Xolido®Sign Desktop

Xolido®Sign Desktop

V2.2.1.X
User manual

Digitally signed by: XOLIDO SYSTEMS,S.A.
Reason: Approval of the document
Location: Valladolid (Spain)
Date and Time: 3/10/2017 12:39:44 PM

XOLIDO

electronic signature, notifications and secure delivery of documents

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

ÍNDICE

1. Introduction 3
2. Xolido®Sign - Panel de Control 4
3. Xolido®Sign User Guide - Sign 11
3.1. Document Management Area 12
3.2. Electronic Certificate Management Area 13
3.3. Output Folder Management Area 14
3.4. Operating Options Management Area 15
3.5. Start Operation Area 16
4. Xolido®Sign User Guide - Timestamp 17
4.1. Document Management Area 18
4.2. Timestamp Server Management Area 19
4.3. Output Folder Management Area 19
4.4. Operation Options Area 20
4.5. Start operation Area 21
5. Configuration Guide for Xolido®Sign – Sign / Timestamp 22
5.1. Certificate Options Area 22
5.2. Signature Options Area 25
5.3. TimeStamp Server Area 32
5.4. PDF Options Area 34
5.5. Output Options Area 38
5.6. Advanced Options Area 41
6. Xolido®Sign User Guide to Verify 44
6.1. Verification modes 44
6.2. Electronic verification process 46
6.3. Verification results 49
7. Technical information about Xolido®Sign 55
8. Other Xolido®Sign interesting information 56

Mod.: D201000074v07 20170301

1. Introduction

This guide describes step by step the procedure for using the **freeware application** for Windows platforms provided by Xolido Systems for digitally signing all kind of documents.

Xolido®Sign allows you to perform, on your computer and in an intuitive way, the digital signature of all the documents you need to sign. Xolido®Sign also allows you to timestamp your documents and include a timestamp into your electronic signatures, using for that a RFC 3161 compatible server that you determine.

Xolido®Sign provides functionality for verifying electronic signatures. It supports external signatures of any kind of file and extension, regardless to their size. It also supports integrated PDF signatures and timestamp verification.

During the processes, the application takes care of proper security blankets, as revocation status checking, integrity evaluation...

It performs a quick and automatic process, without complications in the form of use. It has a simple interface and self-explaining style that will guide you along the process.

Xolido®Sign is intended for use by any professional or citizen bringing new technologies of digital and electronic signature, smart signatures verification and time stamping functionality for all kinds of groups, like students, engineers, professionals of any kind, SMEs...

Using this application, the process of signing electronic documents will be greatly simplified. It also gets your shipping costs (stamps, envelopes, paper ...) reduced using electronic documents, maintaining security in your electronic transactions (invoices, contracts, posting notes...).

Mod.: D201000074v07 20170301

2. Xolido®Sign - Panel de Control

Xolido®Sign starts up by default showing the Control Panel interface. From there the user can manage and access the main features of the application. The image below shows the Control Panel.

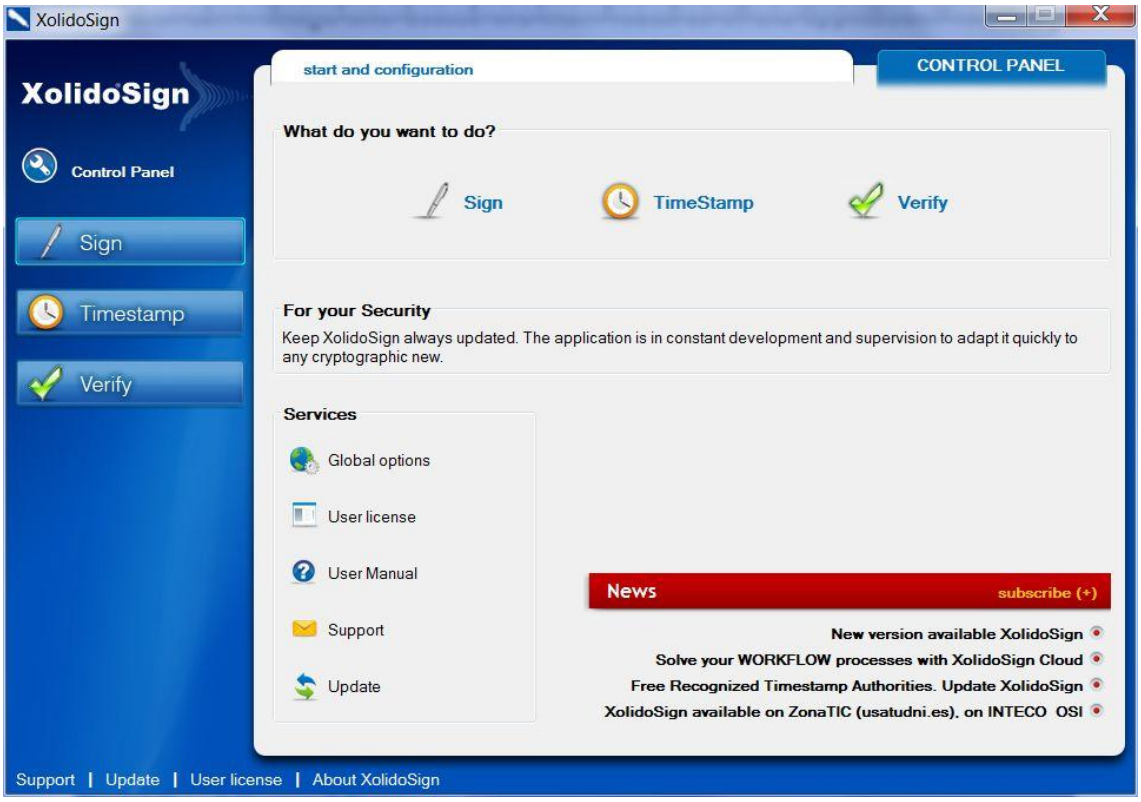

Fig. 1. Xolido®Sign Control Panel.

In the left lateral there are shortcut buttons from which user can access Xolido®Sign options for processing Signatures, Timestamps and Verifications. Users can also access to one of these functionality from the shortcut links in the area framed entitled "What do you want to do?"

Control Panel has a News section for Xolido®Sign, from which the user stays abreast of possible developments or improvements arising in the environment of general cryptographic services and of the application in particular.

In the lower left shows the "Services", from which it has direct access to several generic features of the application.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

Also, at the bottom of the application, are presented several shortcuts for accessing *Support*, *Update*, *User license* and *About Xolido®Sign*, which remain visible all the time, regardless of which functionality is running.

Global Options settings of Xolido®Sign refer to the generic parameters used and are presented below:

- Startup application for Xolido®Sign

This section of the global settings panel you can select the **startup application**. The default value at startup is the Control Panel, but can be set either Sign, Timestamp or Verify options, so that the application will start presenting, at the upcoming executions, the selected functionality interface directly.

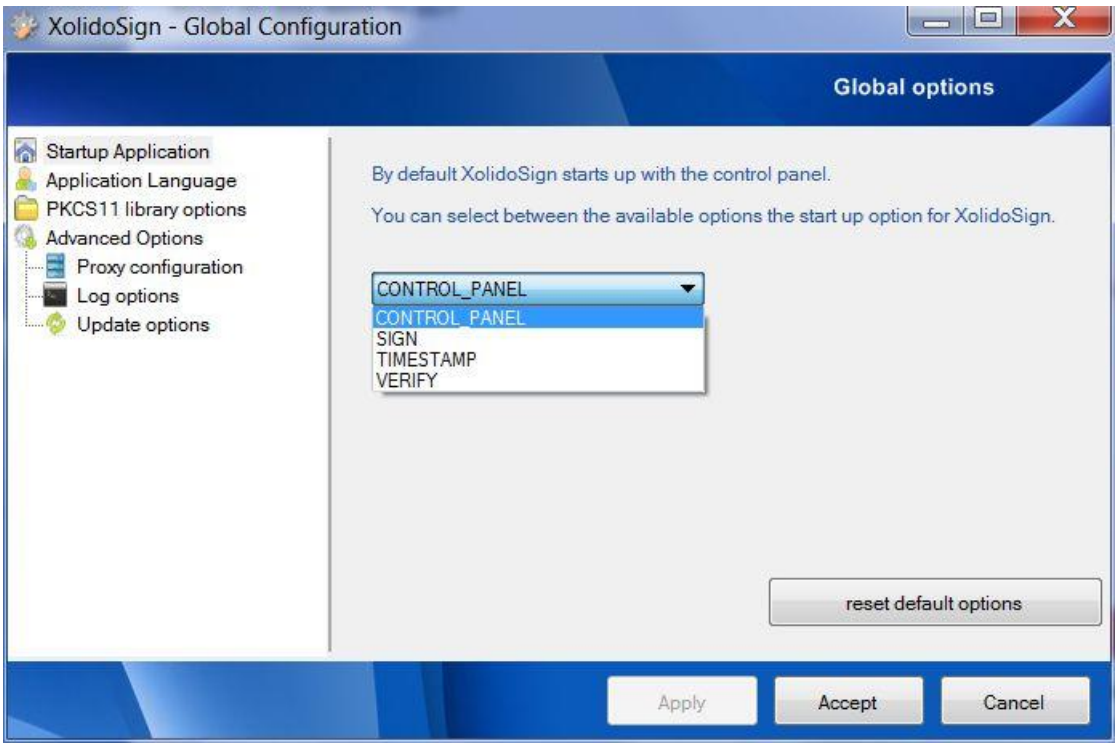

Fig. 2. Startup Configuration menu.

- Application Language options

The application also lets the user the option of selecting the **working language of the application**, by default, it automatically detects the language based on the location declared in the control panel

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

of your computer, however in the application it's possible to predefine the desired language, whose effect occurs after restarting the program.

Fig. 3. Language Configuration menu.

- PKCS11 Library options

Xolido®Sign works by default with the operative system certificate store, based on the CSP driver that every smart card manufacturer deploys for its smart cards.

There is also an option to access electronic certificates located on smart cards through **Pkcs11 libraries**, allowing users to configure a set of libraries and enable this functionality so that Xolido®Sign could access these electronic certificates unattended.

User has to introduce for each library wanted to set up an identifying name and an access path to the library itself, so that Xolido®Sign could invoke it when the use of an electronic certificate is required.

Below is the image for the tab of this configuration option.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

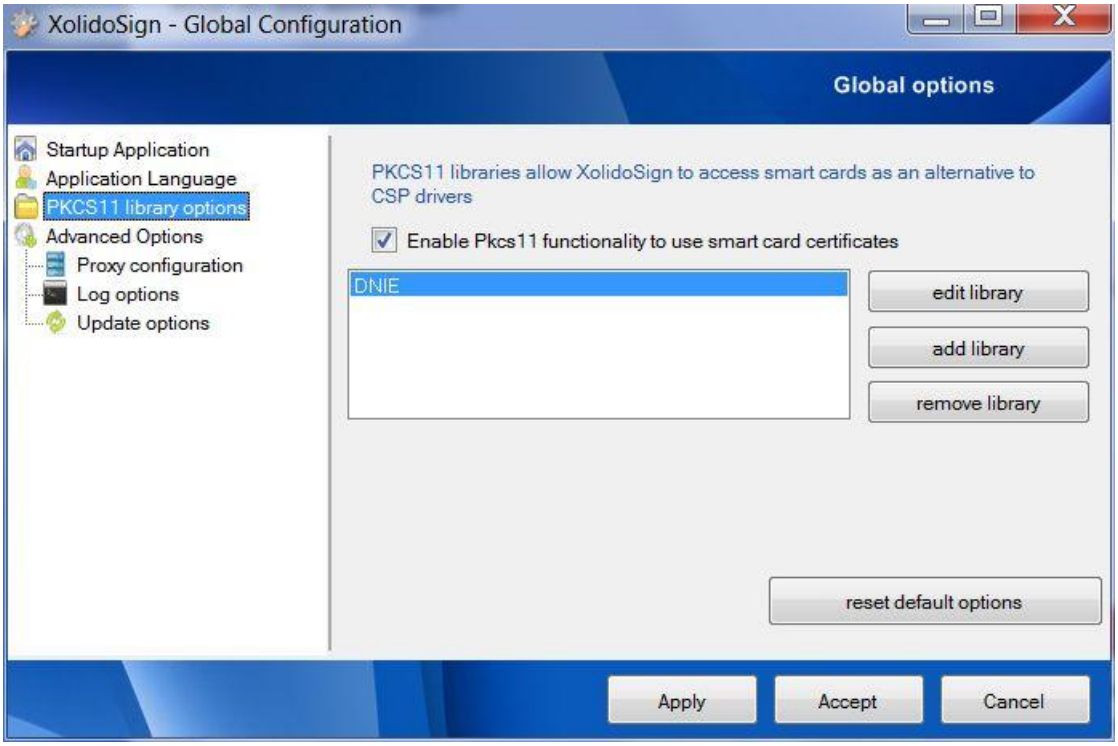

Fig. 4. Pkcs11 options Configuration menu.

- Proxy Configuration

Xolido®Sign includes the functionality to configure **network connections through proxy server**.

First option, by default, the application will connect to the network directly, without intermediate proxy server.

User can also establish Xolido®Sign to use an intermediate server for connections to the network, using as reference the Internet Explorer established configuration for a proxy server, which operative system uses by default.

Also, it is possible for the user to specify a custom proxy configuration, so that Xolido®Sign connects to the network through it.

Next image shows the tab where options to configure proxy server are available.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

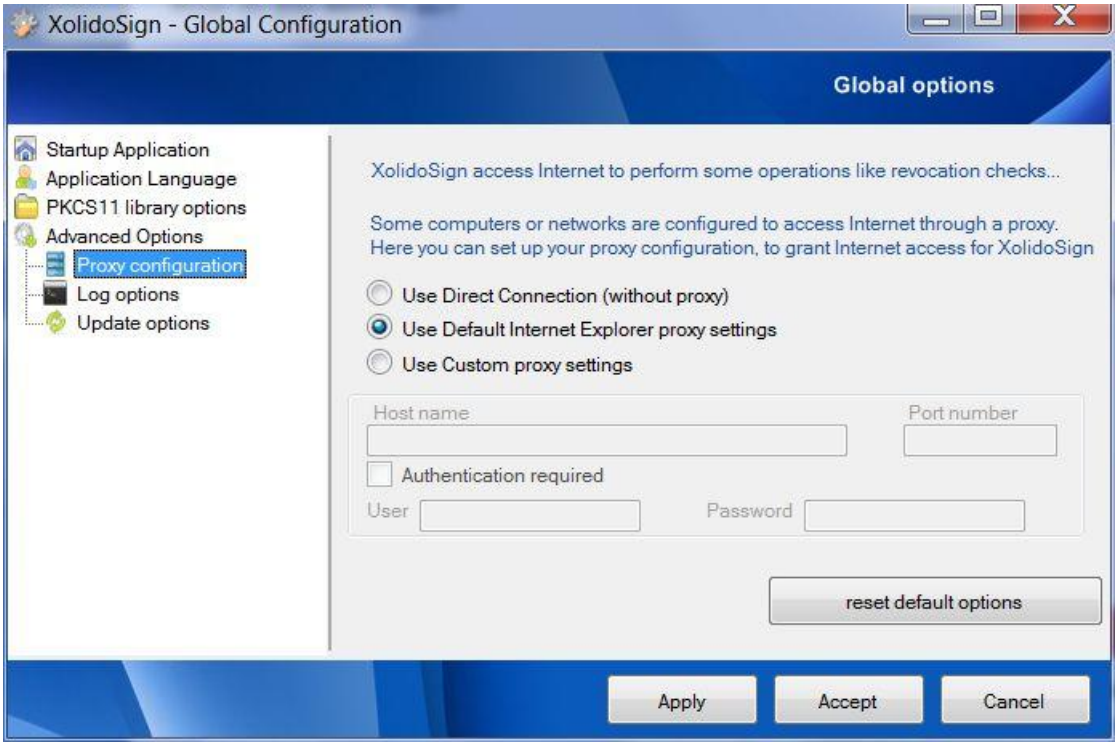

Fig. 5. Proxy Configuration.

- Log configuration options

This panel provides a text box with which users can hand-edit the route set for the **dump Log data**, in case you want to carry out an inspection of incidents during the execution of the application.

