Volume

1

INFOMOSAIC CORPORATION

Making Digital Signature Easy

SecureSign User's Guide

SecureSign Desktop Document Signer User's Guide

Version 1.0.6

2118 Walsh Avenue • Suite 200
Phone 408.988.4337 • Fax 408.516.9427

Table of Contents

Chapter

1

Installation

Please read this section first.

After you have downloaded SecureSignInstall.exe executable file please double click it to launch the SecureSign InstallShield setup application, which will walk you through the set up process. Please accept all default settings for the installation. The installation program may install the .NET Framework on your computer if it is not present already. If the installer gives you an option to install the .NET Framework please accept it.

The following are the supported platforms:

- Windows 98 SE
- Windows 2000 Professional
- Windows XP Professional
- Windows XP Home
- Windows ME

Memory Requirements: 128 MB
Hard Disk Requirements: 30 MB

Additional features:

- Live signature image capture using an external electronic signature pad.

  If you have a Wintab32 compatible electronic signature pad, please make sure that the vendor provided Wintab32 device drivers are installed before installing SecureSign Desktop Document Signer. If you have already installed SecureSign please follow the following steps after you have installed the signature pad vendor provided Wintab32 device drivers:

  On a DOS prompt please change directory to C:\Program Files \Infomosaic\SecureXML and type the following command

Regsvr32 securepad.dll
You should get a message window declaring that the registration was successful. If you get a failure, the Wintab32 drivers are not properly installed.

- Microsoft Word file signing with signer information included in the word document.

  If a recipient of a signed document has Microsoft Word XP installed on the computer, SecureSign adds the signer information to the Word file footer and at the end of the word file. The file end signer information also includes the signature image if one was included during the signature creation process.

  No additional setup or installation is needed to enable this feature.

  Future versions of SecureSign will allow user customizations for how the signer information is displayed in the signed document. Future versions will also support additional file types such as other MS Office documents for the display of the signer information in the signed documents when they are opened for viewing or are printed.

