



USER'S MANUAL

SOFTWARE TO SIGN AND ENCRYPT DOCUMENTS "FILE PROTECTOR"

November 2011

Introduction.....	3
Basic concepts.....	3
How to sign a file.....	5
Sign a set of files.....	6
Sign a set of XML files.....	7
Sign a set of PDF files.....	7
How to sign a folder.....	8
How to sign in PDF mode.....	9
How to sign in XML mode.....	11
How to do multiple signatures.....	11
File Encryption.....	13
Verification and/or decryption.....	15
Signatory verification.....	16
Folder verification.....	18
Time stamping.....	19
Time stamping verification.....	22
Certificates management.....	24
PIN management.....	25

Introduction

This manual indicates how to use the software for digital signature, time stamping and coding of files of any type and dimension, in compliance with current laws and technical requirements referred to.

The software is available for Windows, MacOS X e Linux.

Basic concepts

Digital signature

Digital signature is an operation that creates a crypto code that proves identity and integrity of a document. In other words, digital signature allows to verify:

- if document is signed by a specific person;
- that such document has not been modified after being signed.

Digital signature is based on crypto algorithms that request to use the ownership of a private key and of a relevant certificate. Private key and certificate are usually stored on an electronic device similar to a credit card, called smartcard or on a USB token (both are microchip devices with crypto functions). During a signature creation, it is necessary to type a PIN code to use the smartcard or the USB token.



Smartcard



Token USB

A certificate is a file containing necessary information to verify signature:

- owner's name and tax code;
- company's name (when needed);
- Certification Authority's name;
- expiry date;
- owner's public key;
- other related information.

Certificate is granted to user by a third trusted party, called Certification Authority.

After being created, the signature is usually stored in a file called crypto envelop; the envelop also contains the document and subscriber's certificate, to keep together all information necessary to verify. There are different kinds of crypto envelope: the most common is known as PKCS#7 (in this case file ends with P7M).

To have legal value (in this case the signature is defined "qualified") there are legal requirements to be fulfilled (for keys, certificates, smartcards, Certification Authorities, etc.).

Icon of a document signed using the software is the following.



Time Stamping

Time-stamping is an operation to get, from a trusted third party, a small file called time stamp. This allows to prove that document was really existing starting from a specific moment (date and time), to solve any claims related thereto. Document time stamping is very important in several situations, such as:

- dispatch of document on a certain date;
- dispatch of offers in reply to tenders;
- contract registration;
- patent registration.

In addition, time stamping of a digitally signed document enables to verify date and time of digital signature if such information is available in no other way.

You get time stamp sending a request via internet to an Authority called "Time Stamping Authority" (TSA). The request contains document digest. TSA replies creating time stamp and sending it to users. Time stamp contains:

- sure data and time creation;
- document digest;
- TSA name;
- TSA digital signature;
- other related information.

To have legal value, time stamp must be issued by a Registered Authority, acting in compliance with ruling law. TSA is therefore a role belonging to a Certification Authority. Time stamping icon is the following:



Encrypting

Document encryption makes a document totally illegible to anybody except for the owner of the key that allows decryption. Encryption grants to keep information as confidential.

To encrypt a document in such a way that only a particular user can read it, sender must have at disposal certificate of said user, as encryption needs to use public key.

To decrypt a document, user must have his own smartcard, as encryption needs to use private key.

Encryption and digital signature can be mixed: a document can be signed and subsequently encrypted, to grant both authorship and privacy.

The icon of a document encrypted is the following:



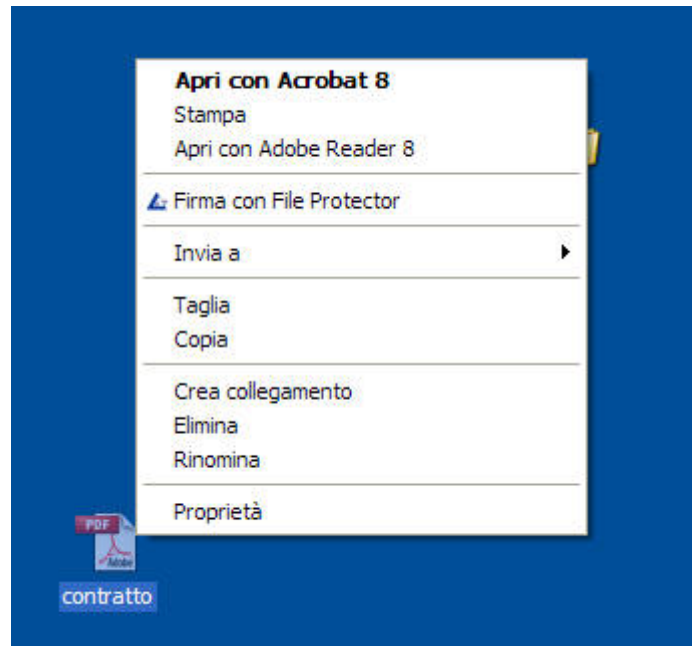
How to sign a file

To sign a file, you need at least one valid certificate on you smartcard. Should you have more than one, so you will have to choose the certificate when signing.

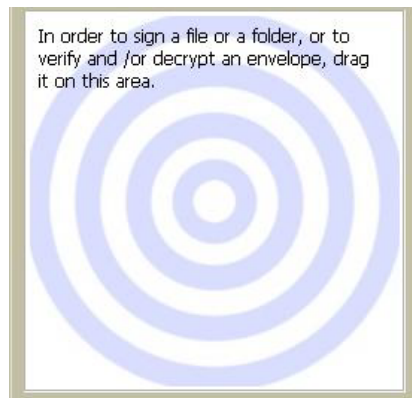
You can start digital signature in three different ways, as follows:

- outside the application, using Windows Explorer menu;
- inside the application, using “drag and drop”;
- inside the application.

The first way is available at the moment only in Windows environment. It consists of clicking on the icon of the chosen file using right mouse button to see the relevant menu, then select “Sign with File Protector” to start application and sign the file. You will be requested the smart card PIN code. Digital signature will be stored in the same folder you started with, carrying P7M in the end. E.g., the signature on the contract.pdf will be stored in a file called contract.pdf.p7m.



Second way is particularly useful if the application is already running. In this case, signing a file can be started by dragging the icon of the chosen file to target area.



Third way is possible if the application is running:

- choose "Sign" on the "File" menu;
- or Click on the "Sign" button on the toolbar.

In both cases you see a file selection box.

Starting signature inside the application also enables Multiple signature (see paragraph relevant to).

Sign a set of files

By selecting "Sign a set of files" you can sign "in one solution" a set of files stored in different folders.

The files to be signed are listed in the higher basket of the box showed by the application. You can add a file to this list both by clicking on "Add" button and by dragging the file icon in the basket

(drag and drop). Can be signed also file already signed (in these cases another signature will be added).

"Remove" and "Remove all" buttons allow you to cancel the selected file or all of them from the basket.

In order to open a file before signature, you can double click on the item in the list: the file will be opened running the associated application (for example a PDF will be opened using Adobe Reader).

By clicking "**Sign**" button, P7M signature will be applied to all the files in the list. Resulting envelopes are stored in the same folder as original.

Sign a set of XML files

In a similar way to "Sign a set of files" you can run "Sign a set of XML files" that allows to sign in XML Detached signature mode a set of XML files stored in different folders.

In the higher basket are listed the XML files to be signed. You can add a XML file to this list both by clicking on "**Add**" button and by dragging the file icon in the basket (drag and drop). Can be signed also file already signed (in these cases another signature will be added).

"Remove" and "Remove all" buttons allow you to cancel the selected file or all of them from the basket.

In order to open a file before signature, you can double click on the item in the list: the file will be opened running the associated application (typically Internet Explorer).

