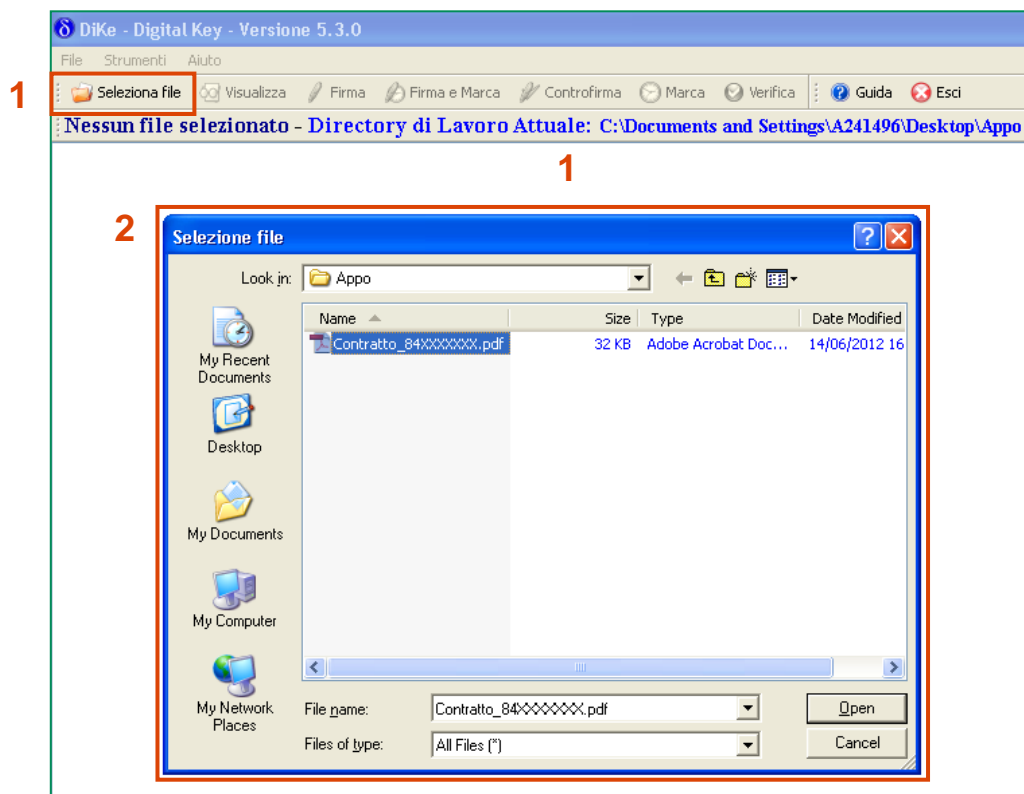
(*) Please remind that the timestamp service is subject to fees defined by the used provider

Dike 5.3.0 program utilization

Digital signature and timestamp (1/4)



To sign a document and to associate it a timestamp^(*) it is necessary to visualize it by clicking on **Select file** (1), getting access to the Files list (2) and select the document of interest, then click on “Open”