In addition, to carry out the dump information in the log file, the option **Enable Log File dump** must be marked and configured.

By default this option is off and so it is recommended to stay.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

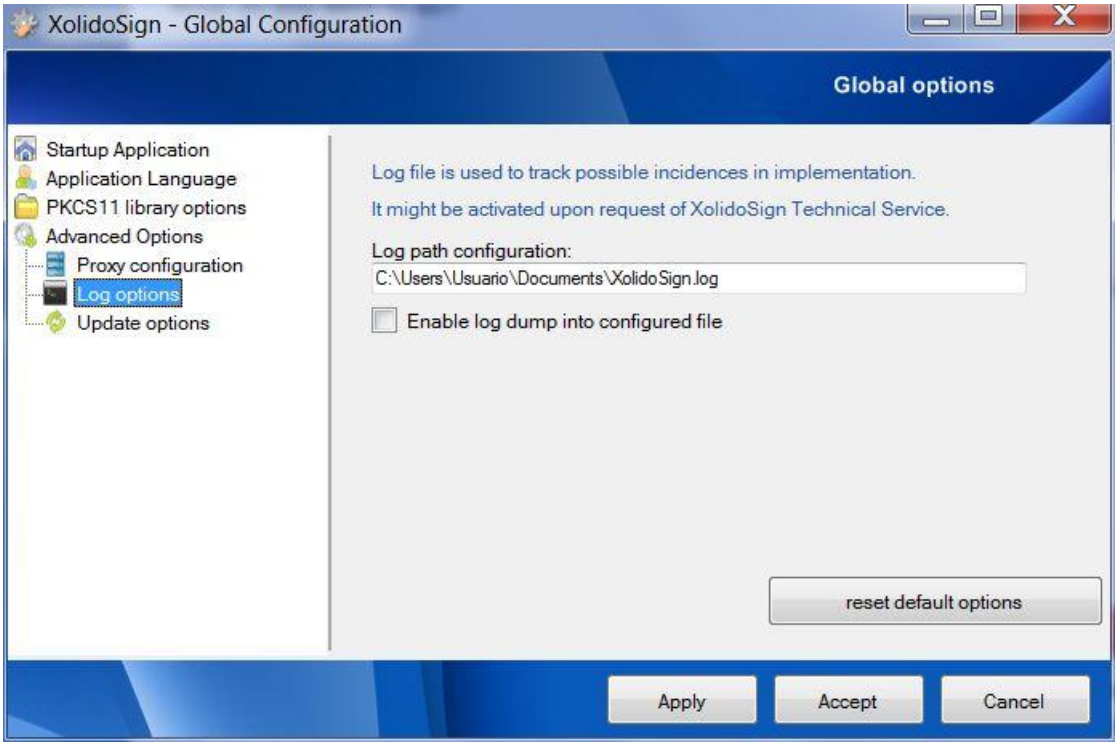

Fig. 6. Log Configuration options.

- Update configuration options

You can also **enable or disable update warnings** that appear at the start of the application. By default this option is enabled, so that users will be notified automatically if there is a new version of Xolido®Sign. It is more than advisable to stay updated about your safety before any new cryptographic algorithm implemented or improved in advanced information including electronic signatures.

There is a button, called **Check for Updates**, with which users could launch a query to online application repository in order to check if there is a new Xolido®Sign version.

Mod.: D201000074v07 20170301

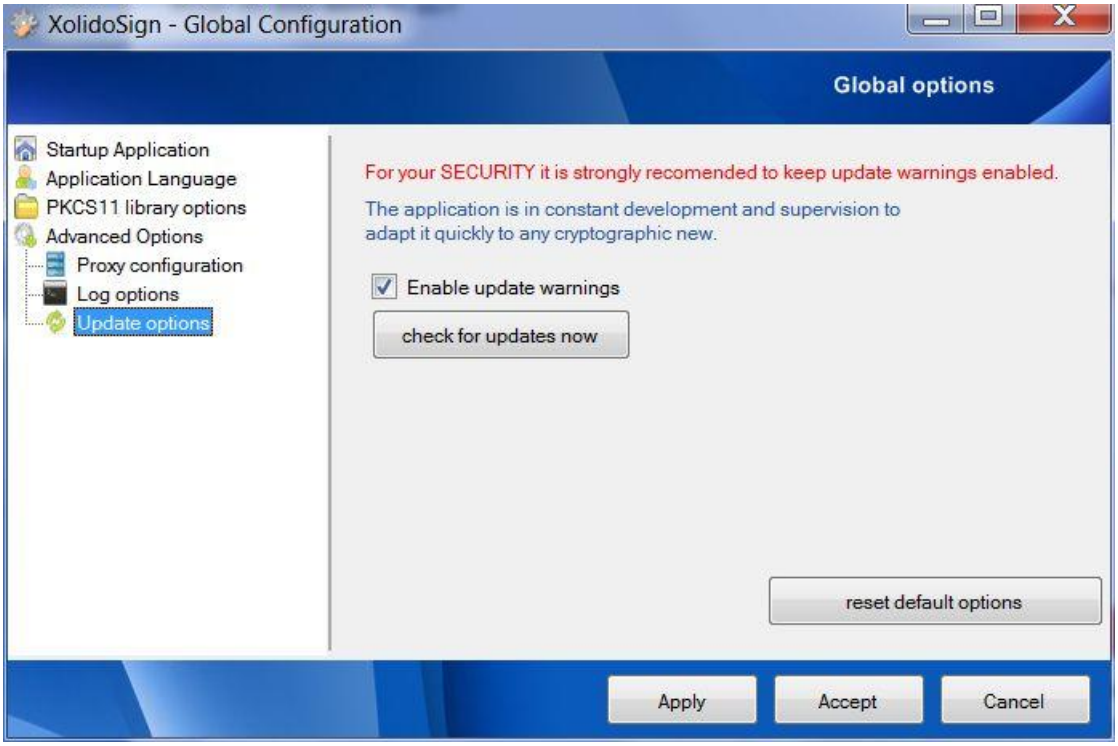

Fig. 7. Updates Configuration options.

Below are explained each of the functionalities of the application, including its usage and if applicable, own configuration options.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

3. Xolido®Sign User Guide - Sign

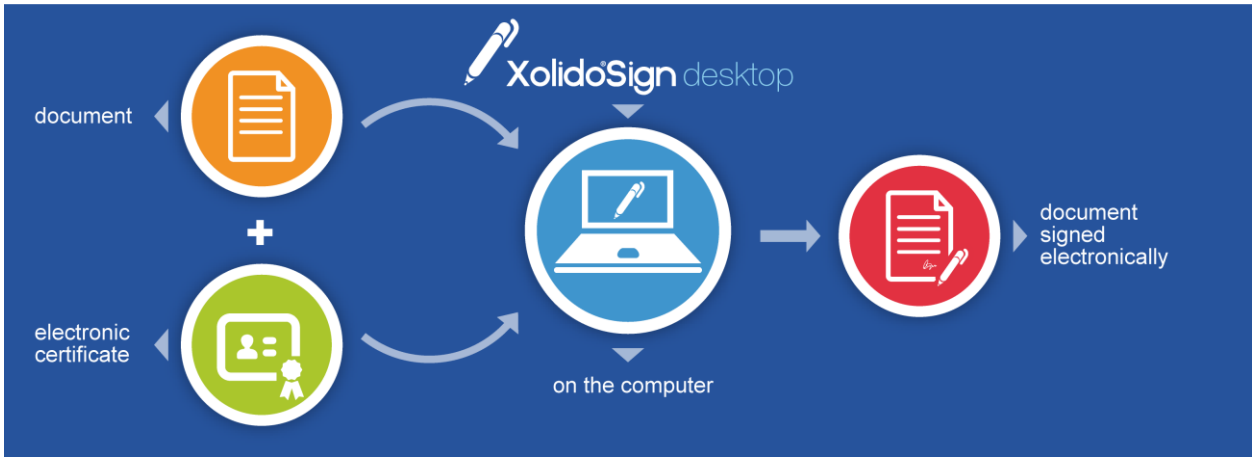

Fig. 8. How to use free Xolido®Sign application to Sign.

Xolido®Sign allows to perform advanced electronic signatures of all the documents you want, ensuring that this documents hold integrity property, has not been amended since it was signed or stamped, and certifying the identity of the author or signer.

Once completed the process of digital signature, signed files will be available in the selected output folder, with their corresponding digital signature files.

If you work with Adobe PDF documents, there is the option of embedding digital signature into the file itself; in that case, no external digital signature file will be created.

Below, there is an image corresponding to main Xolido®Sign – Sign window interface.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

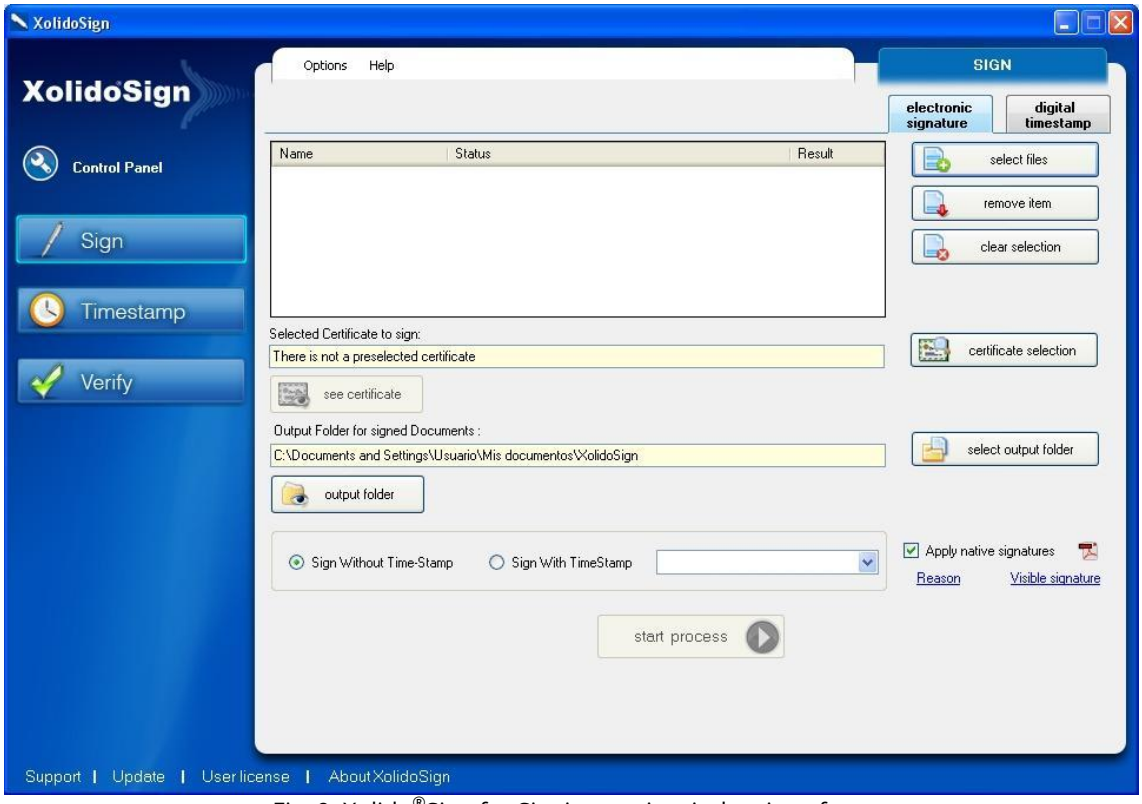

Fig. 9. Xolido®Sign for Signing, main window interface.

Different areas can be appreciated within the application interface, each of which is responsible for conducting small choices that will guide users towards the ultimate goal, which is to perform digital signature and/or timestamp for all accessible documents.

3.1. Document Management Area

In the user interface is first presented a block of three options regarding the document management of files accessible by the user, either on your own computer or local network.

First option (**select files**) leads the user to a Windows dialog box to complete the selection of all the files wanted to be included in the digital signature or time stamping process.

File selection can be multiple so that the application reports a significant time saving for the user who needs to sign a large number of documents. For this multiple file selection you must press *Ctrl* on your keyboard and then select all the files you want to operate with.

After selecting the files you wish to sign or stamp, the application will show a table with the data of the **Name**, **Status** and **Result** of each one.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

State and Results properties refer to the situation in every moment of waiting to the launch of the operation, success in the operation...for every document selected.

Second option (**remove item**) allows you to delete from the list those selected documents that you do not want to sign or stamp, and third option (**clear selection**) allows you to quickly delete all documents in the selection.

Below is the image with representing this area of document management in the course of an operation of Digital Signature or Stamp.

Fig. 10. Document Management Area during operation.

3.2. Electronic Certificate Management Area

To perform the digital signature operation is necessary to hold an electronic certificate, and therefore the application has to fill in the correct selection of the same within a "certificate repository", which in this case, to facilitate the work to the user, it is the Windows Certificate Store.

There are also supported external certificates in what is known as smart cards or cryptographic cards.

Connecting correctly the card reading device and with the correct drivers, Windows will detected it and include all certificates into its certificate store, so that electronic certificates can be used easily with Xolido®Sign .

Application interface provides the **Certificate Selection** button to present a list of available electronic certificates so that user can choose the one desired at any time to perform the digital signature of the selected documents.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

Xolido®Sign performs the necessary checks to determine the parameters of validation of the certificate, date of start and end of their period of validity, correct structure of the certificate, checks about its revocation status...

If the application finds that chosen certificate is not totally reliable, show a warning, and in any case user is allowed, by its own risk, to continue with the signing process if desired.

In addition, interface displays a brief data for the selected certificate in order to easily recognize the certificate you are working.

If the user wants to analyse in detail the chosen electronic certificate, he can click on the **View Certificate** option, and Xolido®Sign will display a window with all the data on it.

Below is an image with the snippet corresponding to that certificate selection area.

Fig. 11. Electronic Certificate Management Area.

3.3. Output Folder Management Area

Next block of options allows the user to set the output folder in which application will save the documents and signatures or stamps associated.

Xolido®Sign is configured by default to set as an output folder a path within the Documents directory for the user, however, user are allowed to change this selection, to perform that you must click on **Select Output Folder** and proceed to indicate the desired folder to save the results of the signature and / or time stamp operation.

The **See Output Folder** option will display the contents of that folder through Windows explorer.

Below is the snippet of the interface that corresponds to the management zone for output folder.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

Fig. 12. Output Folder Management Area.

3.4. Operating Options Management Area

In this interface section of users can configure the operation option desired for the selected files.

There are different possibilities, which are detailed below:

- **Sign Without Time-Stamp**

Operation is conducted without embed within the digital signature a timestamp for the time that this signature is carried out.

- **Sign with Time-Stamp**

Selecting this option, the digital signature will embed a digital mark with the date and time for the moment that the signature operation has been made.
That is useful to validate the digital signature from a time instant validated by its time stamp.

- **Apply Native PDF Signatures**

When selecting an option for digitally signing documents it's available the ability to operate differently with Adobe PDF documents.

In this king of documents, digital signature can be embedded in the document itself, so that Xolido®Sign won't include in the output folder a separate file for the signature. Instead, application will include only one PDF document, with the same name that the selected one, but with the digital signature correctly embedded.

Thus, any third party who has the free PDF viewer from Adobe (**Adobe Reader**), can receive and verify the PDF correctly signed and analyse both the identity of the signer and the moment has been signed and the Time Stamp Authority endorsing the timestamp (if the option of Sign With Time-Stamp has been marked).

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

One of the many advantages of Xolido®Sign lies in the possibility of performing embedded signatures of multiple PDF documents completely unattended, with a single click and total flexibility, all absolutely free.

Below is an image with the interface area related to the selection of operating options that have just been explained.