By clicking "**Sign**" button, XML Detached signature will be applied to all the files in the list. Resulting envelopes are stored in the same folder as original. Signed XML documents are name with the suffix (signed). For example the signed version of "pippo.xml", will be pippo(signed).xml.

Sign a set of PDF files

In a similar way to "Sign a set of files" you can run "Sign a set of PDF files" that allows to sign in PDF mode a set of PDF files stored in different folders.

In the higher basket are listed the PDF files to be signed. You can add a PDF file to this list both by clicking on "**Add**" button and by dragging the file icon in the basket (drag and drop). Can be signed also file already signed (in these cases another signature will be added).

"Remove" and "Remove all" buttons allow you to cancel the selected file or all of them from the basket.

In order to open a file before signature, you can double click on the item in the list: the file will be opened running the associated application (Adobe Reader).

By clicking "**Sign**" button, Adobe signature will be applied to all the files in the list. Resulting envelopes are stored in the same folder as original. Signed PDF documents are name with the suffix (signed). For example the signed version of "pippo.pdf", will be pippo(signed).pdf.

How to sign a folder

You can sign in one step all files contained in a folder in two ways:

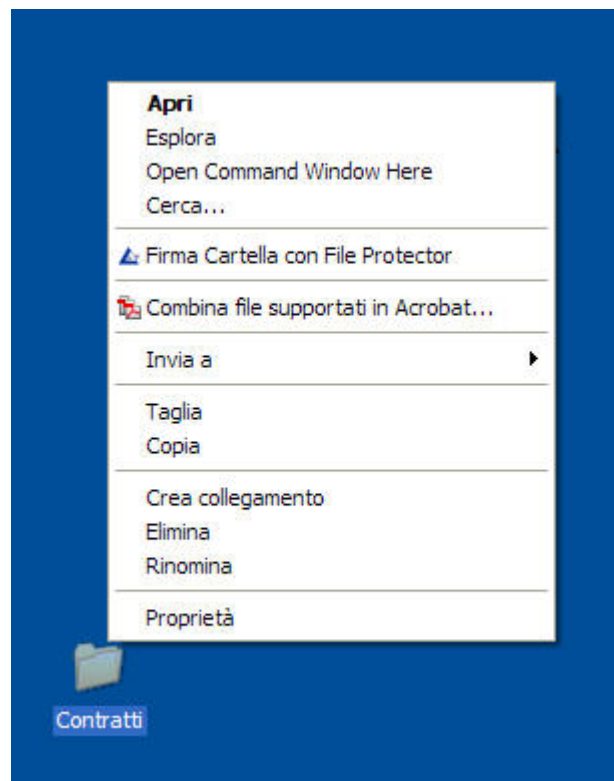
- single signature of each file;
- signature of a list of fingerprints.

In the first case you get as many cripto P7M envelop as the files contained in input folder. In the second case, you get one crypto envelop in XML format. The second way is quicker. If input folders contains many documents, in this way you can save memory disc.

As already seen in single signature, you can start multiple signature in three different ways, as follows:

- outside the application, using Windows Explorer menu;
- inside the application, using "drag and drop" item;
- inside the application.

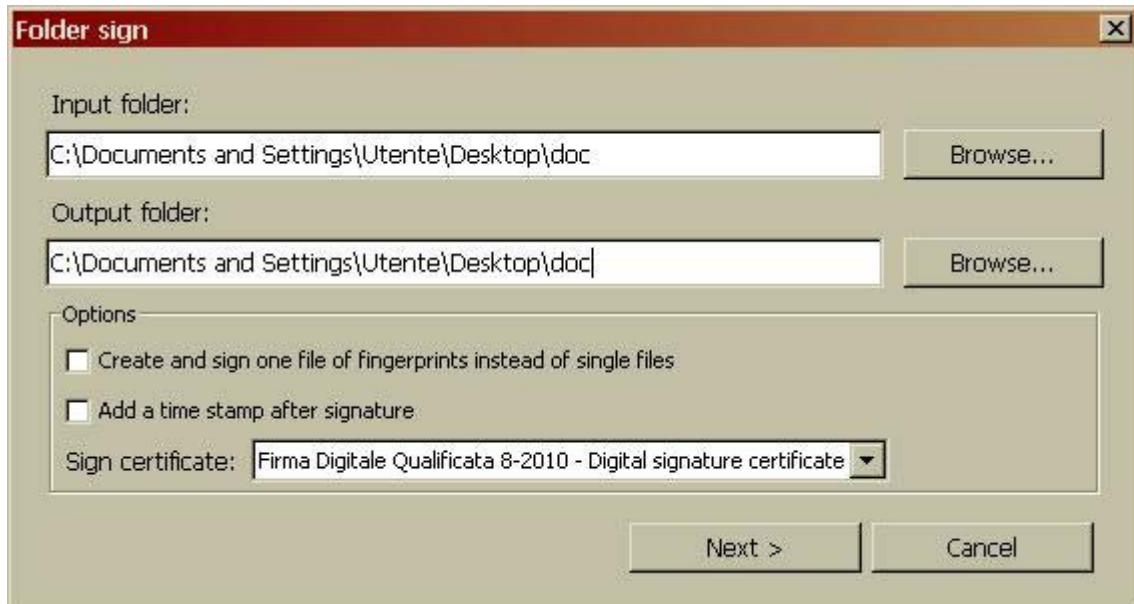
First way is available, at the moment, only for Windows and consists of clicking on chosen icon using right mouse button to see the relevant menu, choose "Sign folder with File Protector" to start application and signature process.



Second way is particularly useful if the application is already running. In this case you can sign a folder dragging the folder icon on target area.

Third way is possible if the application is running. It consists of choosing “Sign Folder” on the “File” menu.

Whatever way you have chosen, you see the following box:



In this box you have to choose way and relevant signature option. Then, clicking on “Forward” button, signature process starts.

How to sign in PDF mode

You can put one or more digital signatures into a PDF document with no need to create a separate crypto envelope. The application can sign also in PDF mode, user can therefore choose P7M signature or PDF signature, if needed.

PDF signature gives you the possibility to be verified using Adobe Reader, very used, and it can be easily compared to an hand written signature. On the other hand, PDF signature is less used and accepted than P7M signature, even if having same technical and legal value. In addition, you can use it only with PDF documents.

There are two kinds of PDF signature, from a graphic point of view

- invisible signature (with no picture for the signature);
- visible signature (with picture for the signature).

The application is always able to create invisible signature, on the contrary, to create a visible signature the document is requested to contain a signature space, expressly conceived. Each signature creates a new document release, PDF mode signature distinguish into:

- certification signature;

- approval signature.

Approval signature is generally referred to a document created by this parties, its only consists of verifying subscriber's identity and document integrity.

Certification signature enables also to document authorizations to subsequent modifications.

Usually the subscriber that signs using a certification signature is either the author or the person in charge to document. In addition, a certification signature is always shown in Adobe applications, even if not create inside a signature box.

Both signature are supported by the application.

To sign a document in a PDF mode you have to choose item "PDF signature" on the menu "File". After having selected the chosen document, the following dialogue box appears:

Signatory	Date and time	TS	Sig...	Revision

Select certificate to use for signing:
Firma Digitale Qualificata 8-2010 - Digital signature certificate

Select revision to be signed: Signature <N>

Reason: I approve this document Certification of this document

Changes allowed after certification: No changes allowed

Locality: Milan

Specify the folder to save signed document:
C:\Documents and Settings\Utente\Desktop\firmati\contratto1(signed).pdf

If you want to create a certification signature, select relevant box and choose on the pop up menu the necessary authorizations.

It is also possible, upon choice, to fill the item "Reason" and "Place". In this case, also such information will be signed.

Finally, to add a signature to a document, you only have to choose certificate and click on the button "add signature".

It is also possible to start PDF signature process on the Windows menu, clicking with right mouse button on the chosen document, selecting menu item "Sign with File Protector".