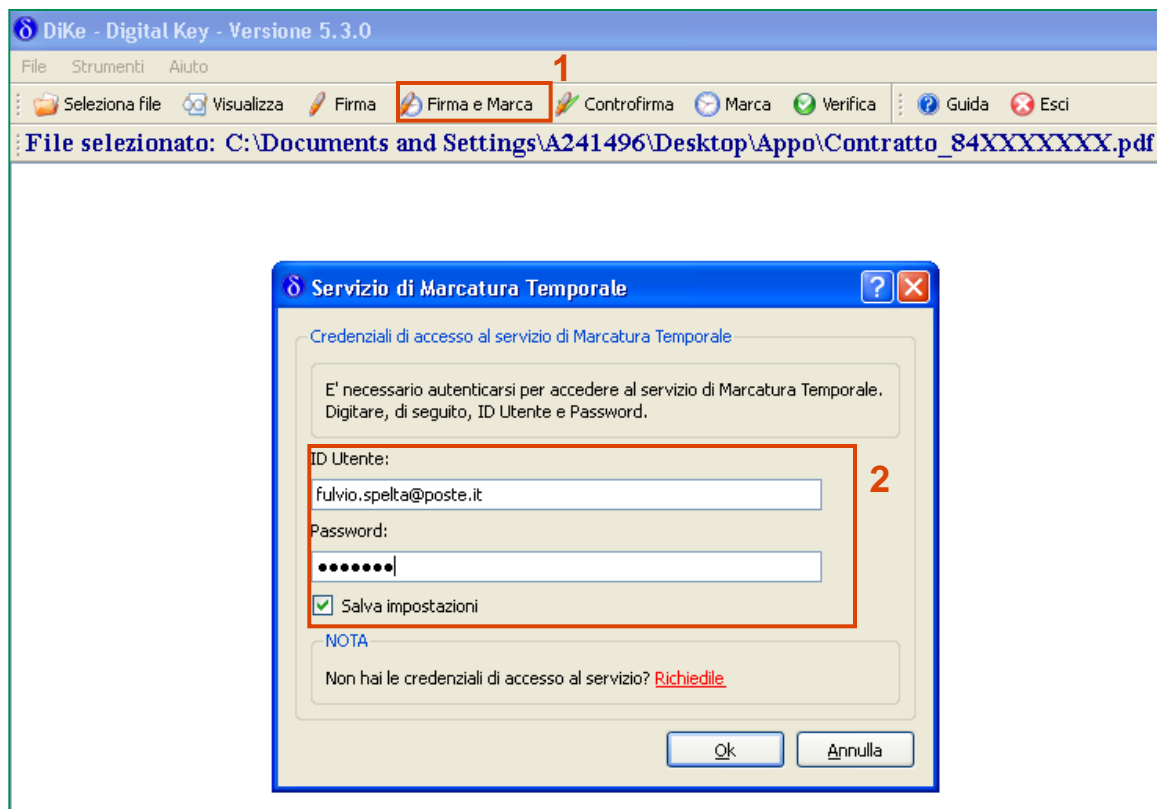
() Please remind that the timestamp service is subject to fees defined by the used provider*

Dike 5.3.0 program utilization



Digital signature and timestamp (2/4)

Now the user can require the timestamp^(*) association by clicking on **Sign and Mark** (1) and inserting only his Password in case User ID was previously set (2)



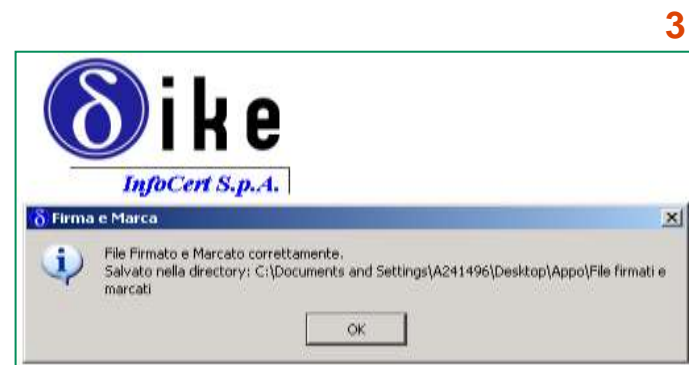
(*) Please remind that the timestamp service is subject to fees defined by the used provider

Dike 5.3.0 program utilization

Digital signature and timestamp (3/4)



The system will **verify the timestamps^(*) availability** (1), will require **the insertion of smart card PIN** (2) and will **return the procedure outcome** and the folder, previously set by the user, where the document could be retrieved (3)



(*) Please remind that the timestamp service is subject to fees defined by the used provider

Dike 5.3.0 program utilization



Digital signature and timestamp (4/4)

By selecting the file in the folder where it was stored, the system highlights several information like **the timestamp^(*) verification outcome** (1). As highlighted, the document kept original .p7m extension (2)

2

Nome File	Esito Verifica	Algoritmo Digest	Firmatario	Ente Certificatore	Cod. Fiscale	Ruolo	Stato	Organizzazione	Unità Organizzative
Contratto_84XXXXXXXXX.pdf.p7m (Firme totali apposte: 2)	Firma CADES OK	SHA-256	CORRADO PIGNATO	InfoCert Firma Qualificata	PGNCRD68C28A522H	GRUPPO ENEL	IT	GRUPPO ENEL/00811720580	
	Marca sulla Firma OK Data Marca: 11/07/2012 11.25.42 (UTC Time)	SHA-256	ICEDT504201206	InfoCert Time Stamping Authority			IT	InfoCert SpA	TSA

1

(*) Please remind that the timestamp service is subject to fees defined by the used provider

Aruba Sign2 (or later) program utilization



Aruba Sign2 program utilization



Initial settings (1/2)

- First step to setup Aruba Sign2 for the digital sign is to link the signature device (i.e. Token USB) and the personal computer
- Then go on with the specific software setup (driver) that will enable the computer to dialog with the signature device
- At this point, configure parameters for Digital Signature and Timestamp^(*) (slide 25 - 30)

For detailed documentation please look at the following link:

- › <https://www.pec.it/DocumentazioneFirmaDigitale.aspx>

() Please remind that the timestamp service is subject to fees defined by the used provider*

Aruba Sign2 program utilization



Initial settings (2/2)

Once the program is open, it is necessary to set the Time Stamping^(*) service by clicking on the button “**Option and Parameters**” (1). In the TSA^(**) section, enter **Username and Password** (2), leaving the “Policy” field empty. Then click on “Save” (3).