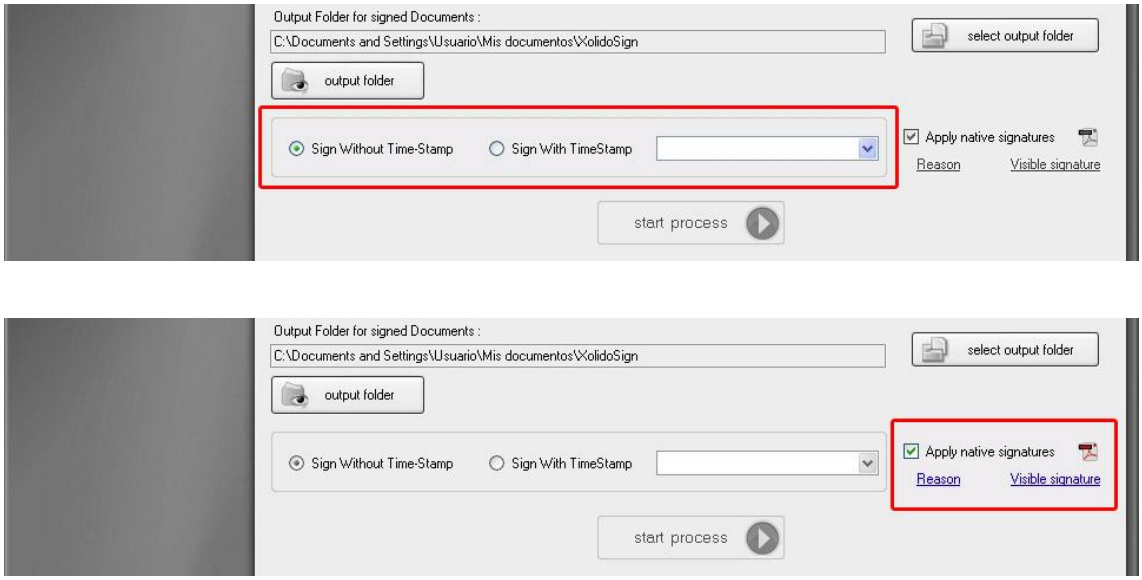

Fig. 13. Operating Options Management Area.

3.5. Start Operation Area

When all the above steps are completed, you can begin the digital signatures and / or time stamping operations for all selected documents, just clicking on **start process** button in a simple and automatic way.

Below is an image with this last section of the application interface.

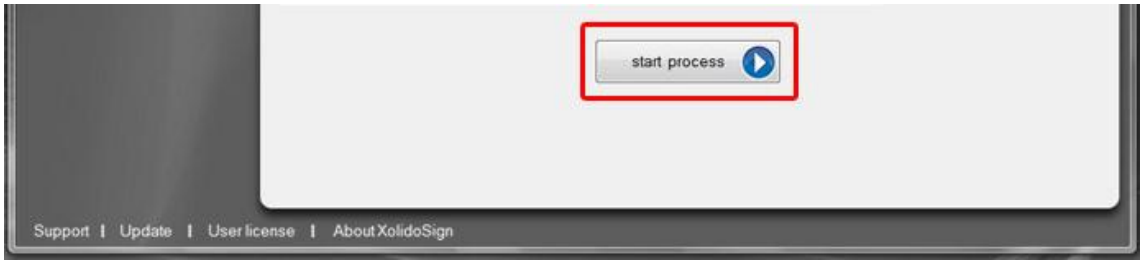

Fig. 14. Start Operation Area.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

4. Xolido®Sign User Guide - Timestamp

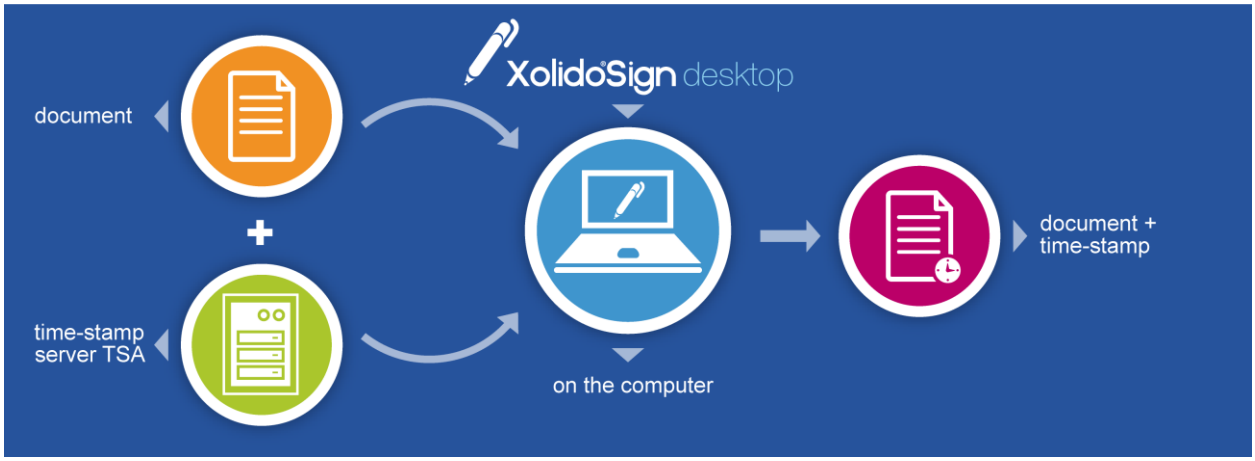

Fig. 15. How to use Xolido®Sign for digital timestamping.

Xolido®Sign allows you to timestamp all your documents and files, so there is a warranty of their existence in a given date, and ensuring that documents and files satisfy integrity property, that is, they have not been modified since their time stamping.

Once completed the process of digital time stamping, documents will be available in the selected output folder, with their corresponding digital timestamps files.

Below, there is an image corresponding to main Xolido®Sign – Timestamp window interface.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

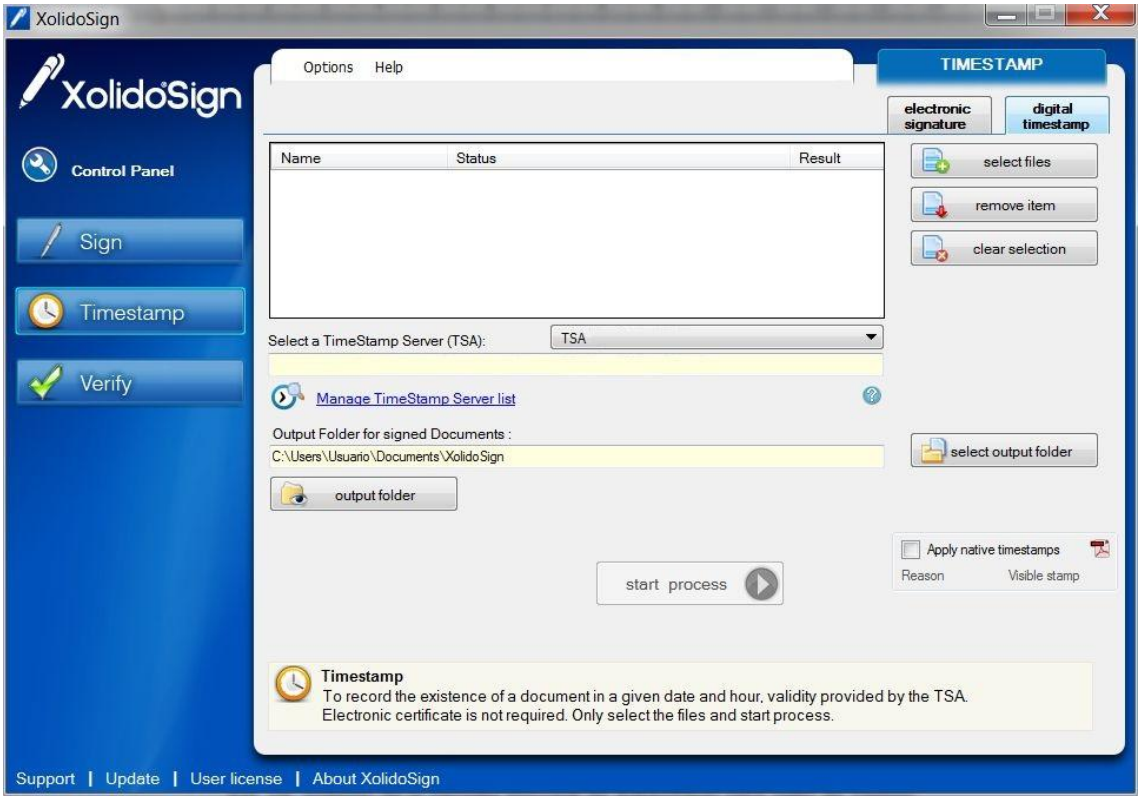

Fig. 16. Xolido®Sign main interface for Timestamp.

4.1. Document Management Area

In the user interface is first presented a block of three options regarding the document management of files accessible by the user, either on your own computer or local network.

First option (**select files**) leads the user to a Windows dialog box to complete the selection of all the files wanted to be included in the digital signature or time stamping process.

File selection can be multiple so that the application reports a significant time saving for the user who needs to sign a large number of documents. For this multiple file selection you must press *Ctrl* on your keyboard and then select all the files you want to operate with.

After selecting the files you wish to sign or stamp, the application will show a table with the data of the **Name**, **Status** and **Result** of each one.

State and Results properties refer to the situation in every moment of waiting to the init of the operation, success in the operation...for every document selected.

Second option (**remove item**) allows you to delete from the list those selected documents that you do not want to sign or stamp, and third option (**clear selection**) allows you to quickly delete all documents in the selection.

Below is the image with representing this area of document management in the course of an operation of Digital Signature or Stamp.

Interface for this operation area is the same as in the Sign functionality.

4.2. Timestamp Server Management Area

Next interface area shows a drop down list box with the identifying name of all those authorities of time stamping (TSA) which have been configured in Xolido®Sign.

User can select the timestamp authority server with which he desires to perform time stamping for all the documents selected in the previous step.

There is also a text box with a brief description of the TSA selected, including the URL of the server if appropriate.

It also appears a **link to access to the manage timestamp server section** in the configuration menu.

Next image shows the corresponding section explained.

Fig. 17. Timestamp Server Management Area.

4.3. Output Folder Management Area

Next block of options allows the user to set the output folder in which application will save the documents and signatures or stamps associated.

Xolido®Sign is configured by default to set as an output folder a path within the Documents directory for the user, however, user are allowed to change this selection, to perform that you must click on **Select Output Folder** and proceed to indicate the desired folder to save the results of the signature and / or time stamp operation.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

The **See Output Folder** option will display the contents of that folder through Windows explorer.

Below is the snippet of the interface that corresponds to the management zone for output folder.

Fig. 18. Output Folder Management Area.

4.4. Operation Options Area

Next block shows the option for the operation to allow the specific process of timestamping PDF documents.

Fig. 19. Operation Options Area.

- **Apply native timestamps into PDF**

With Xolido®Sign it is posible to choose the option to insert the timestamp within the PDF document structure.

In this king of documents, digital timestamp can be directly embedded in the document itself, so that Xolido®Sign won't include in the output folder a separate file for the timestamp. Instead, application will include only one PDF document, with the same name that the selected one, but with the digital timestamp correctly embedded.

Thus, any third party who has the free PDF viewer from Adobe (**Adobe Reader 10 or later**), can receive and verify the PDF correctly timestamped and analyse the moment when it has been stamped.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

4.5. Start operation Area

When all the above steps are completed, you can begin the digital signatures and / or time stamping operations for all selected documents, just clicking on **start process** button in a simple and automatic way.

Below is an image with this last section of the application interface.

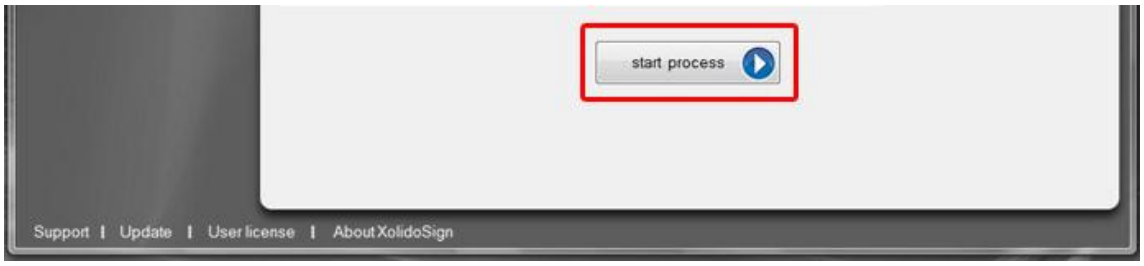

Fig. 20. Start Operation Area.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

5. Configuration Guide for Xolido®Sign – Sign / Timestamp

This section will present the different configuration options supported by the application for the functionalities of Sign and Timestamp.

The configuration menu options are designed to further streamline the operation and the steps to complete the signing of documents and the digital time stamping of files and documents.

Below is a picture to see graphically the way to access the configuration menu of Xolido®Sign. It can be also acceded by pressing *F5* key on your keyboard.

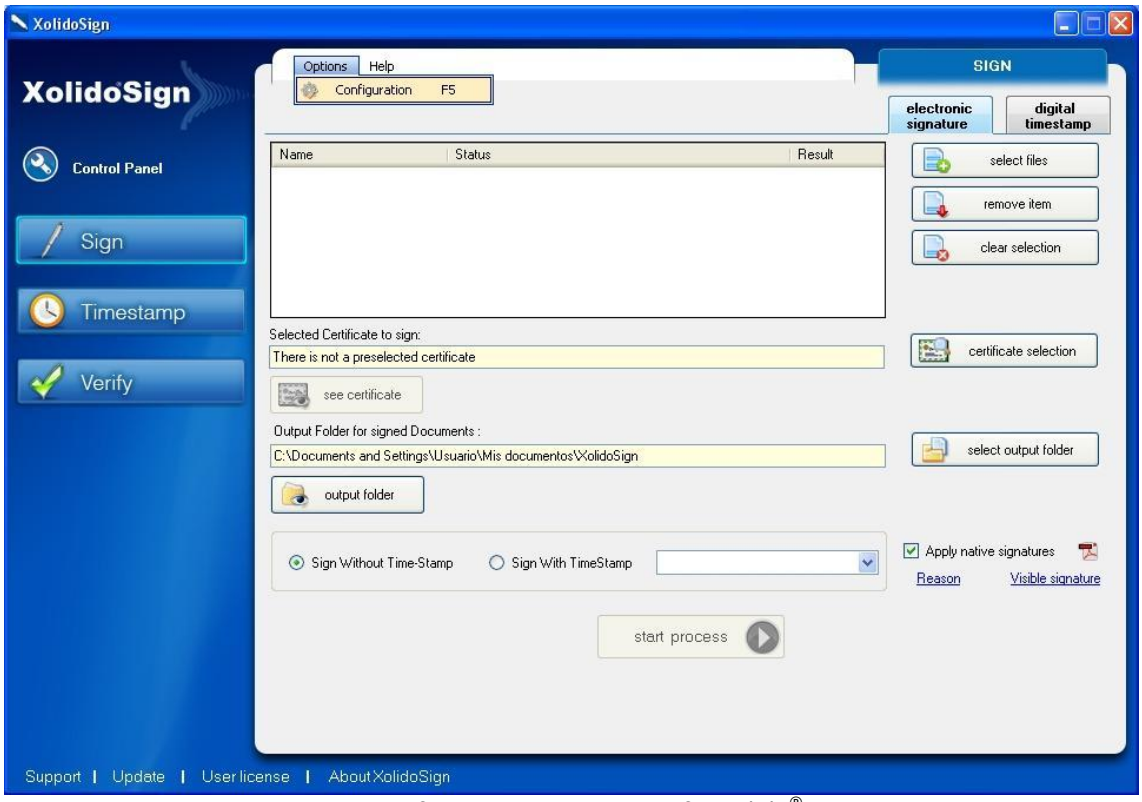

Fig. 21. Configuration menu access for Xolido®Sign.

Configuration menu is divided into different tabs, each of which associated with different configurable concepts within the application, in order to make it as intuitive as possible for the user.

5.1. Certificate Options Area

The first group of settings concerns the most basic options relating to electronic certificate options.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

5.1.1 – Certificate selection

In this section you can set the default certificate used by Xolido®Sign. By clicking on the **configure default certificate** button the user is prompted to choose one of the available electronic certificates.

If the selection is successfully completed, the certificate is presented from now as the default preselected certificate and there will be shortlisted to carry out the selection step if you want to work with this preconfigured certificate, thereby saving Xolido®Sign users this procedure step.

The panel also showed a brief description of the pre-selected certificate, if any, and you can also analyse in detail the certificate by clicking **view configured certificate** option.