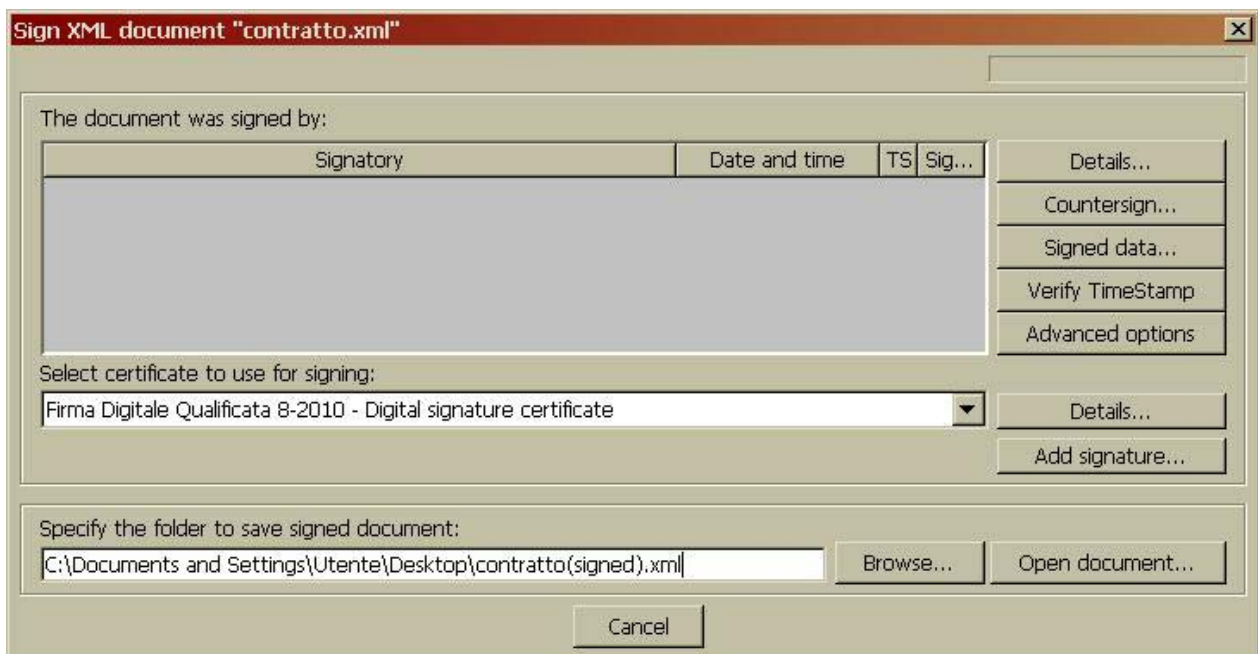
How to sign in XML mode

As an alternative to p7M and PDF modes, digital signature can also have a XML code (extended Markup language). XML mode signature is particularly suitable to XML documents, but can also be used with any kind of documents.

XML mode signature is not very common yet, as it is used most in finance and health fields, anyway XML signature has the same value of P7m and PDF ones.

In comparison with p7M signature, XML signature is more adoptable but also more "technical": in fact it can be issued into three different forms (enveloped, enveloping, detached) and has many choices that, for the sake of brevity, we don't delve deeper in this manual.

To sign a document in a XML mode, choose item "XML signature" on the "File" menu. After having selected the document, the following dialogue box appears:



How to do multiple signatures

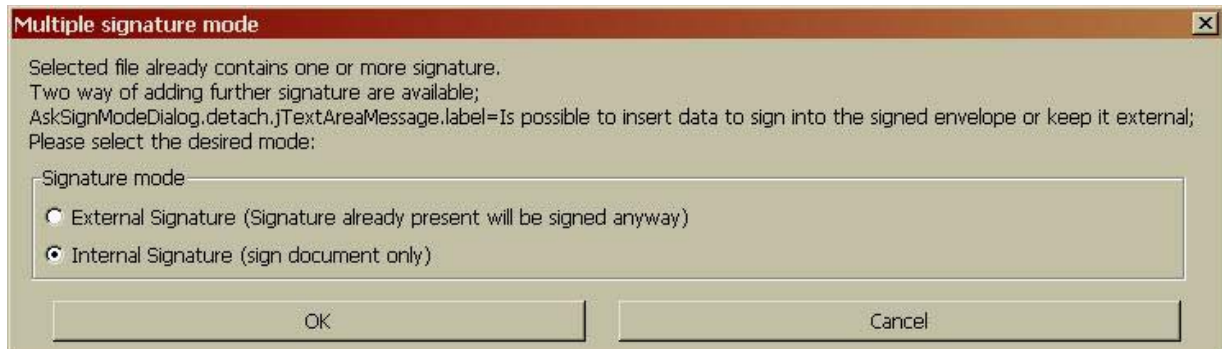
A single document can be signed by many digital signatures. These are called "multiple signatures". This allows to prove that many people had got authorship and/or responsibility as to document, maybe on different moments, as it often occurs with handwritten signature (e.g. as to contracts, balance sheets etc.).

There are three kinds of multiple signatures:

- "matrioska";
- "parallel (also called independent);
- counter signatures (also called nested).

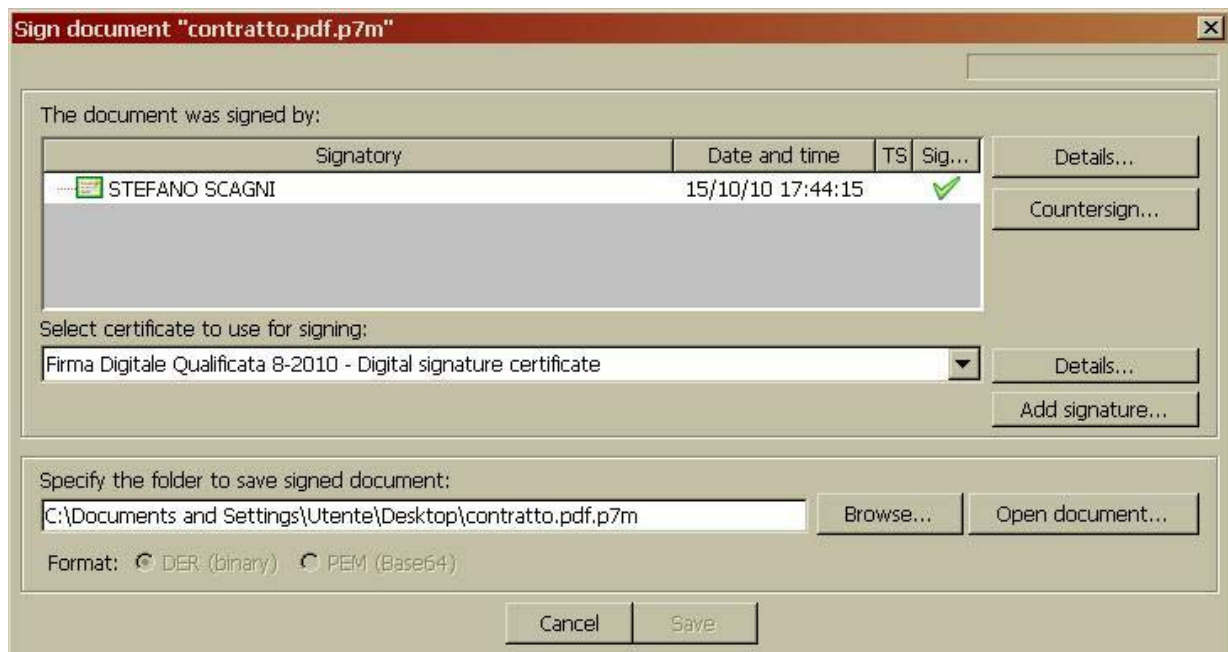
The first kind is obtainable by simply signing a crypto P7M envelope (that contains a document that is already signed). This digital operation is equal to sign a paper envelope already containing a

signed document, as a matter of fact, sometimes this operation is really done in this way (e.g. as to paper envelopes containing offers to tenders). To create a matrioska signature it is requested to sign inside the application, clicking on "sign" button or choosing the relevant menu item. When the application realizes that the chosen document is a P7M envelope, the following dialogue box appears:



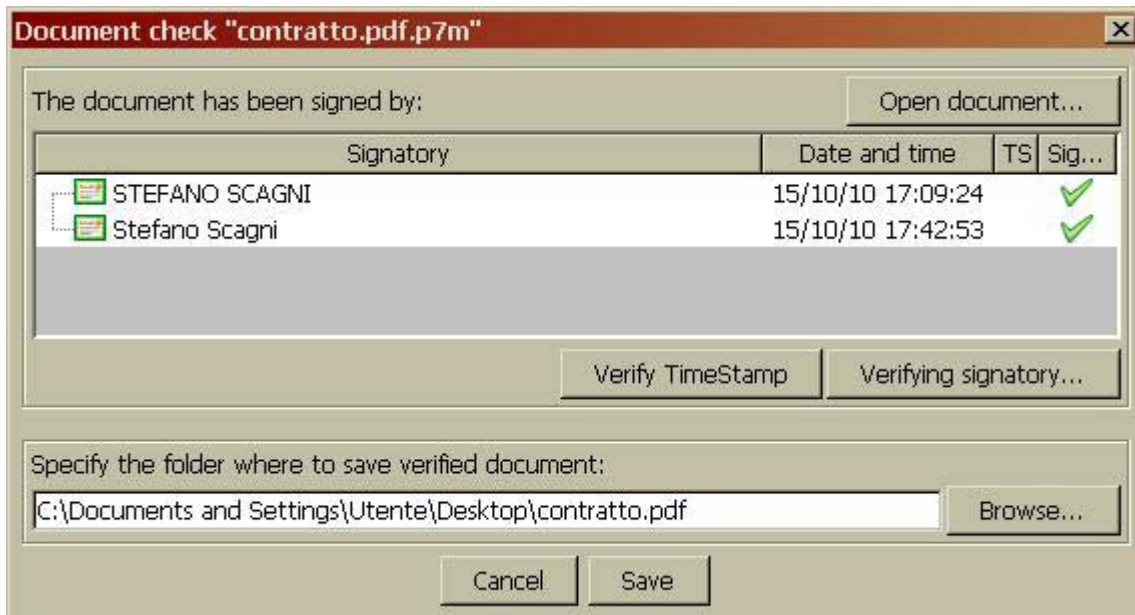
To create a multiple matrioska signature you have to choose "external signature", while choosing item "inside signature" it is possible to create multiple signatures of the first and second kind.

The following dialogue box appears:



The second kind of digital signature (called parallel or independent) consists of adding more signature beside the first one, each signature is independent (each subscriber signs the same data the others have already signed). This digital operations is equal to signature made by different people at the bottom of the same paper document.

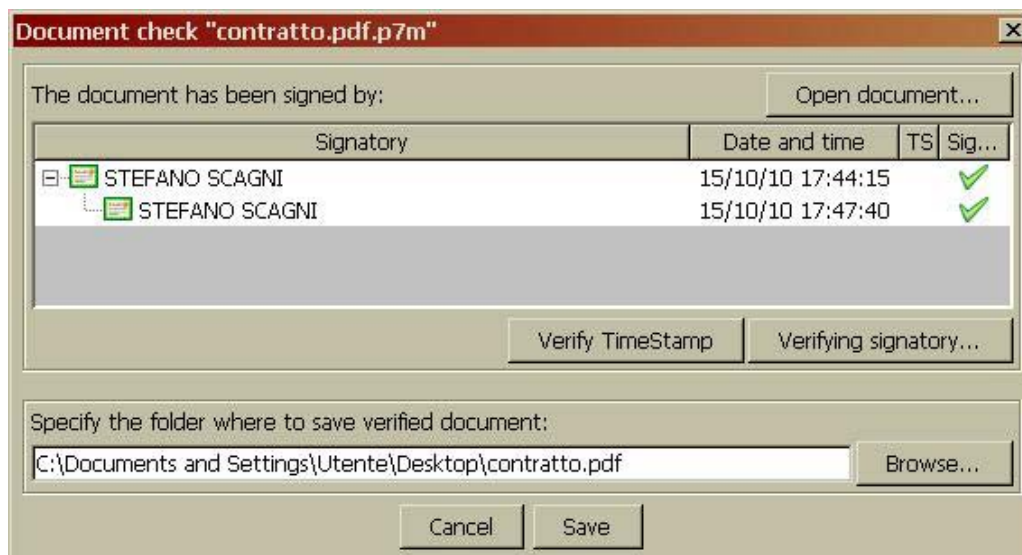
To add an independent signature, click on the button "add signature" in the box shown before. When verifying, you see that the document contains three added signatures:



The third kind of multiple signature (called counter or nested signature) is created by signing an already existing signature and keeping the result (called countersignature) inside the same envelope. In this way the second subscriber agrees with or validates the first signature. The second signature can be also signed by a third person, and so on.

To add a counter signature, choose the relevant box, then click on the button "counter sign" in the box shown above.

When verifying, you see the document contains counter signature (please note the tree shape).



File Encryption

Encrypting a file requires the encrypting certificate of the addressee (the user meant to be the only one to decrypt the document).

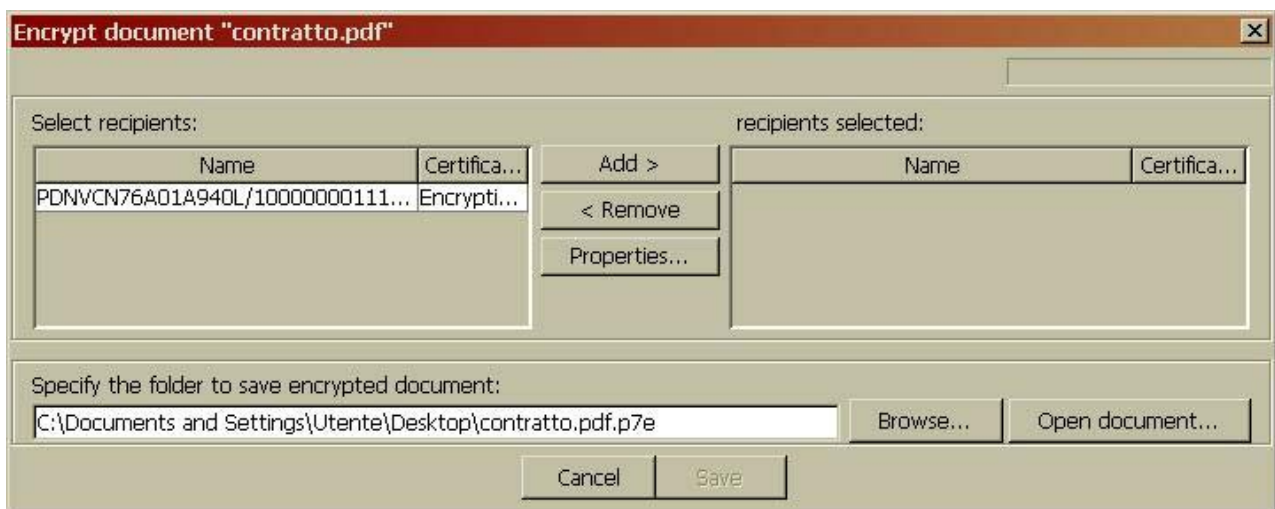
Should the certificate be issued on a directory server, you can download and import it in your certificates database, directly from inside the application (see paragraph referred to).