The screenshot shows the Aruba Sign2 application window with a toolbar containing icons for Firma, Verifica, Timestamp, Opzioni e Parametri (highlighted with a red box and labeled 1), Gestione Carta, and Cifra. A dialog box titled 'Opzioni e Parametri' is open, with the 'TSA' tab selected. The 'Parametri Time Stamping Authority' section contains the following fields: 'Indirizzo Server' (https://servizi.arubapec.it/tsa/ngrequest.php), 'User Name' (tsa.test.ale, highlighted with a red box and labeled 2), 'Password' (masked with dots, highlighted with a red box and labeled 2), and 'Policy' (empty). The 'Salva' button is highlighted with a red box and labeled 3.

(*) Please remind that the timestamp service is subject to fees defined by the used provider

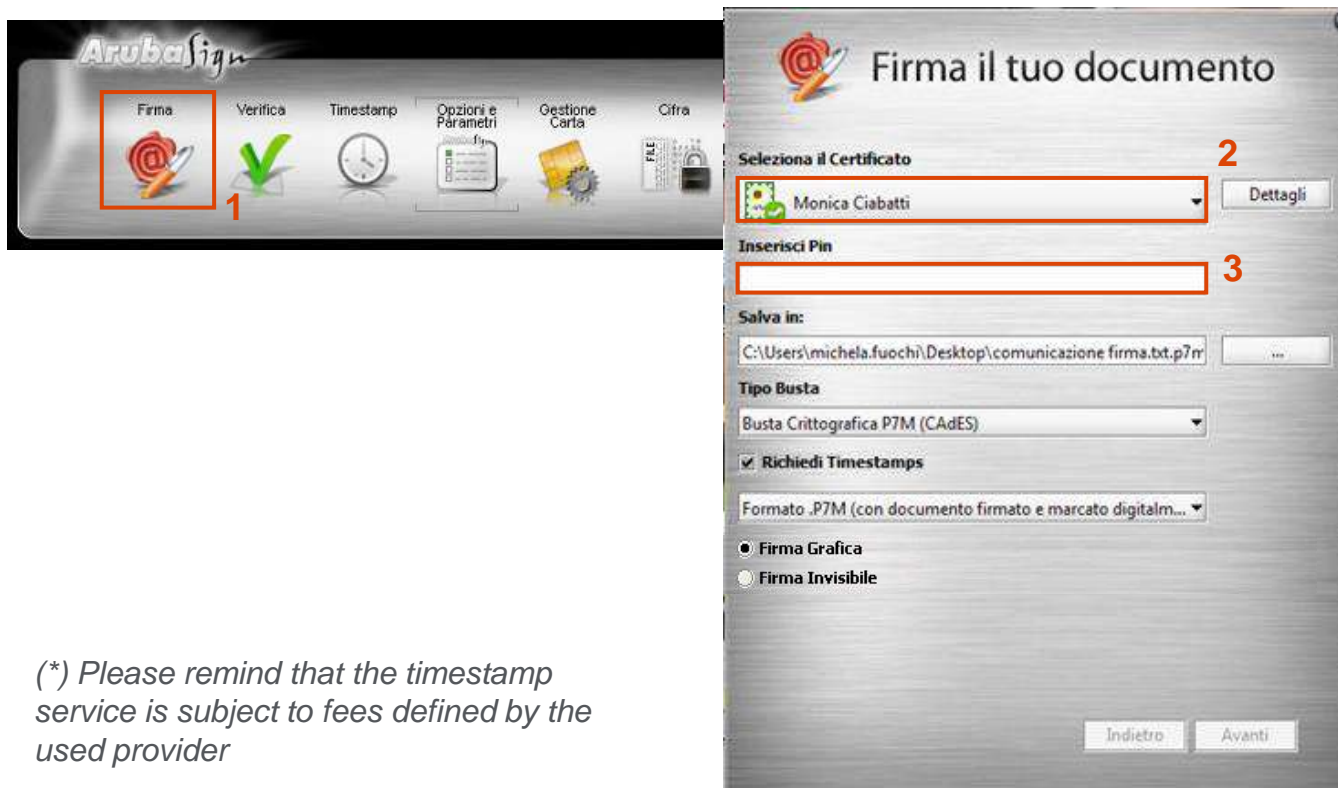
(**) Server address parameters refer to timestamp purchased from Aruba provider. In case of different type of timestamp the users has to ask his provider for the right parameters