The image below shows this first options panel.

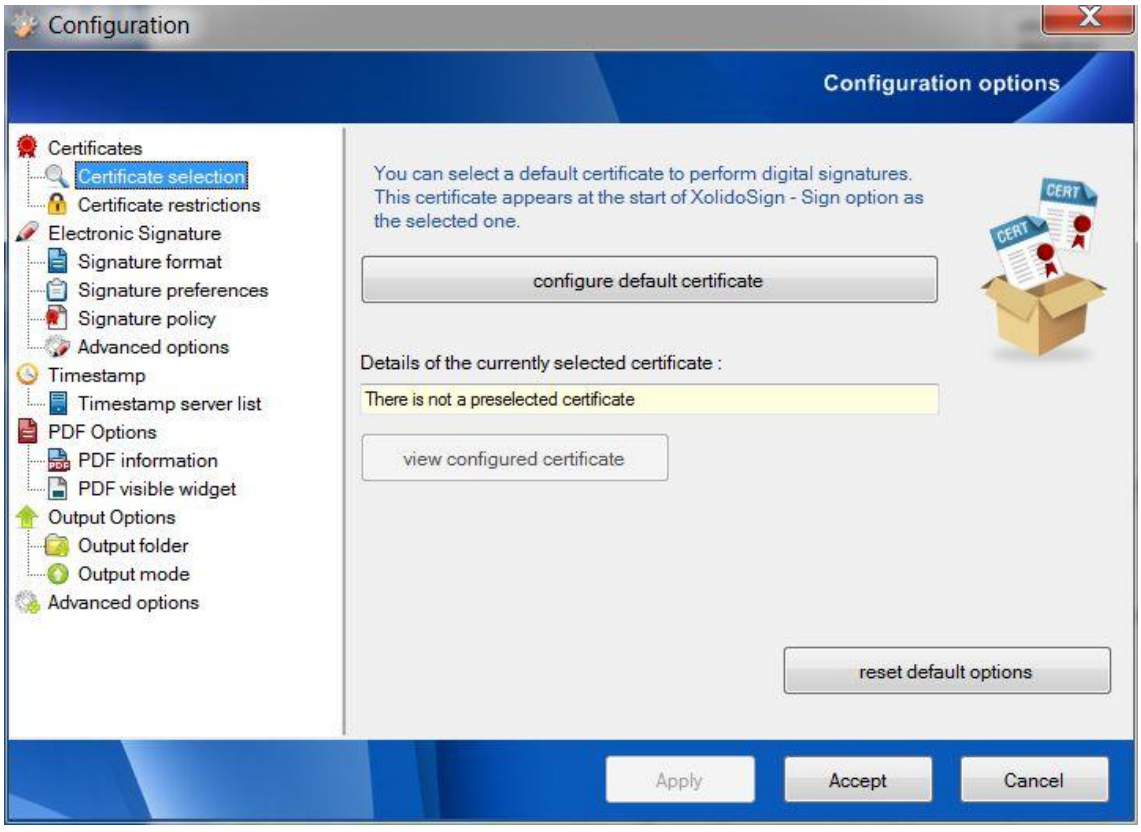

Fig. 22. Certificate selection panel.

5.1.2 – Certificate restrictions

In this second panel, you could configure the restrictions to be applied, by Xolido®Sign, when selecting a certificate.

Users could configure Xolido®Sign so that it only uses **not revoked** certificates, **not expired** certificates, and only exclusively certificates **with digital signature purpose**, by checking the corresponding boxes.

By default, the application performs an online verification of revocation status of certificates by connecting to the relevant certifying authorities.

A user may wish to omit these online checks, for example by being in a computer that temporarily has no Internet connection. To do this you must deselect the option **Check Online Revocation Status for Selected Certificates**.

With the option **Check Online Status of the certificate when Xolido®Sign starts**, the user can ensure that the application verifies the validity of the Preselected Certificate each time he runs the application.

In addition, the application makes a new query to certificate authorities to obtain the values of certificate revocation status, if mechanism available for that certificate, just before starting the process of electronic signature, storing this information internally and updating it through a new petition once the period of validity of ***internal revocation cache*** ends, the user can define with the appropriate field, as shown in the image, this time validity of the internal cache.

In any case, the changes are reversible and users can return to the default signature options by simply clicking on the **reset default options** button.

The image below shows this second options panel.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

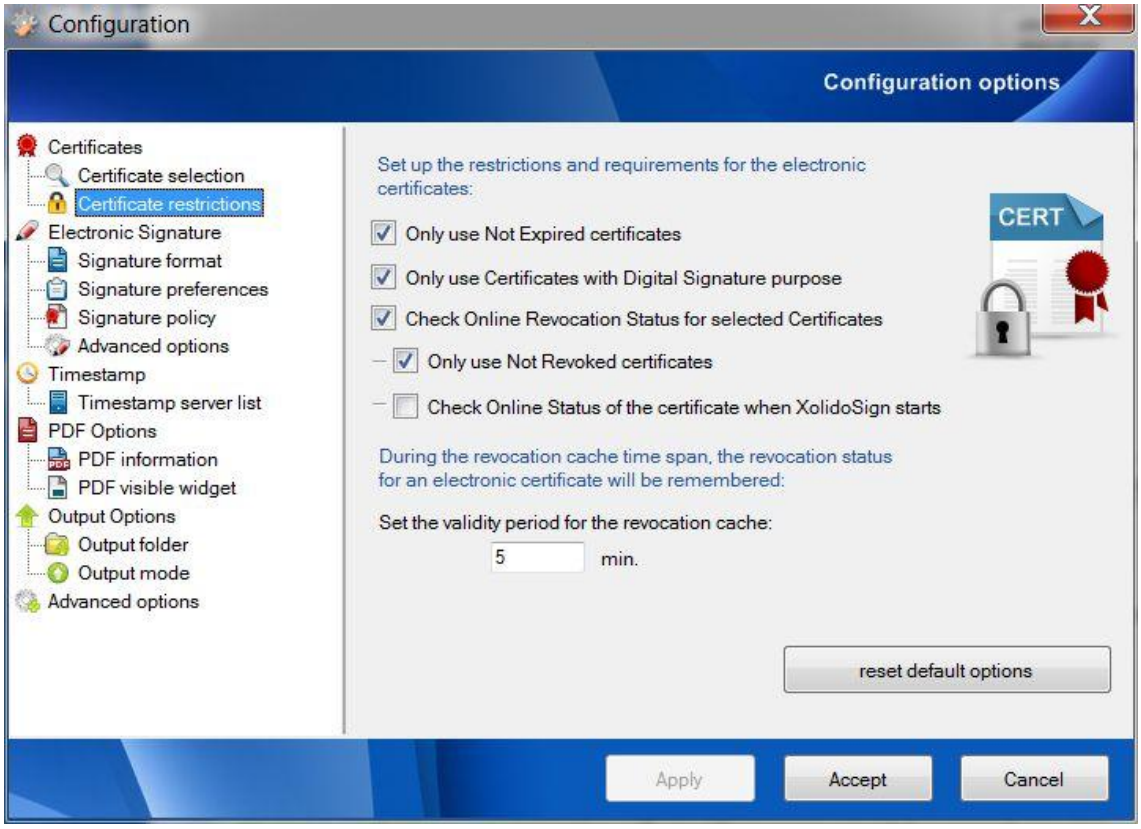

Fig. 23. Certificate restrictions.

5.2. Signature Options Area

This section of the configuration panel is responsible for managing the options and settings that involve a change in the type of electronic signature performed by the application.

5.2.1 – Signature format

First the user can select one of the operating modes available:

- **Perform basic signatures (Profile –BES; e.g. CMS / CAdES-BES)**

  With this option the user will perform basic signatures which are valid according to the basic electronic signatures standard (For example: RFC. 3852 - Cryptographic Message Syntax (CMS)) of the IETF.

- **Perform signatures with revocation references. (Profile –C; e.g. CAdES-C)**

  With this option the application adds to its electronic signatures a reference to that certificates used in the operation, as an unsigned attribute, and references to that values obtained for revocation status of the certificates implied in the process, also as an unsigned attribute,

following the IETF standard (RFC. 5126 - CMS Advanced Electronic Signatures) and the ETSI recommendation for advanced electronic signatures (ETSI TS 101 733).

- **Perform full extended signatures with revocation values. (Profile –XL; e.g. CAdES-XL)**

If the application operates in this mode of electronic signature, in addition to the references of the certificates and revocation values that were added in the previous choice (CAdES-C), they will include the values itself of those certificates employed within the process and the revocation objects for each one of the certificates involved in the electronic signature.
This information will be added as an unsigned attribute, in compliance with the directives contained in the standard IETF (RFC. 5126 - CMS Advanced Electronic Signatures) and the ETSI recommendation for advanced electronic signatures (ETSI TS 101 733).

For electronic signatures embedded in PDF, the information of the underlying certificates and revocation values is added according to the reference provided by Adobe in *PDF Reference 1.6* and higher.

With these electronic signatures reliability is achieved through advanced electronic signature files generated by the application.

Below is an image with the configuration panel relating to these options.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

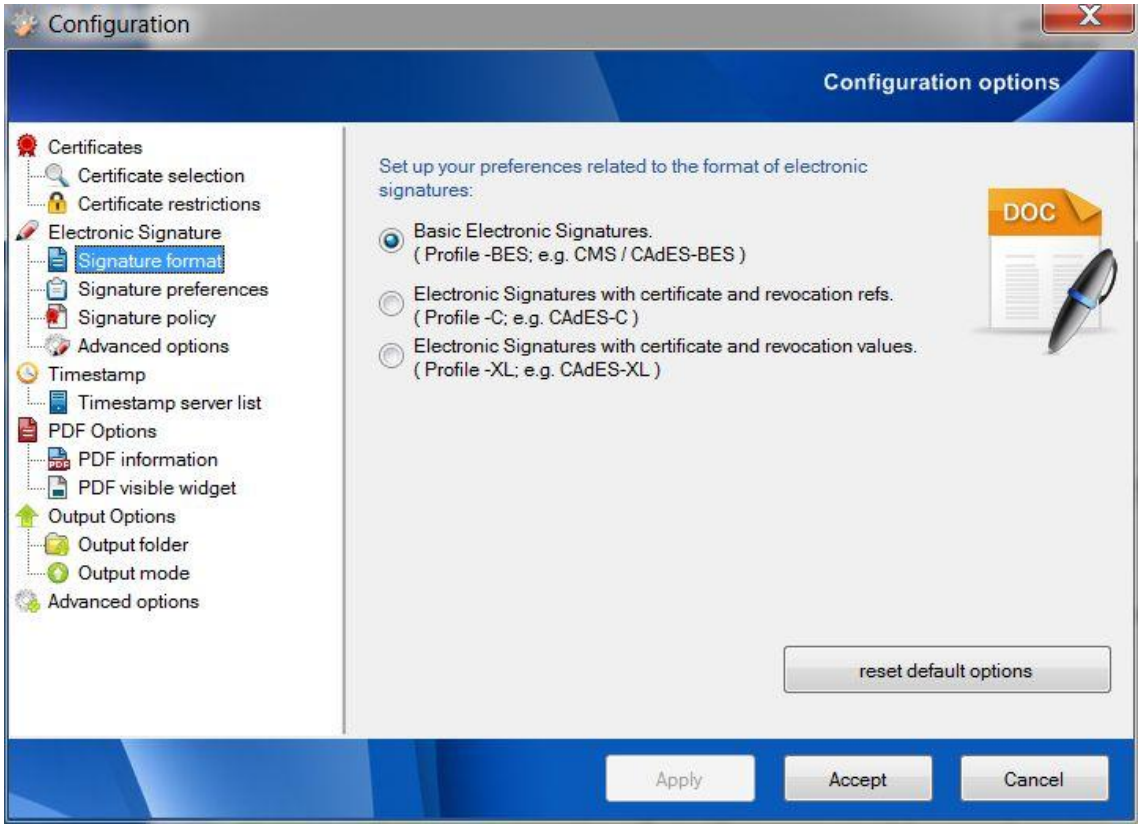

Fig. 24. Signature format.

5.2.2 – Signature preferences

In this second panel, users can configure other options for the signing processes.

In this panel users can mark **Auto detect PDF and perform embedded PDF signatures**, whereby the application Xolido®Sign, automatically detects PDF documents within the selected list to sign and proceeds to perform with them the embedded signature in the document itself. This option preselects the alternative of *Apply native PDF Signature* available on the main interface of Xolido®Sign.

By default, it follows the PAdES-CMS compatibility profile, with the specifications added by Adobe on the Adobe PDF Reference document, relating to the references and values for revocation information.

It also includes the possibility of performing the embedded **signatures according to PAdES-BES profile**; nevertheless it isn't enabled by default because only Adobe Reader X and later versions are prepared to this compatibility.

The option **Add Timestamp to Electronic Signatures** involves a pre selection for the operation mode *Signature with TimeStamp* on main interface of Xolido®Sign.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

Performing this option, a request to time stamp server is done for the moment when digital signatures are made. If the request was successful digital signatures resultant will have a timestamp ensuring its existence at a given time.

Xolido®Sign also leaves the possibility (enabled by default) that users choose to remove digital signatures if the application was not be able to complete connection to time stamp server, if the option *Sign with TimeStamp* is chosen. This option corresponds to the tag **Cancel Signature process if required Timestamp is not available**.

The effect of this option is not to proceed to complete the digital signing operation in case of not being able to get a time stamp from the Time Stamp Server configured for embedding time stamps into digital signatures.

When this option is not selected and operation option is *Sign with TimeStamp*, in case of unavailability of time-stamp service, it will be notified that the operation was completed successfully but does the signature does not include any time-stamp.

The application also adds the option **Cancel Signature if selected certificate has access methods for revocation info but fails obtaining data**.
In this situation, the application cancels the operation of electronic signature warning users if you cannot get the revocation information (CRL or OCSP).
This option has no effect when the certificates involved in the signature process do not have a revocation status service or when users are operating with basic digital signatures, PKCS7/CMS, for which the standard does not contemplate the possibility of including certificate revocation values.

It includes the possibility to check ***Auto detect PDF and perform PDF embedded TimeStamps***, which pre-sets the functionality of inserting the timestamps within the PDF structure natively. This functionality is only supported in Adobe Reader version 10 and later.

In any case, the changes are reversible and users can return to the default signature options by simply clicking on the **reset default options** button.

Below is an image of this configuration panel:

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

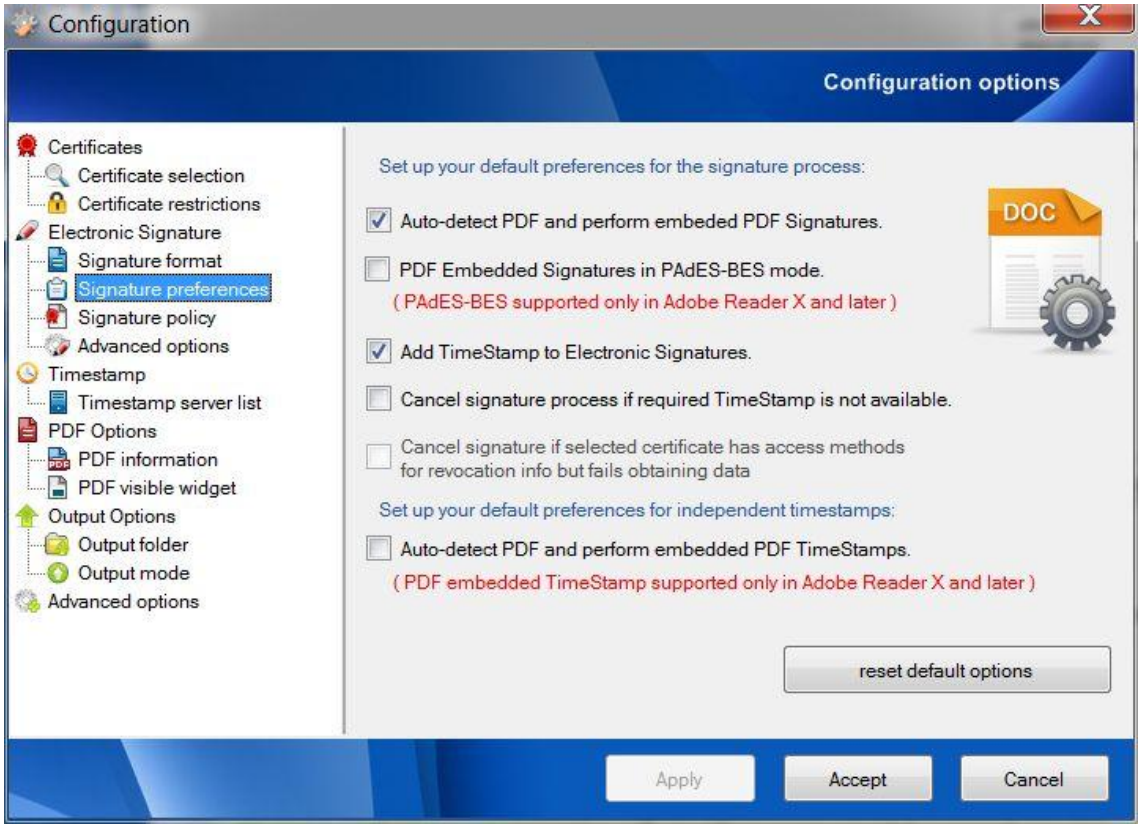

Fig. 25. Signature preferences.