Otherwise, you can ask the addressee for the certificate and manually import it in your certificates database.

It is possible to encrypt a document for many addressees, so that they - and only they - are the only ones able to decrypt it.

To encrypt a document, click on the "encrypt" button in the main application box, or choose the relevant item on the "File" menu.

After having chosen the document, the following dialogue box appears:



On the left there is a list of available encryption certificates (the ones in your own certificates database), on the right there is a list of addresses certificates. You can add and remove the addressee of encrypted document.



To complete operation, click on "save" button.

Digital signature and encryption can be made together on the same document, to grant both origin (and integrity) and secrecy. To do this, click on "sign and encrypt" button on the main application box, or choose the relevant item on the File menu.

Encrypting a file requires the encrypting certificate of the addressee (the user meant to be the only one to decrypt the document).

Similarly to file encryption, you can encrypt all files in a folder and recursively in subfolders.

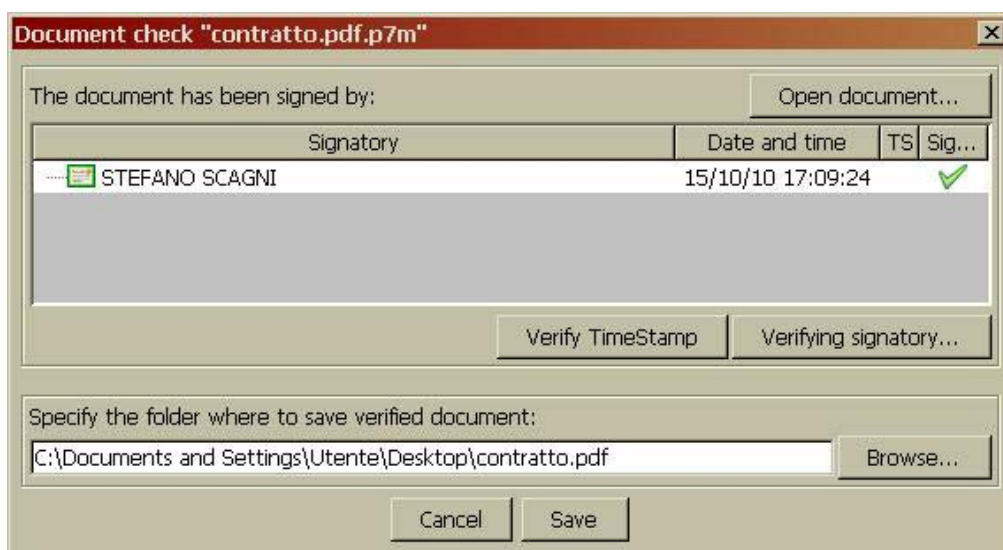
In order to encrypt a folder select "**Encrypt folder**" in "**File**" menu . You are requested to specify folder to encrypt and application will proceed like file encryption.

Verification and/or decryption

To verify and / or decrypt a document signed using P7M standard can be done in five different ways:

- by double clicking on the file to be verified;
- on Windows Explorer menu (choose the item "verify");
- with "Drag and drop";
- clicking on "verify" button or choosing the item "verify" of File menu.

At the end of verification the following dialogue box appears:



In this box you can:

- verify the signature validity;
- verify the validity of the signature of each subscriber;
- see the signed document, take it and store it in a file;
- see and verify digital stamp of the digital signature (when existing).

Verification of a document signed using xml standard can be done in two different ways:

- outside the application, with Windows explorer menu (as above described);
- inside the application (as above described).

At the end of verification the following dialogue box appears:

The same procedure is provided in case of document signed in XML or PDF standard.

To encryption of a document can be made different ways:

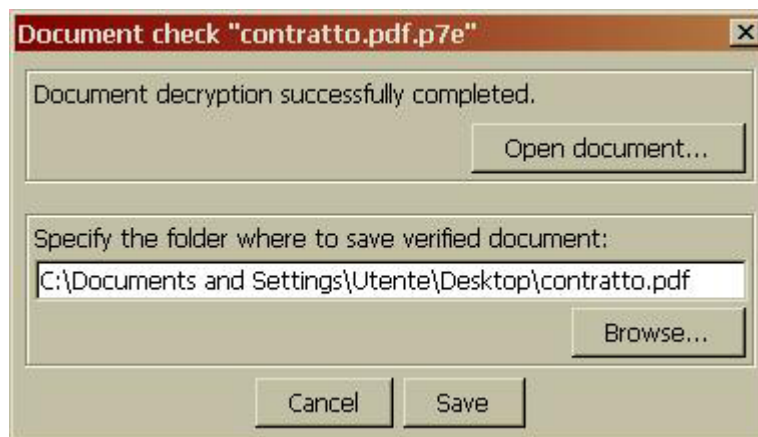
- click on "verify" button in the main box;
- choose the "verify" item on the "File" menu;
- either drag the chosen document on the target area.
- either with double click on document icon.

Then choose item "encrypt with File Protector" on the relevant menu.

If you do not have the private encryption key, the following error message appears:



Otherwise, the following dialogue box will let you save the original document:

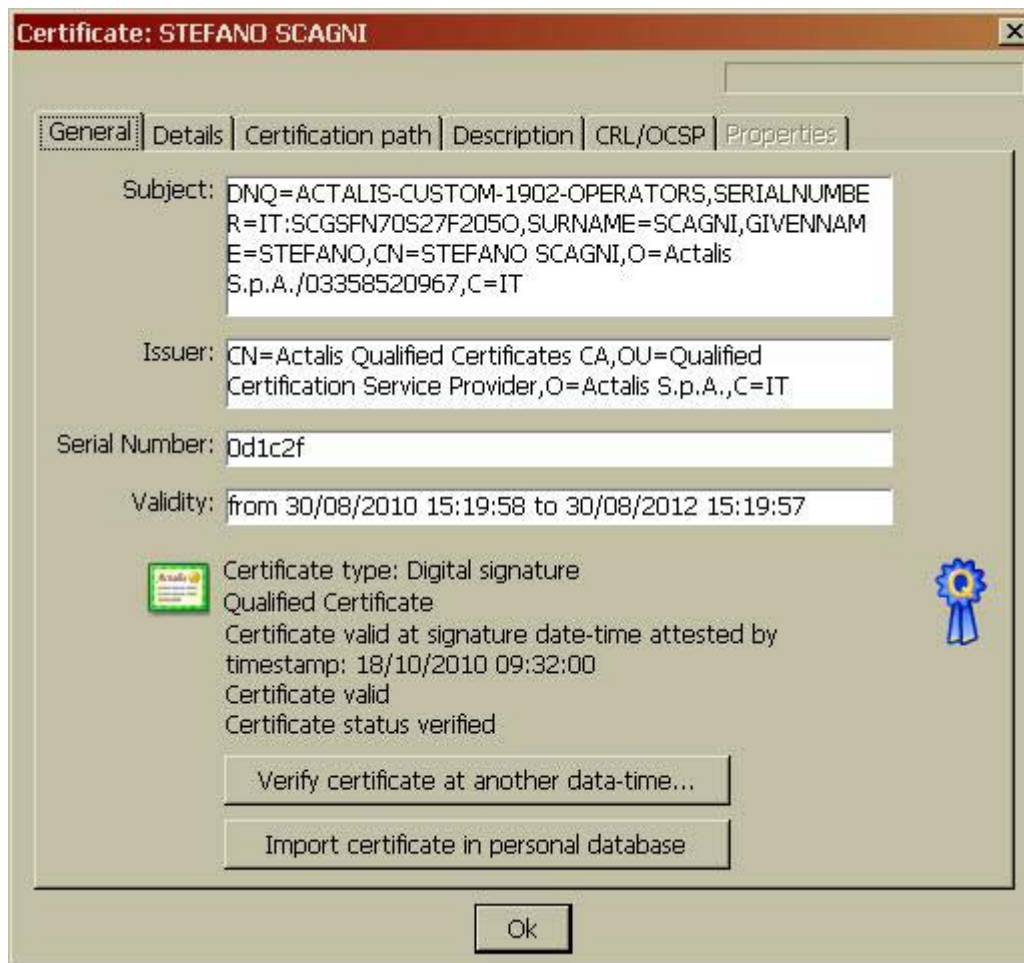


Signatory verification

Complete verification of a digital signature always requires two steps:

- digital signature verification (integrity verification);
- verification of subscriber's certificate.