Aruba Sign2 program utilization



Digital signature and timestamp (1/5)

To digitally sign a document and mark it with a valid timestamp, click on “**Sign**” (1) and select the file to sign. In the next screen, make sure to have selected **the proper certificate for the digital signature** (2) and insert the pin code of the device (3).



(*) Please remind that the timestamp service is subject to fees defined by the used provider

Aruba Sign2 program utilization



Digital signature and timestamp (2/5)

Verify that the path used to save the signed file is the desired one (1), select the option “**Encrypted Envelope P7M**” (2) and check that the options “**Request Timestamp**” (3) and “**Graphic Signature**” (4) have been selected. To go on, click on “**Next**” (5).



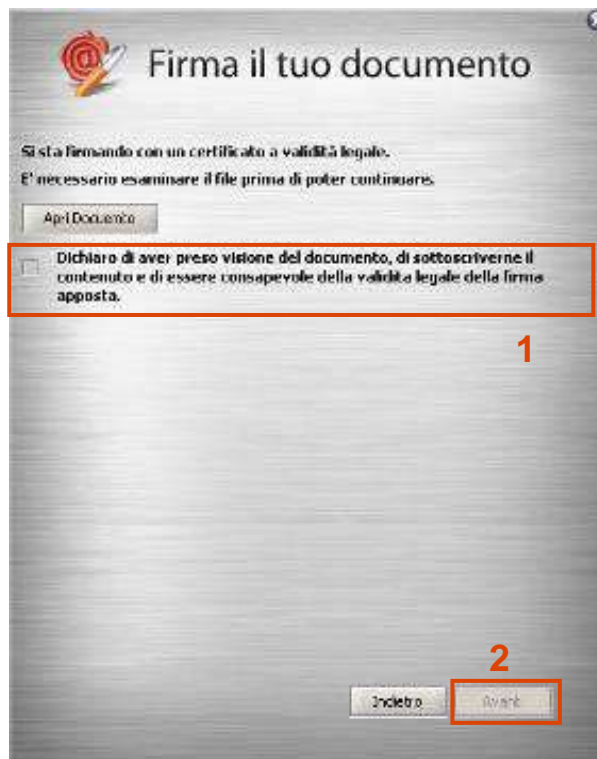
Aruba Sign2 program utilization

Digital signature and timestamp (3/5)



If needed, review the file to be signed clicking on “Open Document”. To continue **mark the disclaimer**, declaring to be aware of the legal validity of the signature that is going to be appended to the document (1).

Now, the “**Next**” button is enabled and it’s possible to proceed (2).

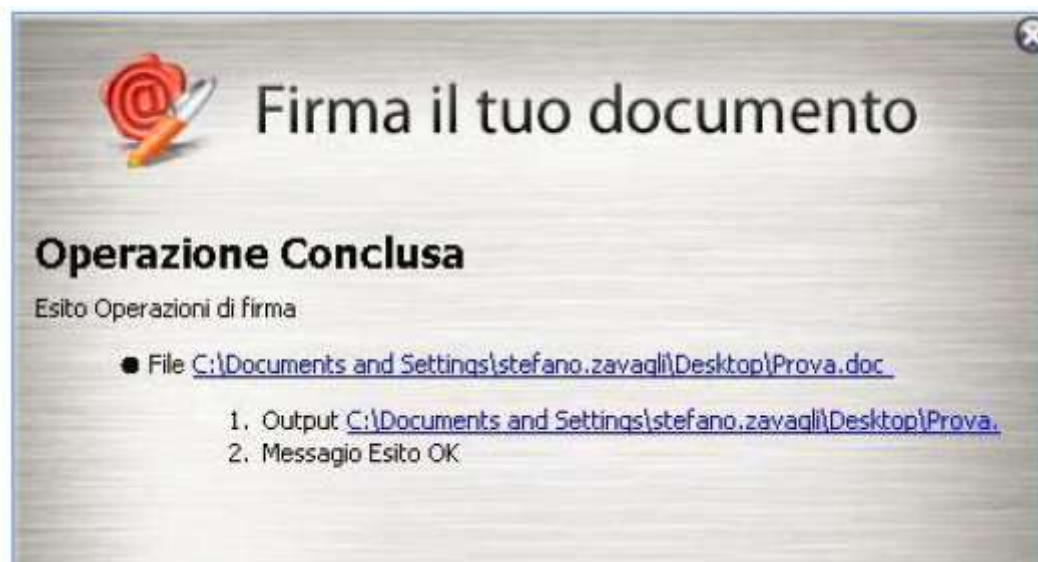


Aruba Sign2 program utilization

Digital signature and timestamp (4/5)