5.2.3 – Signature policy

This options block allows stablishing the desired values referring to signer's commitment and/or a defined signature policy.

Firstly, there are options to select the commitment acquired by the signer for the electronic signatures.

With its use, the signer explicitly indicates to a verifier that by signing the data, it illustrates a type of on behalf of the signer himself.

The set of commitments among which the signer can select the desired to apply to his process of electronic signatures:

- *Origin*

The signer recognizes to have created, approved, and sent the message.

- *Receipt*

The signer recognizes to have received the content of the message.

- *Delivery*

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

The TSP providing that indication has delivered a message in a local store accessible to the recipient of the message.

- *Sender*

The entity providing that indication has sent the message (but not necessarily created it).

- *Approval*

The signer has approved the content of the message.

- *Creation*

The signer has created the message (but not necessarily approved, nor sent it).

To add the commitment to signatures, this option needs to be checked: ***Insert signer's commitment in electronic signatures***.

In the next group of values, there are fields that allow defining specific values to indicate an electronic signature policy followed by the signer.

The values of this information are: an identifier of the policy (in a valid OID format), an URI which indicates the location where it is available the data defining the terms of the policy, the hash algorithm used and its corresponding value in a Base64 string format.

To add the information of the signature policy, it's required to check the option ***Insert policy values in electronic signatures***.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

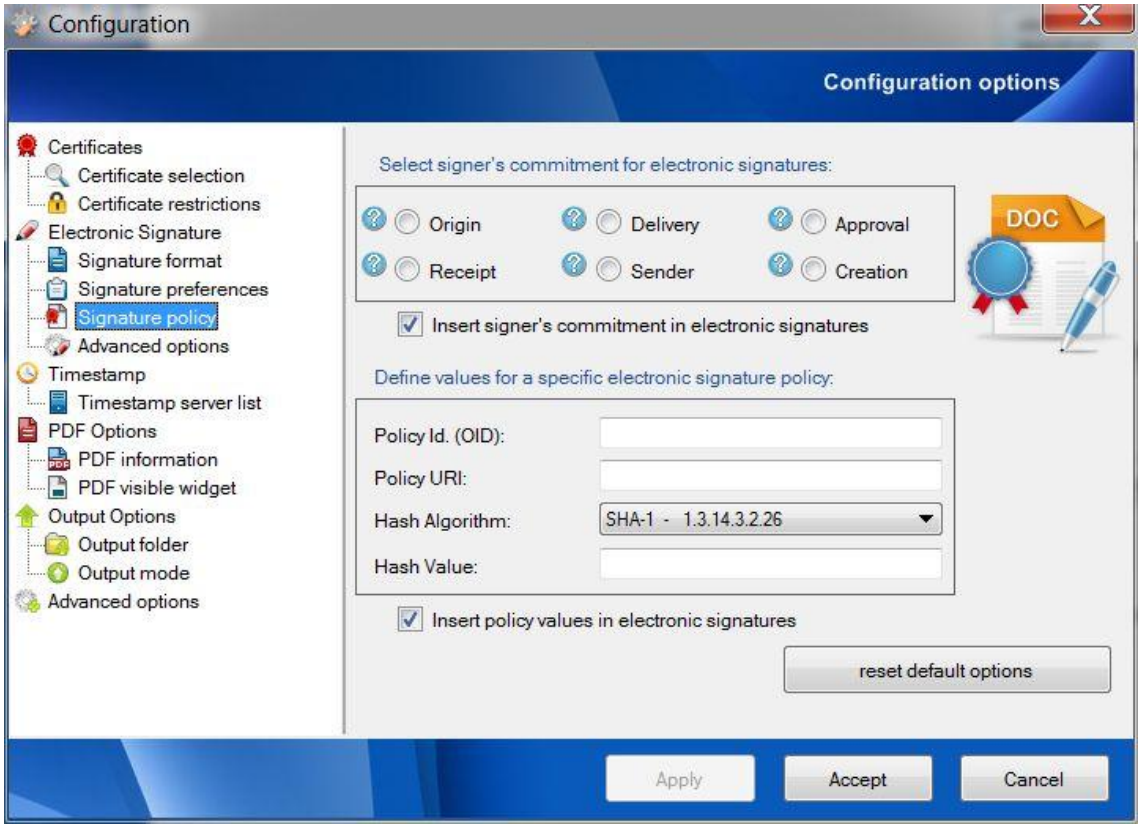

Fig. 26. Signature policy options.

5.2.4 – Advanced options of electronic signature

Next configuration options group is related to some advanced options in the signature processes, such as hash algorithm to use by default (SHA1 nowadays).

There are also two options to set the behavior of the application with PDF embedded signatures, which can be used to achieve compatibility with some PDF reader applications that give special treatment to embedded signatures.

Next image shows this configuration panel.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

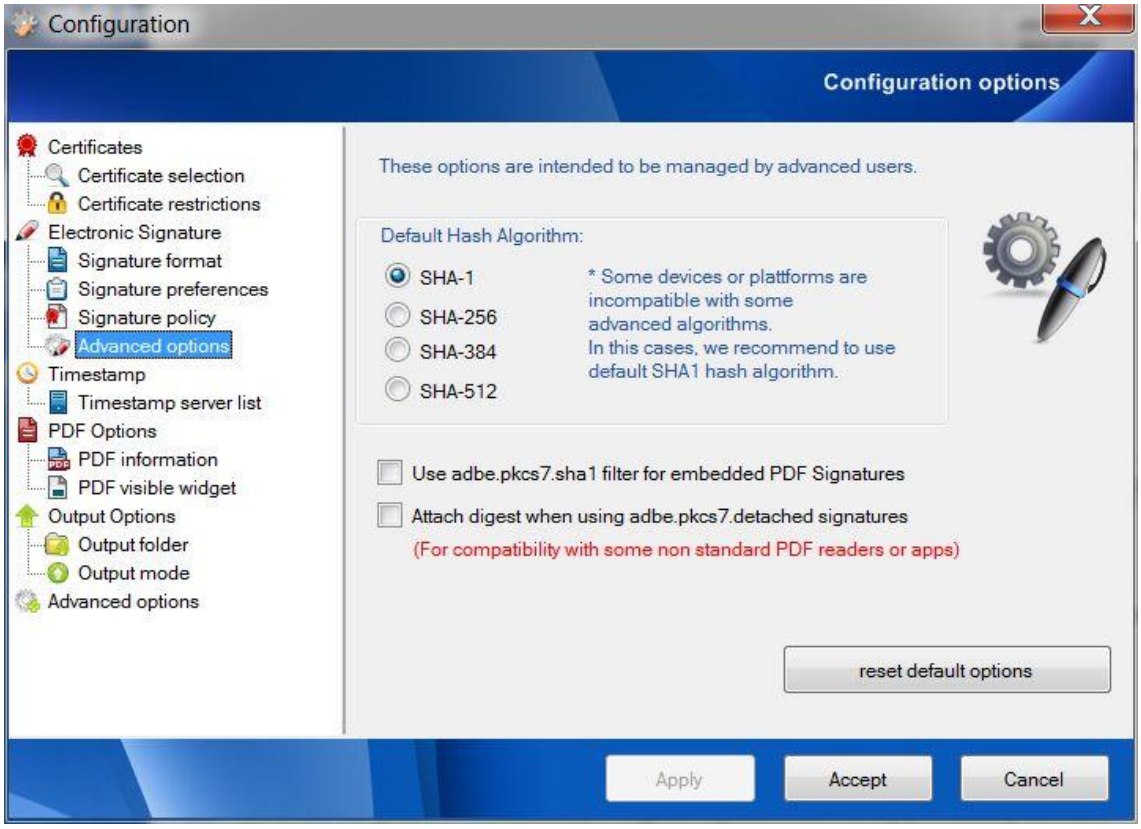

Fig. 27. Signature Advanced options.

5.3. TimeStamp Server Area

Next configuration tab is related to TimeStamp Server list used by the application to obtain external timestamps associated to some file or document, and for timestamps included in the electronic signatures when the option *Sign with TimeStamp* is selected.

5.3.1 – Timestamp server list

Digital Timesting allows you to secure the existence of a document or an electronic signature in a given date. Security here refers to the fact that anybody, even the author or owner of the document or signature is enabled to modify it, provided the integrity of the TimeStamp Authority.

Next image shows the tab corresponding to this option.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

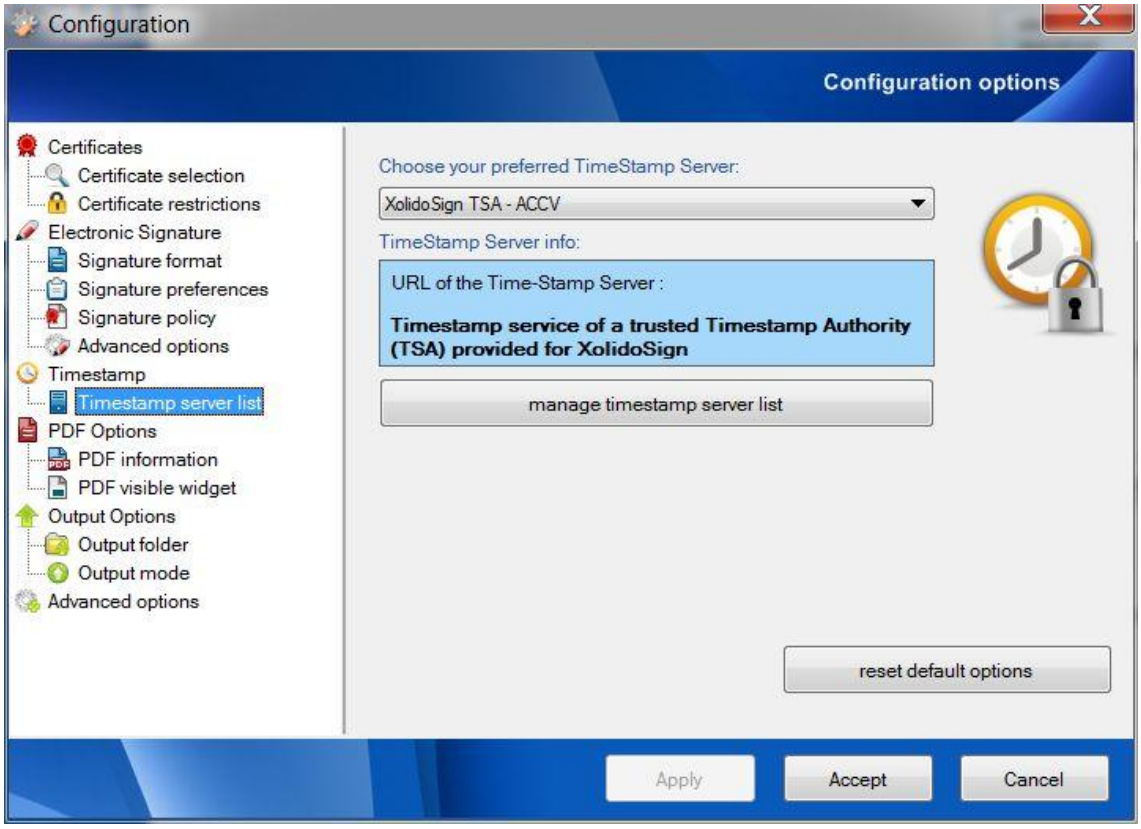

Fig. 28. TimeStamp Server.

With the option *manage timestamp server list*, it's possible to **manage an array of several timestamp server authorities (TSA)** available for the application.

For each one of the elements users could establish an **access URL to the time stamp server**, as also the **user id and password** if authentication is required.

Each server included in the list must have an **identifier name**, so that Xolido®Sign users could select them in an intuitive way, through drop down list boxes.

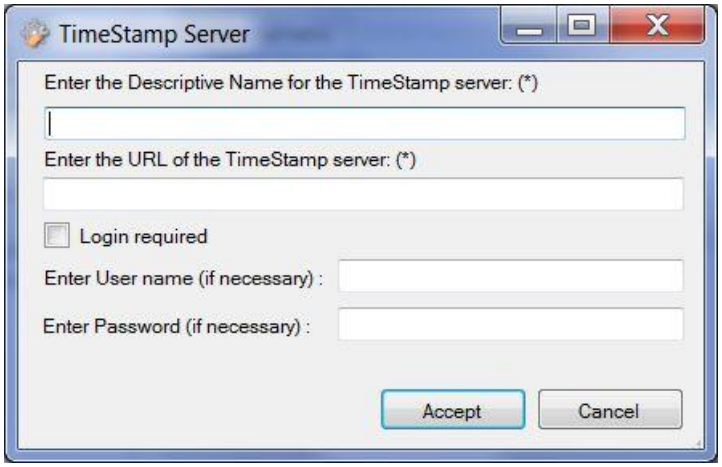

Fig. 29. Inserting a new Timestamp server.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

Xolido®Sign users can configure as predefined the timestamp server desired, provided that it has a valid URL.

If user selects to **reset default options**, all the options added by the user will be reverted, and only shown the timestamps servers included in Xolido®Sign.

5.4. PDF Options Area

The following is the configuration group for PDF document signatures.

5.4.1 – PDF Signature information

In this panel you can edit two text fields whose contents appear in the information regarding the signatures embedded in the PDF document itself.

These are the fields **Reason** and **Location** of signatures, the first is used to indicate why that the document is to be signed (approval, review, close of the document ...) and the second refers to geographic location that is being declared for embedded signatures.

In any case are newsworthy and its content is free of responsibility.

Users can also specify a password value in this panel, so that the program automatically opens protected PDF files before proceeding to complete a native PDF signature. This option is labelled as **Default password for opening protected PDF files**.

If the password with which it's protected the PDF file was different from which is pre-set in this field, Xolido®Sign interactively asks the user for it during the signing process.

Finally, as in previous cases, you can **reset default options** for the panel in case you want to return to the original state of the configuration.