In previous passage we described the first step. The second very important step starts with clicking on the button "verify subscriber" of the summary digital signature box. In a short time, a box of the following kind appears, to show the result of verifications:



Please note that verification of a certificate is always at the same date of digital signature, as follows:

- time and date of digital stamp of the digital signature (when existing);
- otherwise date and time taken from signing Time (when existing);
- otherwise current date and time of operating system.

To verify a document on a different date and time, click on the "verify certificate at a different date and time" button. The following dialogue box appears:



Using the selectors provided, it is possible to set chosen date and time to verify certificate. Clicking on "today" button, date and time are resettled according to operating system:

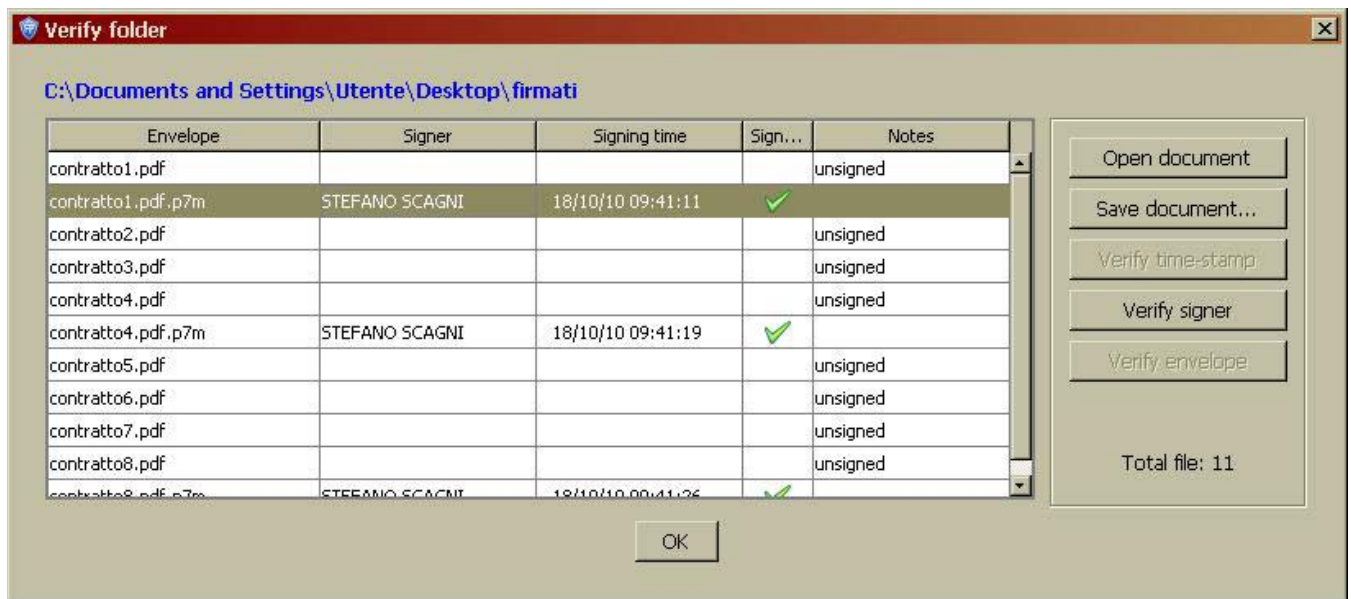
Back to certificate box, use the button "import certificate in personal database" to see the certificate in your own certificate database, to be able to take it afterward, if encrypting is needed.

This step is valid only for encryption certificates (e.g. S/MIME or general) and is not valid for qualified certificates, as the latter cannot be used to encrypt.

Folder verification

If a folder has been signed using list of fingerprints mode, to verify it please proceed as provided for an ordinary XML digital signature verification. Please choose carefully the file named "signature.xml" in the folder signed.

If single files of a folder have been signed, you can do a mass verification by choosing the item "verify folder" of the "File" application menu. After selecting input folder (containing signed documents to be verified) the following dialogue box appears:



Should the selected document have a single signature - as normally provided for a folder signature - the box shows main information resulting from verification: subscriber's name (taken from certificate) signature date and time (when existing, and proved by a digital stamp), digital signature validity and, if any, additional notes issued in case of error. To complete verification, click on the "verify subscriber" button and on "verify digital stamp" button, when existing.

Should the selected file have many signatures, so it is necessary to click on "complete verification" button.

If document is in the signed file, it is possible to see it and save it by clicking on "open document" button.

Function "verify folder" supports all kinds of signature managed by following applications: P7M/CMS, PDF, XML.

If a folder (and its subfolders) has been encrypted using "Folder encryption", you can do a mass decryption by choosing the item **"Folder decryption"** in the "File" menu.

After selecting input folder you are requested to enter token and PIN. If credentials need for decryption are available on the token, every file will be decrypted.

The functionality is performed recursively on the encrypted files in the subfolders.

Time stamping

The time stamping can be done in two ways with the application:

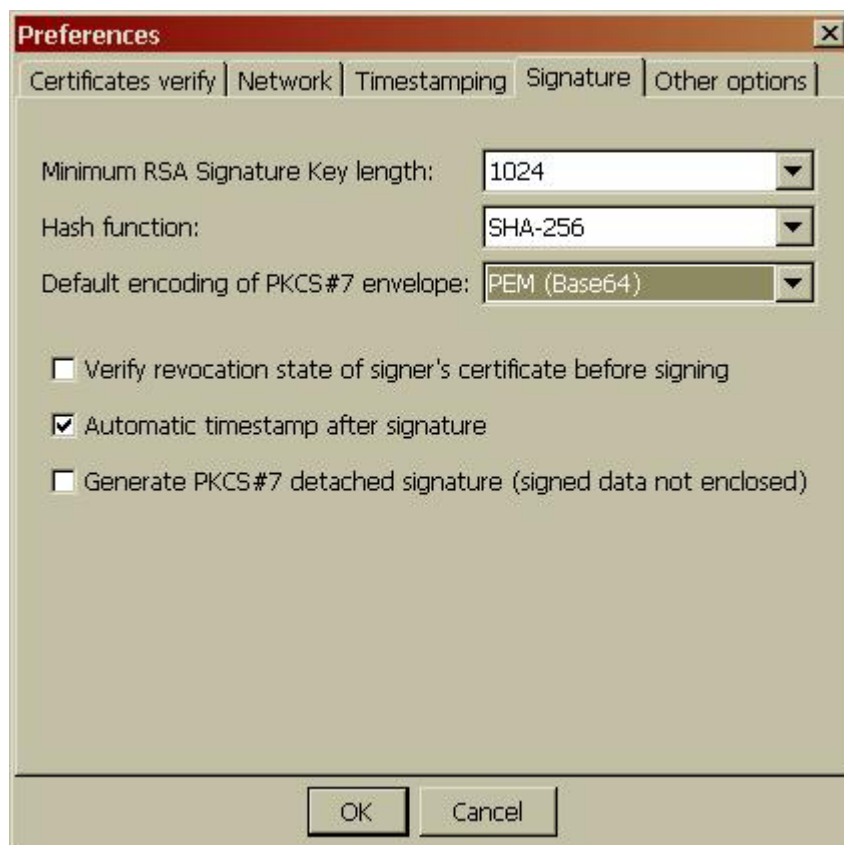
- time stamping of a single digital signature;
- time stamping of a whole document.