The system will go on verifying the availability of timestamps(*) and **returning the message with the outcome of the procedure** and the indication of the folder, previously set by the user, where the document can be retrieved



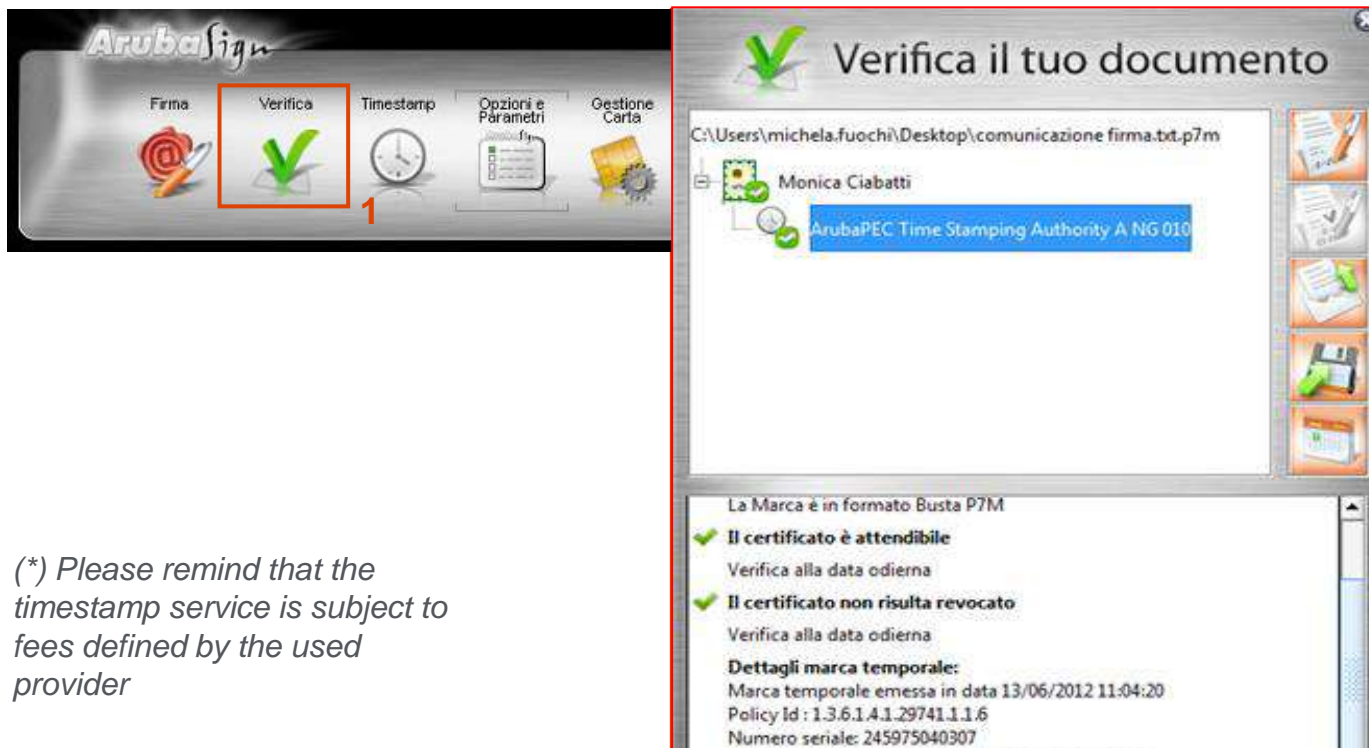
(*) Please remind that the timestamp service is subject to fees defined by the used provider

Aruba Sign2 program utilization

Digital signature and timestamp (5/5)



Drag the document that you have just signed and marked on the “Verify” button (1). The software starts checking the document and at the end of the process a summary screen is displayed (2) where detailed information are about the validity of the certificate and the timestamp used to sign the document



(Please remind that the timestamp service is subject to fees defined by the used provider*