Below there is the image of the configuration panel of firms to PDF documents.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

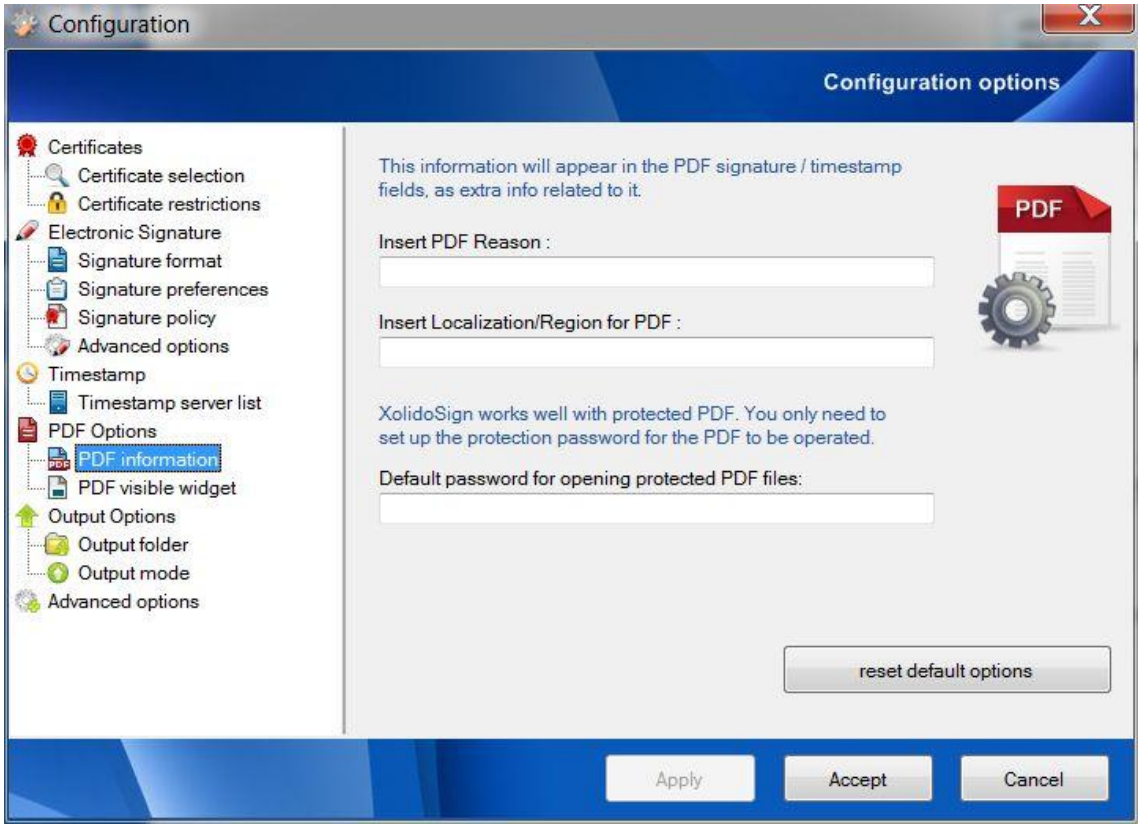

Fig. 30. PDF Documents signature. Configuration Menu.

5.4.2 – PDF visible signature widget

The following tab corresponds to the configuration panel for signatures appearance into Adobe PDF documents.

Below there is an image with this options panel:

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

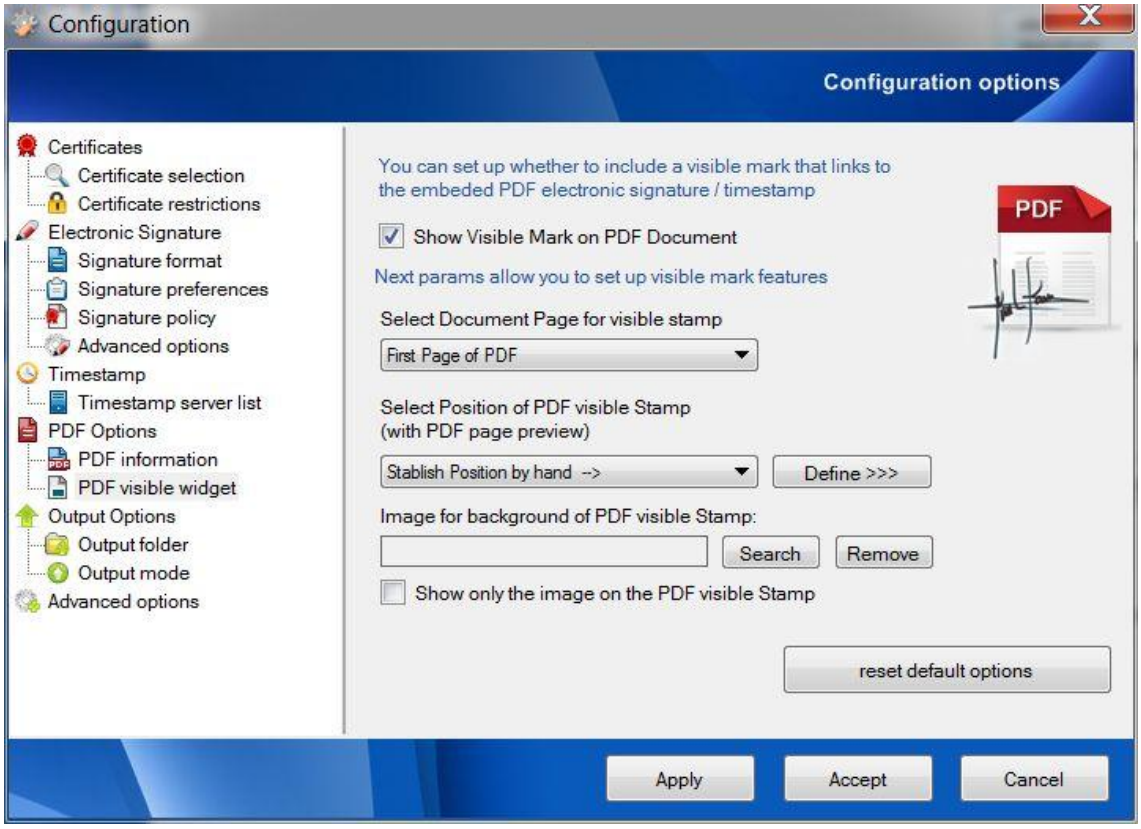

Fig. 31. PDF visible signature widget configuration.

First option allows user to configure **Signature visual widget** within PDF files. By selecting **Show visible signature mark on PDF document**, all PDF signatures will be associated with a visual field into signed PDF document.

This functionality of visible widget of the PDF signature is an option created by Adobe in order to have a visible link to electronic signature embedded inside the document. This link is located inside one page of the document.

Therefore, this visible widget is not the electronic signature itself and its scope is only to link to real electronic signature included within the document, and Adobe PDF allows that this link, in the form of a visible stamp, may only be placed in one position of one page of the document.

Nevertheless, it's important to annotate that embedded electronic signature covers the entire document (it signs the document completely) no matters if the visible widget appears or not, or where this visible stamp may be located.

Through both options included below title **Select Document Page for Signature stamp**, user can select first or last page of PDF document or set another page, within the valid page range of the PDF document, to display this visual Signature field.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

Through options included in **Select position of PDF Stamp**, user can establish Signature visual field position into PDF selected page.

It is also added the option to establish manually the position of the visible signature on PDF page that best suits their needs. It includes the possibility of previewing the pdf page to be signed in order to select exactly over the image the coordinates of the visible widget.

To establish a position and manually configure by the Set button in the Set position, the user must choose the drawing area of the electronic signature on page PDF files using the mouse, a dialog box similar to that shown in the following image.

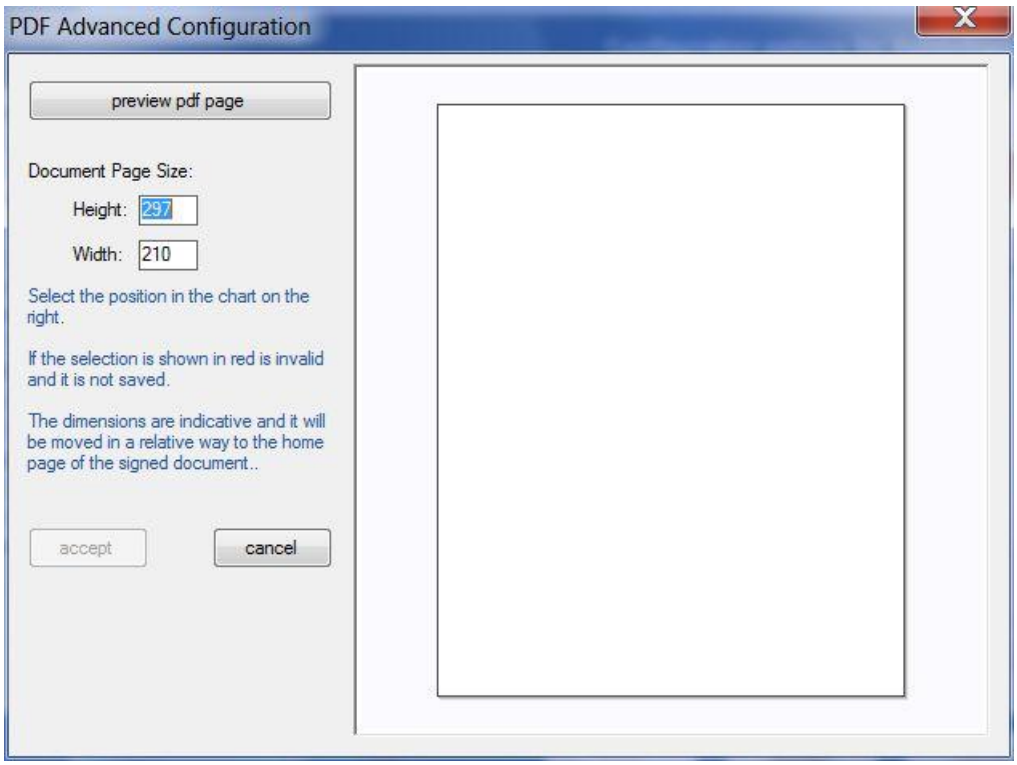

Fig. 32. Manual Configuration of the position for the visible signature.

It is also included an option to add a background image to those visible native PDF signatures. This image could be selected in this panel through last option labelled as *Image for Background PDF Stamp*, and its effect is to apply this image file to all PDF with visible signatures.

This background image could be a WMF vectorial format that will have an optimum visualization independently of the zoom given to the document.
Also, it's possible to indicate that you would like to introduce only this background image on the visible widget of the signature.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

Clicking **reset default options** button, user can retrieve original options selected by default in the application.

5.5. Output Options Area

This options group is related to the way and name configuration of the files processed by the application.

5.5.1 – Output folder

In this panel appear options to **Configure a Default Output Folder** for the documents signed or stamped.

By default, is set in the application a folder within the documents directory of the Windows user, however this is configurable so that, if another route is configured from this menu, at the start of the application it will always appear configured folder, and will not have to manually select it again before starting the operation of signature or stamp of all selected documents.

Also in this menu, users can **See Selected Folder** and **Reset Default** route included in the application.

We must emphasize that after the operation it will appear in the output folder the document to be signed or stamped with its signature or external time stamp associated or in the case of PDF documents (and being chosen to perform an embedded PDF signature), the result in the output folder will be a PDF file with the same name as the original, but with the digital signature embedded in it.

Below, there is an image with the options panel just explained.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

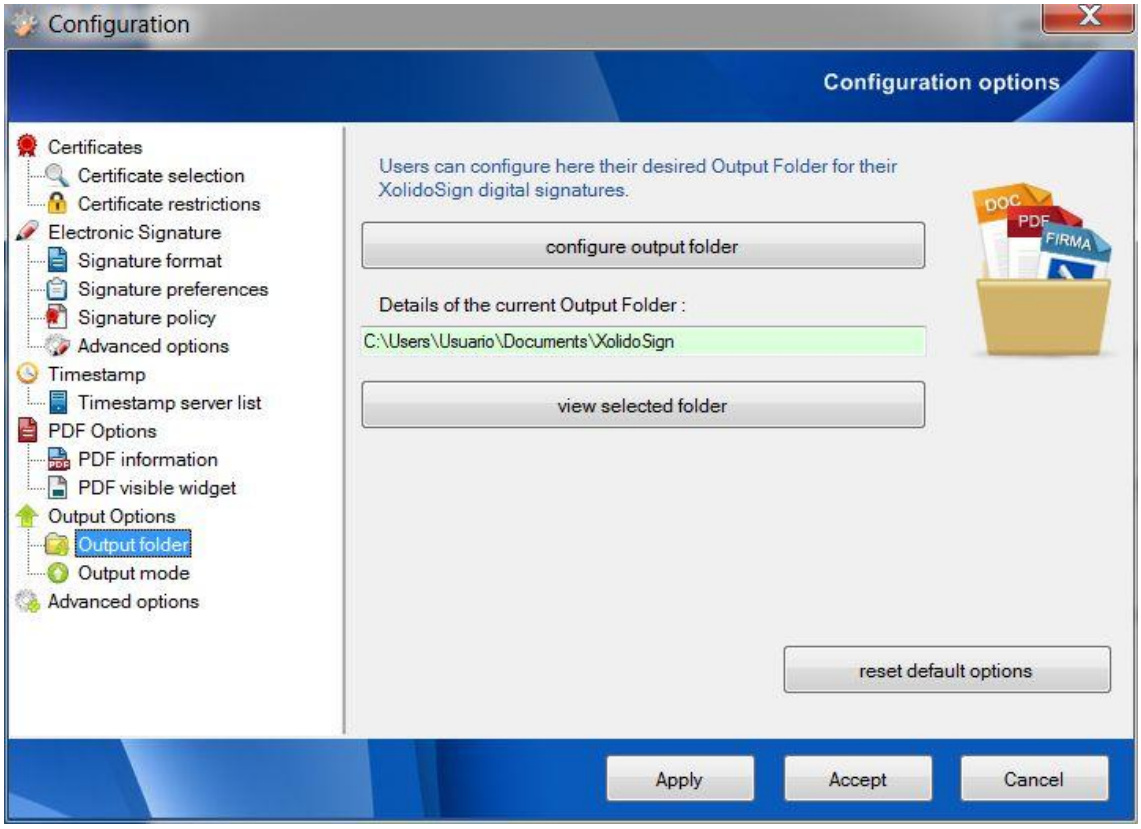

Fig. 33. Output Folder.

5.5.2 – Output Mode

In the following panel, there are some options related to output mode. With these options you can set how the application will save the results during the operation of signature or time stamp in the output folder.

User may choose one of the following options:

- *Direct mode*: the file is saved with the original name.
- *Default mode*: the name is added the string "_signed".
- *Authenticated mode*: adds the string "_signed_by_" followed by the basic name of the selected certificate and ended with the original extension.
- *Folder mode*: For each signing operation creates a folder with the date, time and a unique identifier for the operation of joint signature. Within every folder, files are placed in the same format as identified mode.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

- *Custom mode*: You could set up through a string of editable text. The string is simply copied, except for some special identifiers that are replaced during the signing process.

Special identifiers are:

- **%n** – File name without file type extension.
- **%x** – Former file type extension, preceded by separator dot.
- **%D** - Signature date, in format 'year - month - day'.
- **%H** - Group signature process time. Format is h00-m00-s00.
- **%h** - Single signature process time. Same format as above.
- **%I** - Random unique identifier for group signature process.
- **%i** - Random unique identifier for each signature process.
- **%N** - Name identifier obtained from electronic certified.
- **%S** - Full certified subject.

For operations with a result not embedded, as in the case of separate files signatures or time-stamps, the application adds the extension *.p7b* or *.tsr* to those names determined by the output mode chosen.

Below there is an image with the available options in the configuration tab for output mode.

Mod.: D201000074v07 20170301

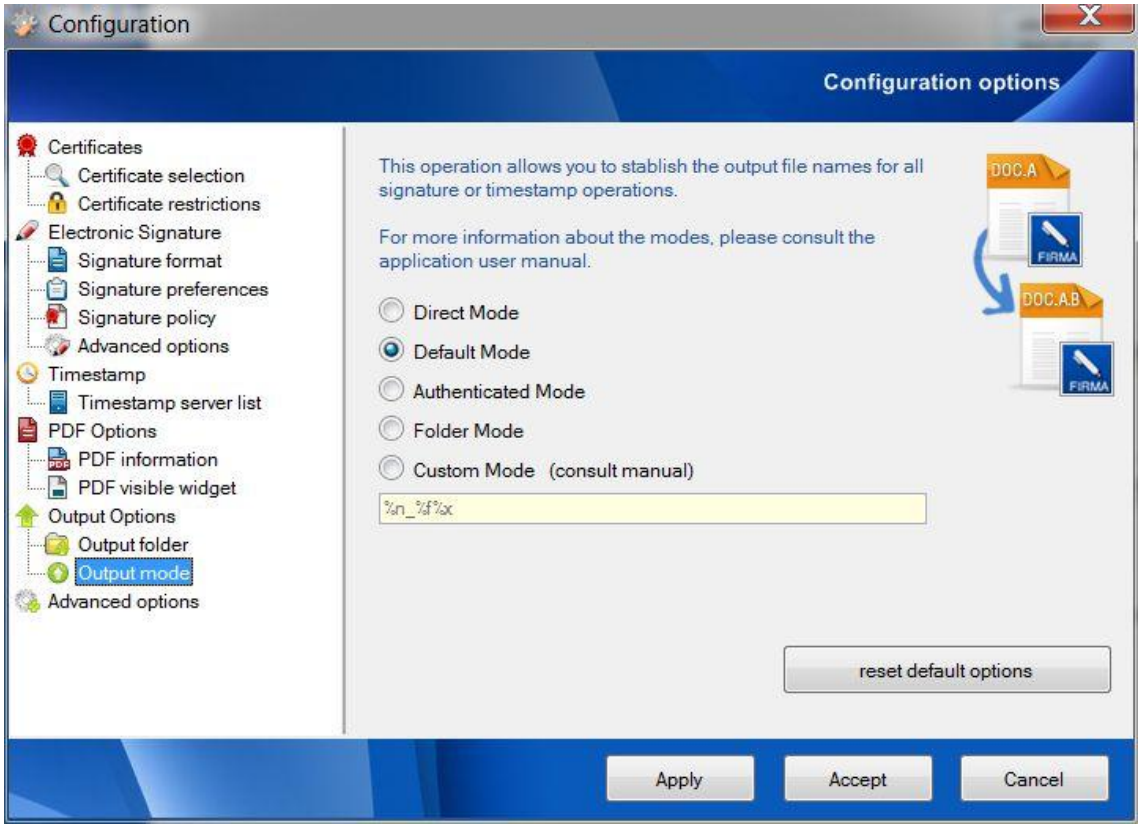

Fig. 34. Output Mode.