Time stamping of a single digital signature

Time stamping proves date and time of a particular digital signature (also consider the possibility to multiple signing). This stamp is therefore linked to digital signature and is inside the crypto envelope.

It is granted that that particular signature was created at digital stamp date and time to the person in charge to subsequent verification of digital signature.

To start this function, as to P7M and PDF mode signature, open signature choice item box and select "time stamp after signature" box:



As to XML mode signature, it is possible to start this function on a case basis, by clicking on the button "advanced options" (see picture).

Time stamps associated to single signatures can be seen and verified upon document verification.

Time stamping of a whole document

It is possible to get a time stamp proving a document existence by a certain date and time, no matter how many digital signatures it has (but it can also be a not signed document).

You can start this function by clicking on main box or choosing the relevant item on the "File" menu.

Digital stamp of a whole document can be saved in two ways:

1. as a separate file (carrying TSR extension)
2. together the relevant document, in a "stamped envelope" (carrying TSD extension).

Stamped envelope is an envelope complying with requirements of TimeStampedData, which contains:

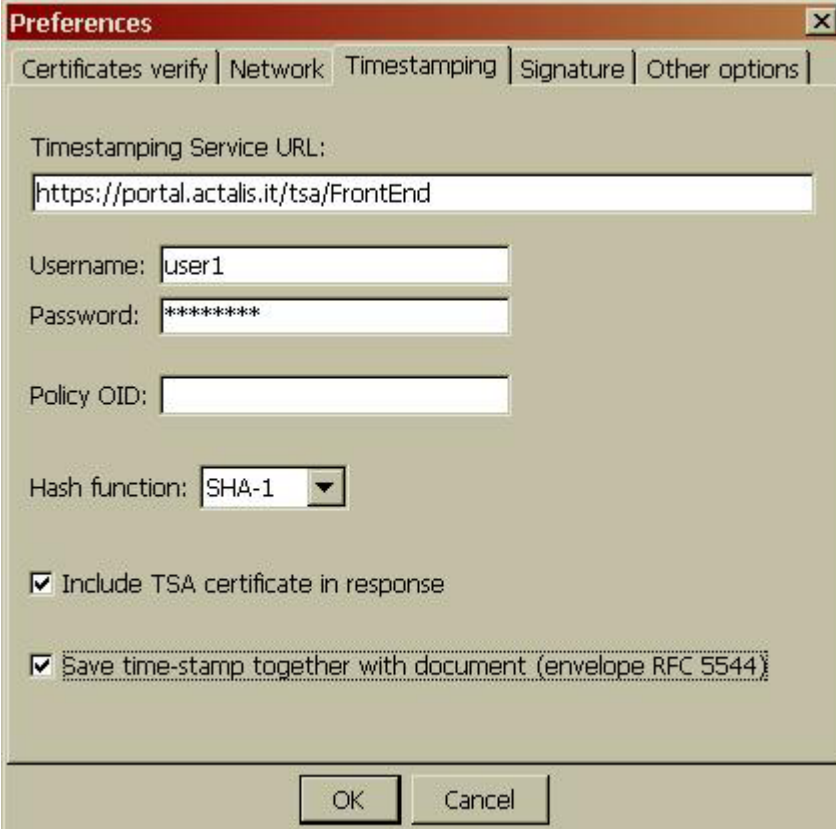
- a general document of file (no need to be signed);
- optionally, metadata referring to document (e.g. the name);
- one or more digital stamps.

Digital stamps are associated to document as follows:

- the first time stamp (T1 time) is calculated basing on document referred to and, if necessary, on METADATA;
- the second time stamp (T2 time) is calculated basing on the first one (and it proves it was existing at T1 time);
- the third digital stamp (T3 time) is calculated basing on the second one (and it proves it was existing at T2 time);
- and so on.

Stamped envelope allows to extend proof of existence of a document at T1 time even after a long time from the first time stamping. It also gives the benefit to contain the document referred to.

The choice between separate or enveloped time stamp can be done in the preference box, choosing the item "save the time stamp together with document".



The image shows a screenshot of a software preferences dialog box titled "Preferences". The "Timestamping" tab is selected. The dialog contains the following fields and options:

- Timestamping Service URL:
- Username:
- Password:
- Policy OID:
- Hash function: (with a dropdown arrow)
- Include TSA certificate in response
- Save time-stamp together with document (envelope RFC 5544)

At the bottom of the dialog are "OK" and "Cancel" buttons.

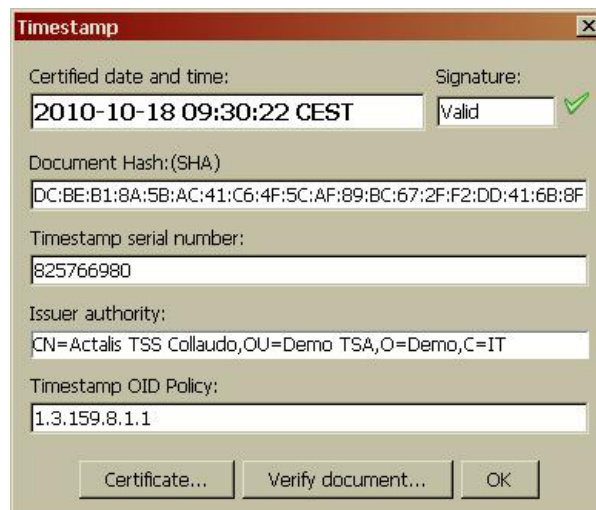
In both above mentioned cases, to get time stamps you have to access to a digital stamping service, setting service address and access credential in the preference box (click on the button referred to in the main box, then select "time stamping" form).

Time stamping verification

It is possible to verify either "free" or "stamped" envelopes. In both cases, verification can be done in four different ways:

- "double click" on the chosen file (having TSR or TSD extension);
- click on the chosen file with right mouse button and then select item "verify with File protector";
- drag the chosen file on target area;
- select item on "verify time stamp" menu.

When verifying a "free" time stamp (file with .TSR extension) the following dialogue box appears:



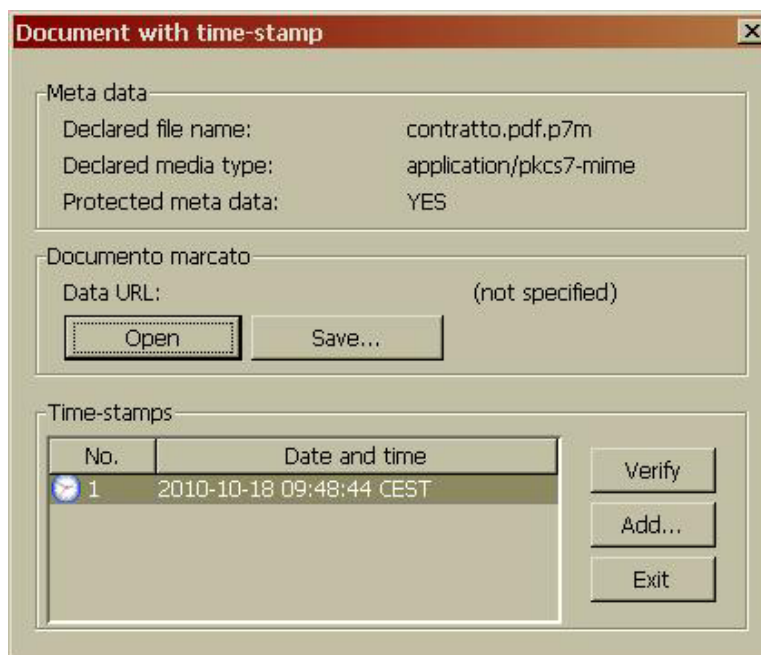
This box gives important information, such as:

- date and time of issue of digital stamp;
- TSA signature validity relating digital stamp;
- TSA (Authority) that issued digital stamp.