5.6. Advanced Options Area

Next configuration group are related to the following capabilities.

5.6.1 – Signatures log

First panel is about the configuration options for the Signatures Log. In the Signature Log file, it will be locally stored data during operations of signature or time stamp, in CSV format.

Once Signature Log file has been opened in any compatible software (like Microsoft Excel), user will find a table filled with following data:

- Signature process identifier
- Path and name of former signed file in signature process
- HASH corresponding with signature process
- Signature process date
- Signature type: embedded PDF signature, or PKCS7 format for external signature.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

- Certified name used in signature process
- HASH corresponding with certified used during signature process

User may activate Signature Log checking corresponding option, **Enable Signature Log into configured file path.**

Path to save Signature Log will be set and displayed into file text **Signatures Log Path configuration**.

Clicking **Reset Default Configurations** button, user can retrieve application selected by default configuration.

Below there is the image corresponding to the Signatures Log configuration tab.

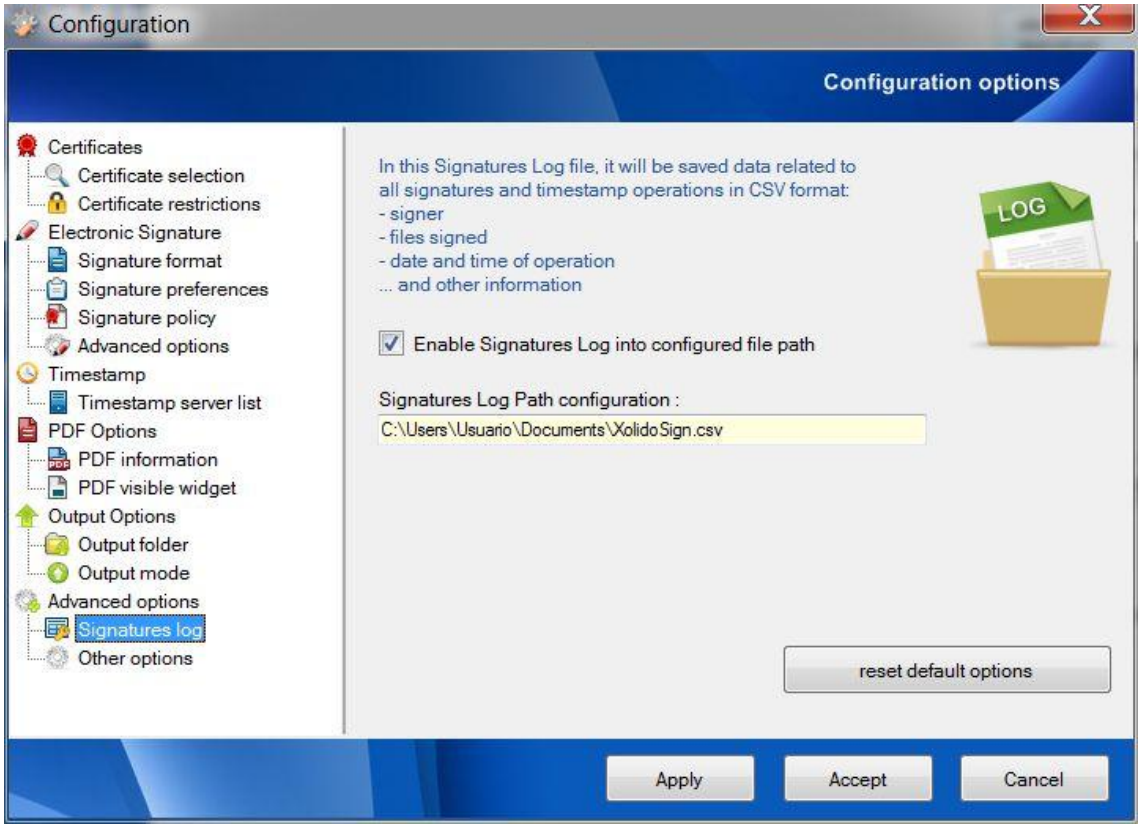

Fig. 35. Signatures Log.

5.6.2 – Other options

Last configuration panel is related to the advanced settings of the application. It is advisable not to change these options without having exact knowledge of the changes to be achieved, since an incorrect change could cause problems in the operation of the application.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

Among the available options we have the possibility to set the **size** within the **PDF reserved for the embedded signature** in these documents. You can change its value even though the application never will accept, for safety, less than 16,000 Bytes.

In previous versions of this panel, Xolido®Sign had additional options for general settings, which can now be accessed through the Global Options in the Control Panel.

Below there is a picture concerning the panel advanced settings that have just outlined.

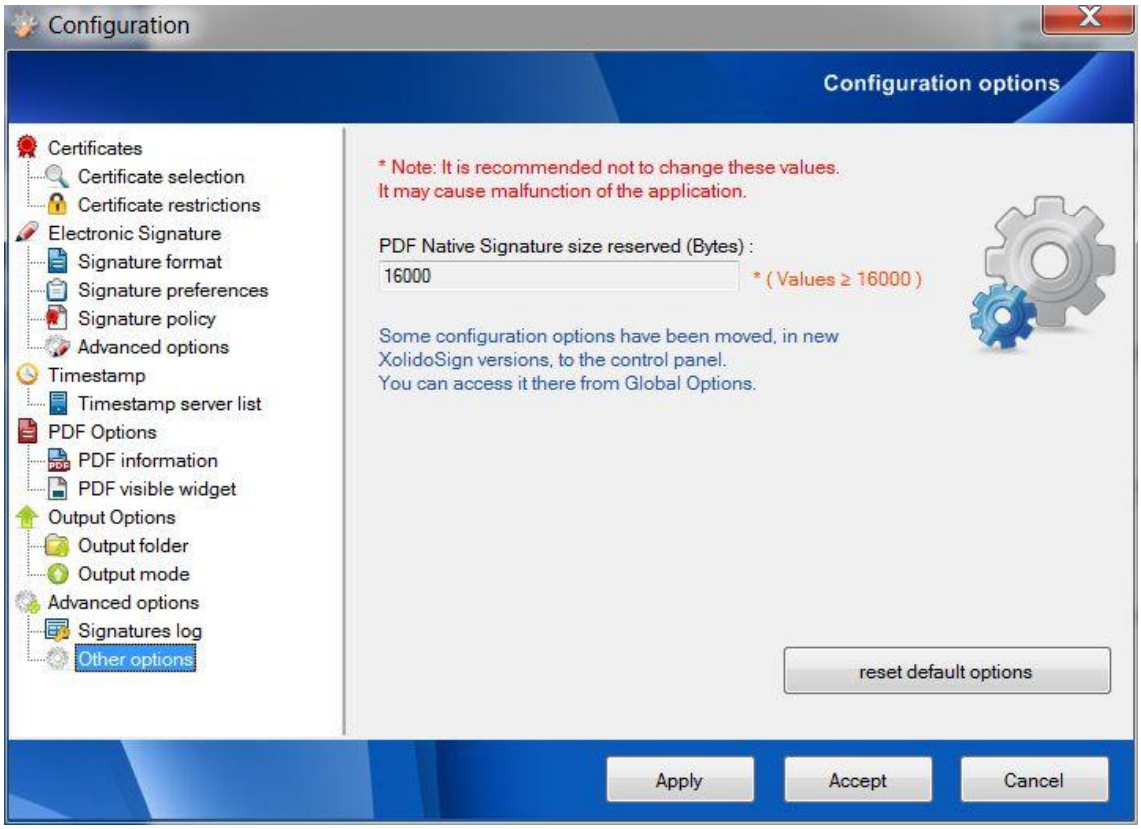

Fig. 36. Advanced Options.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

6. Xolido®Sign User Guide to Verify

Fig. 37. How to use free Xolido®Sign application to verify.

Xolido®Sign allows to perform the electronic verification of signed and/or time stamped files, ensuring that the document which has operated meets integrity properties, has not been altered since signing or time stamping, and ensuring the identity of the author or signer.

It also checks the external electronic signatures and/or timestamps, trying to associate them to the corresponding signed or time stamped files, and showing the corresponding verification information.

The procedure for verifying electronic signatures with Xolido®Sign meets the standards of ETSI (www.etsi.org), and IETF (www.ietf.org).

The electronic signature formats that Xolido®Sign can process are PKCS#7, CMS, integrated PDF signature, CadES, XMLDsig, XAdES and standard time stamping (RFC 3161). In addition, signatures may have external or embedded content, which is commonly known as *attached* and *detached* signatures respectively.

Also, the application is in constant development for integration and support of new signature formats.

6.1. Verification modes

Xolido®Sign has two operating modes, with both intrinsic differences in the features offered as to how to proceed in obtaining the results.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

6.1.1. – Smart verification

Smart verification mode performs an automatic process of pairings and associations between files and electronic signatures and/or timestamps included in the selection list and providing the validity status of signatures, timestamps and files.

Furthermore, the system tries to find electronic signatures and timestamps associated with each file located in the same that the file. Matches are made based on different mechanisms such as search by size referenced in the signature or file name.

Also, for external electronic signatures and/or timestamps that are not associated with any file, Xolido®Sign will try to find the corresponding signed or time stamped files and in any case it will also show their verification information.

Therefore, this mode is recommended for routine use, as it provides the user the task of verifying, delegating the application automatically search for correspondences between the files and electronic signatures.

In this smart verification, the user has to enter exclusively a list of files and signatures and/or timestamps, without concern of its kind when it comes to the selection.

After that, clicking on the button "start operation", all associations have been processed by Xolido®Sign, shown in a structured and intuitive way with the verification results of each file and its associated signers, corresponding well with electronic signatures or timestamps.

This mode shows in the upper band a filter to help users in those cases that have an extensive list of selected elements, which can be classified in their processing as electronic signatures or timestamps, or as files and documents.

Below is the interface that Xolido®Sign presents for this mode.

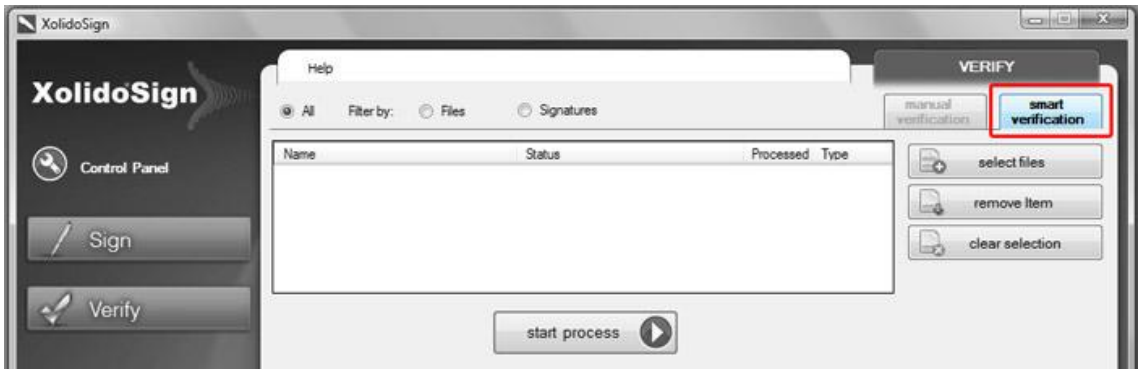

Fig. 38. Smart Verification mode interface.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

6.1.2. – Manual verification

Manual verification mode is used when the user wants to compare a set of signatures and/or timestamps with a specific file, indicating the connection explicitly, ie, presetting which file is to verify and each of the signatures and/or external timestamps that Xolido®Sign are to be contrasted with that file.

To this end the interface presents a first table that will add the item to be processed as a file and a second table to which user can add multiple items that will be computed as signatures and/or timestamps y that would be contrasted mandatory with the selected file.

The result of the process shows the validity status of each of the elements that having been associated with the file, could had been processed as electronic signatures or timestamps.

Below is the image of the application with the manual verification mode selected.

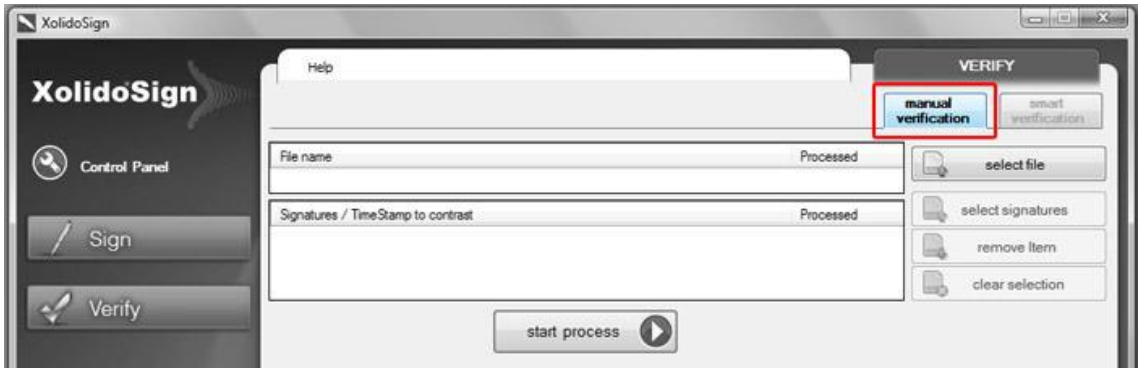

Fig. 39. Manual Verification mode interface.

6.2. Electronic verification process

The procedure for verifying electronically signed and/or time stamped files taken out by Xolido®Sign included, as representing, the following steps:

- Determine, for each of the files to be processed, the relationship of electronic signatures and/or timestamps that can be associated.
- Determine each of the signers involved in each of the signatures associated with a document or file.
- Check the date on which the signatures were created.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

- Obtain and validate digital certificates used for the moment of electronic signatures creation.
- Get revocation status information of the certificates both for the present moment, as in the moment of signature creation (through standard mechanism as CRL or OCSP) to check their validity status.
- Check the integrity of electronic signed data by known cryptographic algorithms.
- Extract the signer's complete data and allow access to the digital certificate used.
- Determine the reliability of certification authorities (CA) and time stamp authorities (TSA), depending on the entities recognized by the user, through its trusted root authorities store.

A key point in the electronic verification involves checking and analysis of digital certificates employed to perform digital signatures by the signers.

The time taken for the application to obtain the results and completion of the operation may vary considerably depending on the slowness or speed with which each CA responds to requests for the revocation status of the certificates.

The procedure for validating digital certificates is described in RFC 5055. Among the steps executed by Xolido®Sign for checking certificates include:

- Validate all certificates in the certificate chain, to determine the degree of trust that can be attributed to the signer's certificate.
- Check the level of trust of the various certification authorities used for checking certificate revocation status.
- Analyze data included into the digital certificates to verify their structural integrity.
- Determine the complete information about the owner of the digital certificate.