Click on the button "verify document" to select the relevant document and check that it really refers to the digital stamp under verification (the re-calculated document hash overlaps with the time stamp hash).

Click on the button "certificate ..." to see all details relevant to TSA certificate.

In case of a "stamped envelope" the following dialogue box appears:

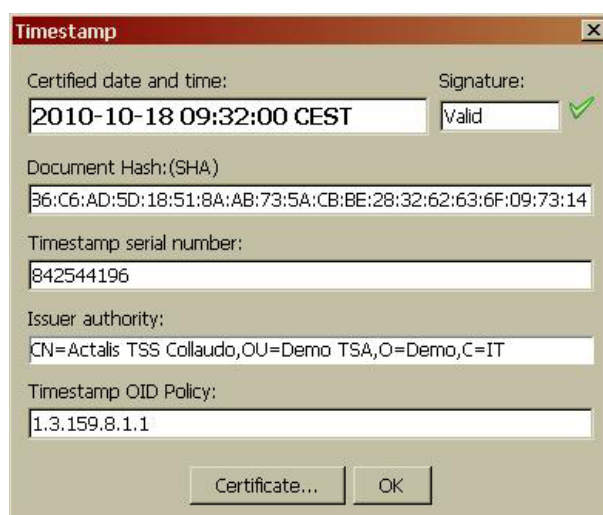


This box shows main information relating the envelope:

- METADATA (usually name of document contained into the envelope)
- list of digital stamps issued to save the document.

There are also two button "open" and "save" that respectively allow to see and save document into the envelope.

To verify time stamps, select the chosen one from the list and click on the button "verify"; the following dialogue box appears:



In this case there is not the button "verify document" as verification is automatically done with reference to document in the envelope.

Click on the button "add ..." in the verification box of a stamped envelope to add a time stamp to the ones already existing, according to procedure above described. This operation is useful if document is to be stored for a long time, beyond expiry date of time stamp.

Certificates management

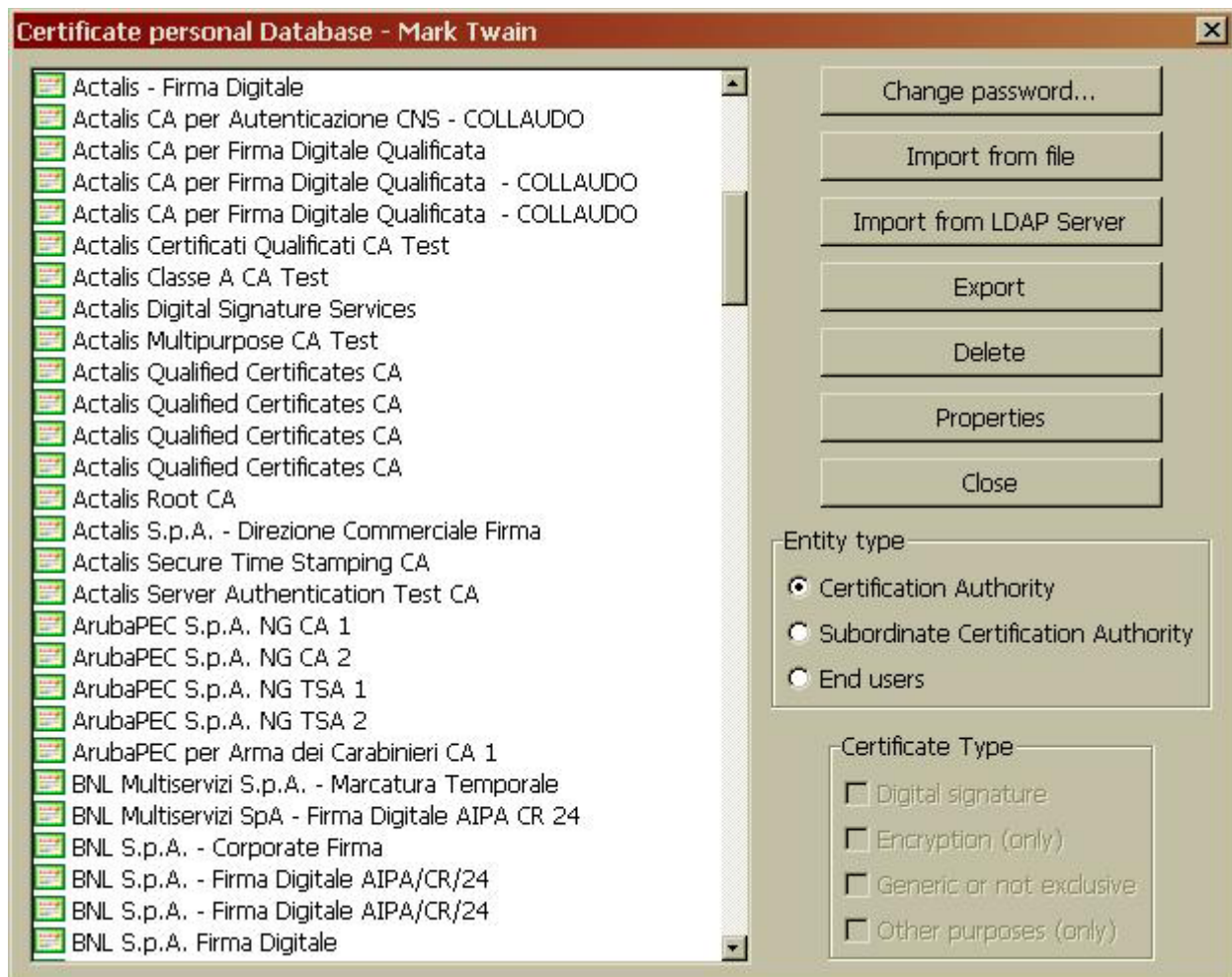
The application can manage a personal certificate database both of Certification Authorities and users:

- CA certificates are used to verify user certificates' validity;
- Users' certificates are used only in encryption.

Database is protected with a profile access password.

To add, remove and see certificates using certificates management box, select item "certificates database" on "tools and options" menu.

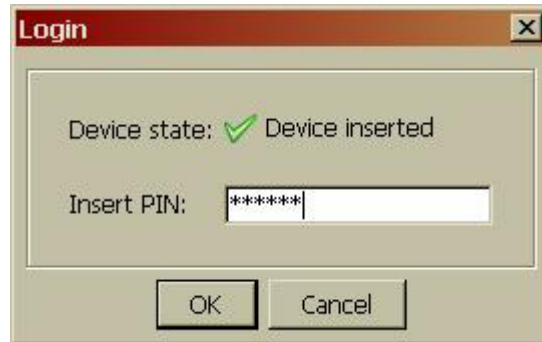
You can set up the LDAP server to use in certificates' search from the main application box.



PIN management

Digital signature device (smartcard or other similar device) is protected by a secret code called PIN. During a session with the application, to digitally sign or encrypt you have to type your smartcard PIN at least once (click on the "login" button on main dialogue box).

In some occasions you will be automatically asked to type PIN:



If you want to have the application running after a session with the application, please click on the "logout" button, to avoid third persons the illegal use of you smartcard.

It is not possible either to create your digital signature or decrypt a document if you don't know your PIN code.

It is very important that you are the only person to know the PIN code and that it is difficult to guess it.

Smart card is usually given to user together with adequate pre-settled PIN; yet you can change PIN by selecting item "PIN Change" on the "device" menu in the main box.

Due to security reasons, if you type wrong PIN more than a certain number of times (usually 3) smartcard is locked, To unlock your smartcard you have to know a secret code called PUK. Select item "unlock PIN" on the "device" menu, in the main box,

Carefully type PUK, because it can be locked too if you type the wrong code. If also PUK is locked, smart card is no more usable.