The verification of electronic signatures and time stamping is based on the degree of goodness of four key features, used to determine the overall state of their validity and are:

- **Trust**

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

The application states that the certificate used by the signer is trusted when you can build a complete trust chain and its root certificate is installed in the Trusted Authorities Store on your Windows computer.

In order to complete the chain of trust Xolido®Sign needs to have all the certificates of it, being able to locate them both from the signature and in the Windows certificate store on your computer.

Xolido®Sign also evaluates the temporal validity of the digital certificates and their purpose.

- **Revocation**

Certification authorities, CA, use online protocols to inform about the status of the certificates issued before the expiration date.

Xolido®Sign considers of importance to obtain the revocation status, since it is the only way to completely ensure that the certificate used for the signature is considered valid at the time of signature creation.

Xolido®Sign indicates a warning if it's not able to obtain the revocation information and indicates a failure if gets the confirmation that the digital certificate was revoked prior to signature creation date.

In the case of signatures with embedded revocation data, Xolido®Sign accepts the values embedded if its assessment is considered correct.

If a failure occurs trying to successfully complete this assessment Xolido®Sign process will continue with an online conventionally check.

- **Integrity**

Electronic signatures contain internal mechanisms that must be respected so that they are cryptographically valid.

Xolido®Sign marks integrity as invalid if some mechanism is not satisfied.

- **Match**

In this section Xolido®Sign notifies if the signed data match the file that has been associated. If Xolido®Sign indicates invalid match, it could be due to the associated file is not the signed one, or the signed file was modified after signing.

In addition Xolido®Sign can notify an invalid state if he had not found an association with a signed file. In that case, Xolido®Sign allows the user to locate and select the file manually.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

- **Signature creation time**

One of the most important aspects in the context of electronic signatures, is to know the date and time when the signature is created.

The signing time of the signature is vital to understanding the validity and revocation status of digital certificates used in the electronic signature process and hence its importance goes beyond a level that comes to granting or denying the reliability of the whole process of electronic signature.

To ensure this fact there are several mechanisms, each of which is associated with a level of trust and credibility, Xolido®Sign computes for all electronic signatures processed the time of its creation and determines a degree of priority if there are several time sources.

First of all, Xolido®Sign considers the case that the signature includes a timestamp provided by a TimeStamp Authority (TSA) of trust. In that case, the date and time that such entity, third in confidence, announced is taken as the moment of creation of electronic signatures.

In case of a signature not including a timestamp, signer could have indicated the creation date as a standard. Being a value that determines the signer himself, Xolido®Sign display that moment just for information but does not accept as reliable.

In case of integrated PDF signatures, not adding a timestamp, the document itself contains information structures with, among other values, the creation date of the electronic signature. Xolido®Sign show that time just for information but neither accepted as reliable because they are far coming from the signer computer time and therefore can be easily manipulated.

6.3. Verification results

From the data obtained during verification process Xolido®Sign presents results in an understandable format and trying to minimize the underlying complexity when showing information, so that users can have a global and comprehensive idea about the validity status of each of the signatures or timestamps associated with files and processed by the application.

In all cases Xolido®Sign presents the summary results for each of the key points to be analyzed in the process of electronic verification, as explained before.

The application has two interfaces for data presentation, for files and signatures, differentiated by type of procedure received by each one, and they are explained below.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

6.3.1. – Files

When the item is processed as a file, the summary will be displayed in the image below.

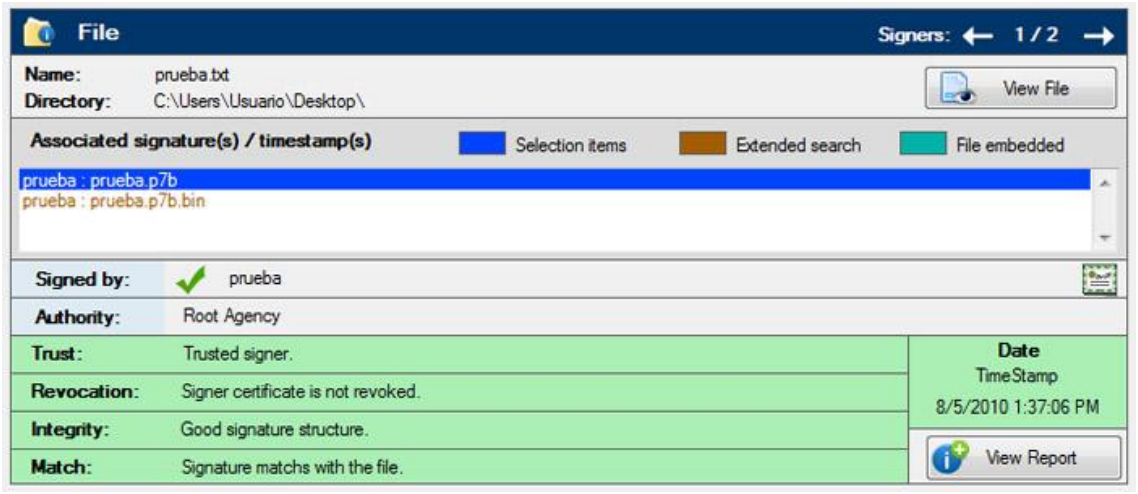

Fig. 40. File verification result.

Several areas can be distinguished; the top indicates the name and path to the file, along with the "**view file**" to open it directly from Xolido®Sign (in case that the operating systems had an associated application).

Below is a listing of each of the signatories related to the file. It's also indicated by a color legend the origin of each of the signatures in which the signer is shown, and may be an existing item in the user's selection, or one that comes from the widespread search by the smart verification, or a signature embedded in the file itself (for the PDF integrated signatures), or an item that the user has connected to a file manually, in manual verification.

Next area of the information panel shows the result of verification for the signer selected in the list above.

As previously discussed, Xolido®Sign considers several points of particular interest in the computation of a verification.

These sections are presented in the panel, color-coded background that indicates the degree of validity in an intuitive way.

Xolido®Sign processes an overall assessment of the state associated with each of the signatories, and indicates it near the signer name, with an intuitive icon.

Icons of this overall state and their meaning are shown below.

Mod.: D201000074v07 20170301

Fig. 41. Valid signature.

Fig. 42. Valid signature but warnings must be considereded.

Fig. 43. Problems with signature.

Fig. 44. Signature is not valid.

Thus, if the user scrolls through all the signers associated with the file and displayed in the list, can quickly view, for a given file, its validity status according to the cryptographic information associated with it, analyzing the reliability of electronic signatures and/or timestamps.

There is also a button, called "**view report**" in the lower left, to access the report issued for the selected signature verification.

This report contains detailed information about small changes and events that occur in each of the verification cases, so that more advanced users can view a complete analysis of the results obtained by Xolido®Sign.

It is used in any case a color code and intuitive symbols so that users can easily perceive easily the result of verification.

6.3.2. – Electronic signatures / TimeStamps

For items processed as electronic signatures and time stamps, will the result shown in the image below.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

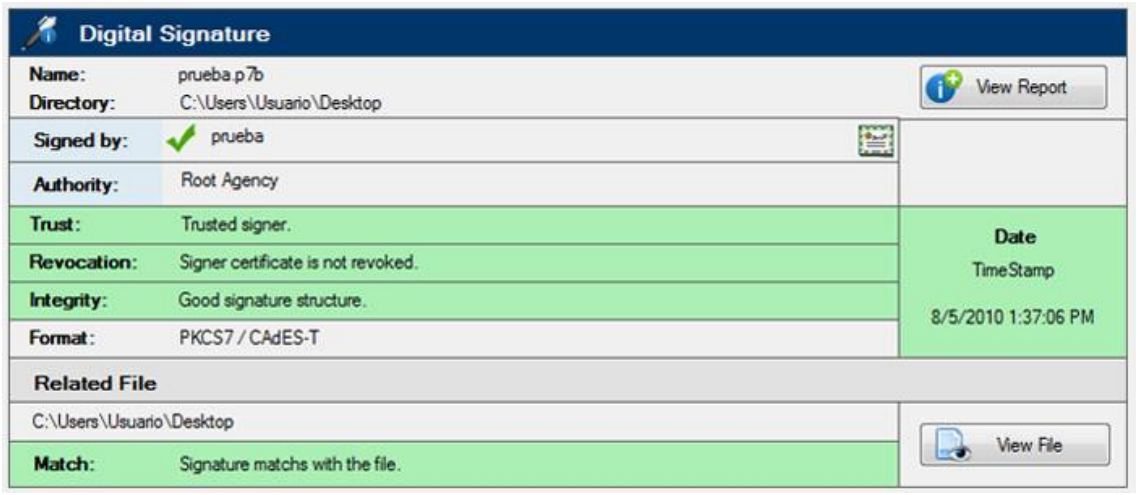

Fig. 45. Signature / TimeStamp verification result.

At the top is the generic information, name and the path where the file of electronic signature or timestamp is located, and the button "**view report**", to access the detailed report with the results of verification for the signature or stamp in question. This report gives advanced users full information about de each of the incidents that may occur during the verification process.

Xolido®Sign present a panel to report situations in which a signature contains multiple signers, which is known as CoSign, so that users can navigate through these signers easily, showing the validity status associated with each of them through the global rating icons used by Xolido®Sign (see Fig.28-31).

For the signatories of each firm shows each of the sections that make up the basic verification information, trust, revocation, integrity, match and signing time in color-coded panels intuitive for users to easily interpret results.

In the lower part of the panel, it shows the section relating to the file associated with said electronic signature or timestamp, indicating both the path of the file and the match status between file and signature or timestamp.

Also there is the button "**view file**" You can access it directly (if the operating system have a program associated with the extension.)

Even for firms which signed content is included within the signature structure (attached), the application tries to extract the content to be shown to the user in a comfortable and easy way.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

6.3.3. – Extended verification report

For advanced users, or those wishing to access detailed information for each of the sections that make up the verification of an electronic signature or timestamp, Xolido®Sign has a verification report panel.

This report looks similar to that shown in the picture below.

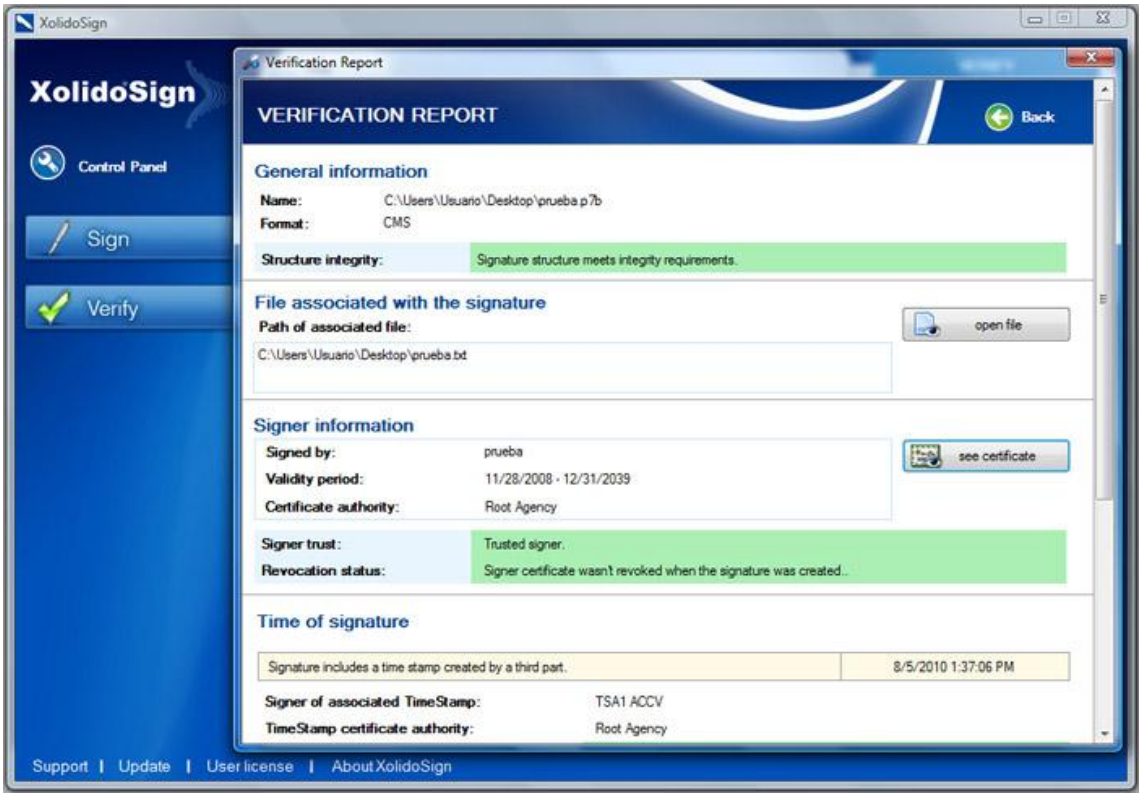

Fig. 46. Extended verification report.

This report shows data processed by Xolido®Sign through the verification process. Has extended sections relating to each of the analysis, including most notably:

- general information about name and location in the user's computer files processed during, also indicating the format for the signature, so that the user can know if the item fits a certain standard.

- information about the number of signers, in case of being a CoSign signature, showing for each one its descriptive name.

- complete information of each of the signers, drawing its name, the authority which supports him, time of validity... and showing the user the extended data about their state of trust and revocation,

with explanations in each case if problems were detected. Also gives the user access to the certificate used by the author, through the relative icon.

- information about the instant of time when the signature was created, indicating , if exist, various sources the date and time. Also, in case of a moment that comes from a timestamp, it will be supplemented with information concerning the time-stamping authority (TSA), and its corresponding status of trust, revocation and integrity, so that the user has no doubts about the degree of validity of the point in time announced for the creation of electronic signatures.

- extended information about the structural integrity of electronic signatures and/or timestamp.

- advanced information about the match between the file and the signature, so that not only is a brief explanation, but will the signed hash (decrypted from the signature or timestamp) and the associated file hash.

Mod.: D201000074v07 20170301

7. Technical information about Xolido®Sign

Xolido®Sign provides additional information for users more advanced on technical issues.

Among the additional data developed for the application is a greater scrutiny of the revocation information for signing certificates.

Xolido®Sign has its own namespace within the object identifiers (OID) that international entity IANA (*Internet Assigned Numbers Authority* – www.iana.org) provides for the establishment of structures with essentially technical level briefing, and starting from root id (*1..3.6.1.4.1.35788*) assigned to Xolido Systems, S.A.

Documentation of such tree data structure used by Xolido®Sign in order to offer users a more exhaustive control for their digital signatures data is available inside the folder ***DOC*** within the application directory, with the name *XolidoSign Información Técnica*. This document is only available in Spanish language.

Also, Xolido®Sign provides users with a record of changes made in the application over its version history. This information may be interesting to see the improvements and new features added over time on the application. This file is named as *Changelog* and can be accessed in the folder ***DOC*** within the directory of the application. This document is only available in Spanish language.

There are also available in this ***DOC*** folder the PDF user manual files, version both Spanish and English.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com

8. Other Xolido®Sign interesting information

Xolido®Sign has a structured offline support, which also contains information about the concepts of digital signatures and electronic time stamp, and can be accessed via the top menu of the application, following the path *Help -> Help Center* or by pressing the F1 key on your keyboard.

The application also makes a quiet control of possible new versions so that the user can keep up Xolido®Sign regarding the version used and to enjoy the new developments which contain the newest versions of this free application.

Xolido®Sign has a free and for all users available mailing list, which everyone interested can subscribe to, and receive the latest news about the implementation.

The address from which you can subscribe to the mailing list is as follows:

Subscribe to Xolido®Sign mailing list

(http://www.en.xolido.com/products/xolidosign/news/subscribe/).

Any suggestions about possible improvements of the application, or doubts about the use or functionality of Xolido®Sign could be sent us through the following mail address: xs@xolido.com

*This is an adaptation of **Xolido®Sign** spanish manual. In any case, the original manual could be consulted if there is any doubt.

Xolido Systems, S.A. · C/ Pío del Río Hortega, 8 – 2ª Planta, Oficina 7 · 47014 Valladolid · Spain · www.xolido.com Tel. +34 983 298 272 · Fax +34 983 298 205 · info@xolido.com