Chapter

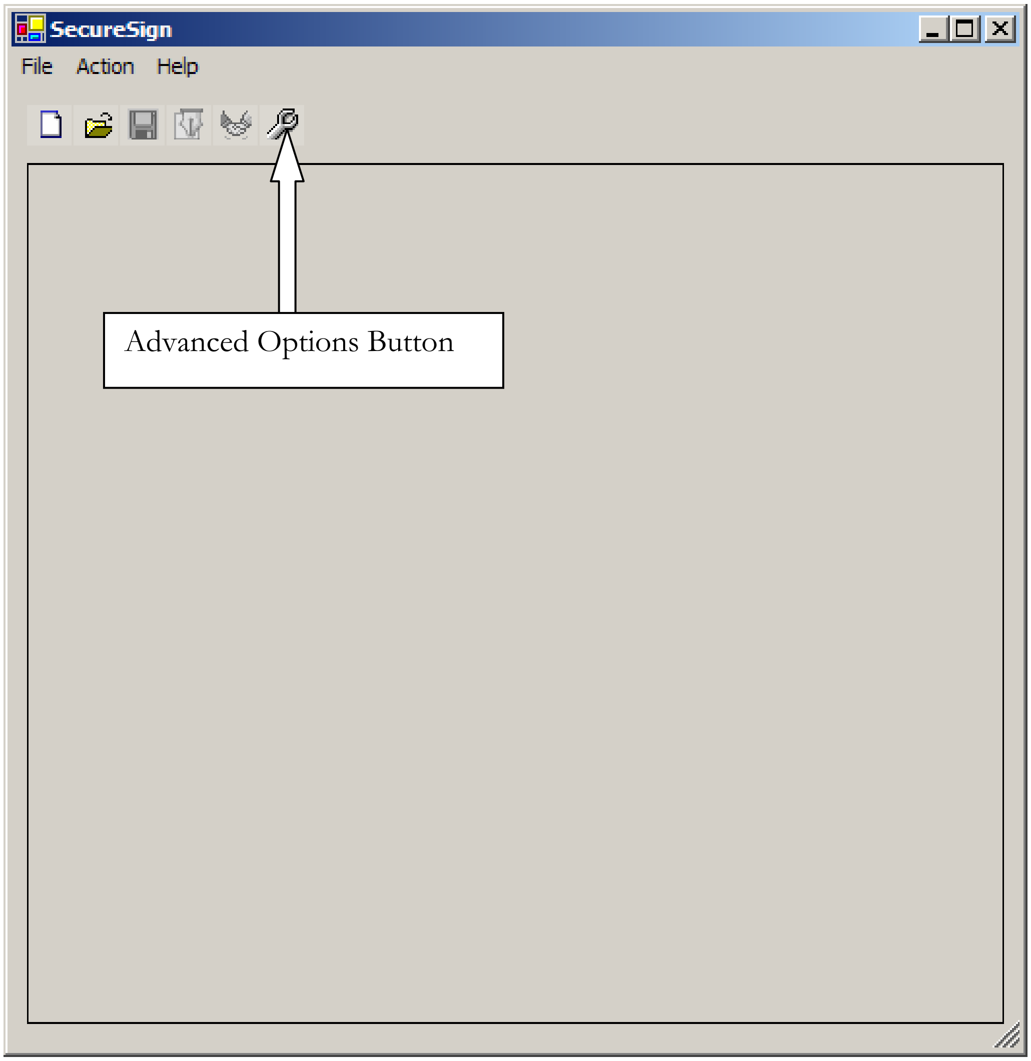
2

Initial Setup

DoD Compliance

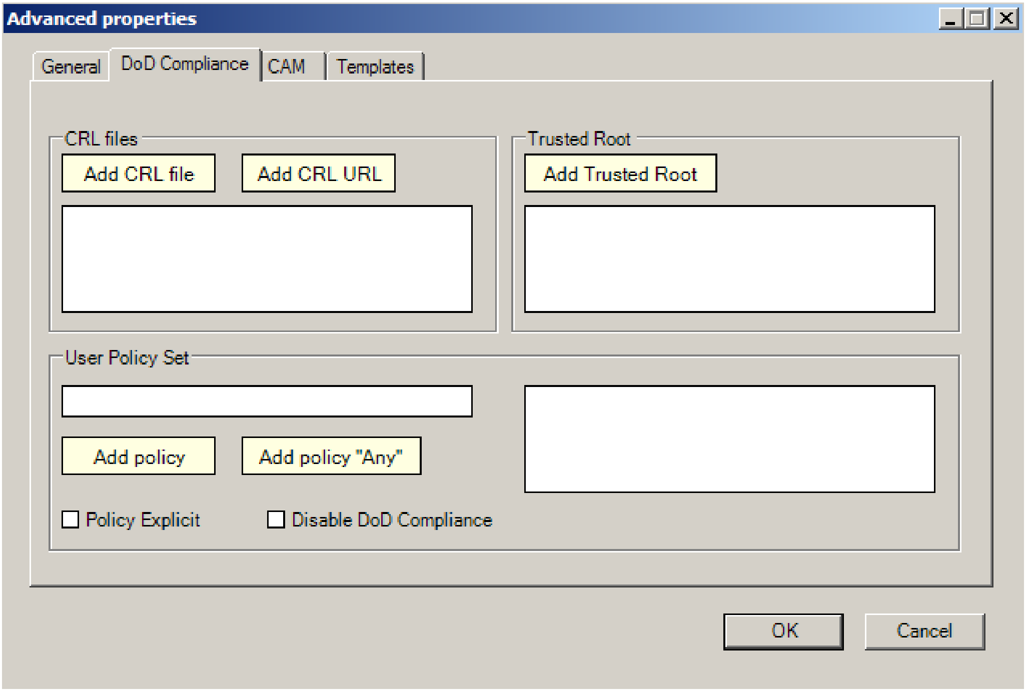
For US Armed Force Users

If you are part of the US Armed Forces, you are required to observe DoD Compliance at all times. SecureSign as shipped by Infomosaic has the DoD Compliance enabled by default. DoD Compliance requires that you specify trusted root certificates explicitly. Before you can either sign a document or verify a signed document, you must select at least one trusted root certificate. This is done in the 'Advanced Options' panel. Please click on the Advanced Option button to get to the Advanced Options panel as shown below. You can also get to the Advanced Options panel by select Action on the menu panel and then selecting Advanced.



Once the advanced panel is visible, please select the DoD Compliance tab and click on the "Add Trusted Root" button and select the certificate file containing the trusted root public key. This trusted root certificate must also be present in the Windows Trusted Root Certificate Store. Once a Trusted Root is specified, SecureSign remembers it across sessions so you don't have to specify it again unless you need to make a change.

For US Armed Force Users, the Disable DoD Compliance must remain unchecked. This also implies that you cannot use the SecureXML Web Service for signature verification as it disables the DoD Compliance.



For Non-US Armed Force Users

For all users who are not part of the US Armed Forces, DoD Compliance is not a requirement and hence you can disable it if you wish. Please note that DoD Compliance enforces better certificate validation and hence is a better framework to use. It does, however, introduce additional processing time and hence can sometimes make the signature creation and verification relatively slow. If you have DoD Compliance enabled, you must have access to CRL information at all times in order to create or verify a signature. It means being connected to the internet such that SecureSign can access the Certificate Issuer's CRL server to fetch the CRL information to ensure the certificate validity before use.

CRL Files

If the certificates being used do not have a CRL distribution point specified in them, then you would need to specify them in the advanced panel. Please note that if you specify a CRL file here and it is not accessible during signature creation or verification, the certificate validation will fail. Both local files and web based (both http and ldap accessible) file locations are allowed.

For US Armed Force users, to the best of our knowledge, approximately 100,000 of the early issued PKI certificates did not include a CRL distribution point. In order for all users to be able to use these certificates, a CRL file location must be specified in the Advanced Panel. In the event a CRL file location is not specified, and you happen to receive a signed document from personnel who is using one of the non-DP PKI certificates, you will not be able to verify the validity of those documents. Please ask your local IT person to help you with the CRL file locations. They are most probably stored in an LDAP server in your intranet. If this is indeed the case, please click on the "Add CRL URL" button and type in the complete URL starting with either http:// or ldap://.

Policy Settings

This is relevant if your organization requires enforcement of certificate policies. By default, the policy is set to "Any Policy" i.e. every thing is acceptable. If DoD Compliance is disabled, policy checking is turned off except when one or more policies are entered by clicking the "Add Policy" button. For US Armed Force users certain certificate policies may be enforced. Please check with your local IT personnel and set them accordingly. You may also be required select the "Policy Explicit" check box.

Selecting Signer Certificate

Certificate Installed In Windows Certificate Store

If you use the same computer for all your signatures it may be more convenient for you to setup a signer certificate to be used for all subsequent signature creations. It will prevent SecureSign from displaying the certificate selection window before each signature creation. If the private key for your certificate is stored in a smart card such as CAC and the smart card requires a password for accessing the private key, you will be prompted for this password before each signature. SecureSign does not have access to this password and cannot supply it to the smart card automatically. Same is true if you have the certificate private key in the Windows certificate store and it is password protected.

Using P12/PFX File For Signature Creation

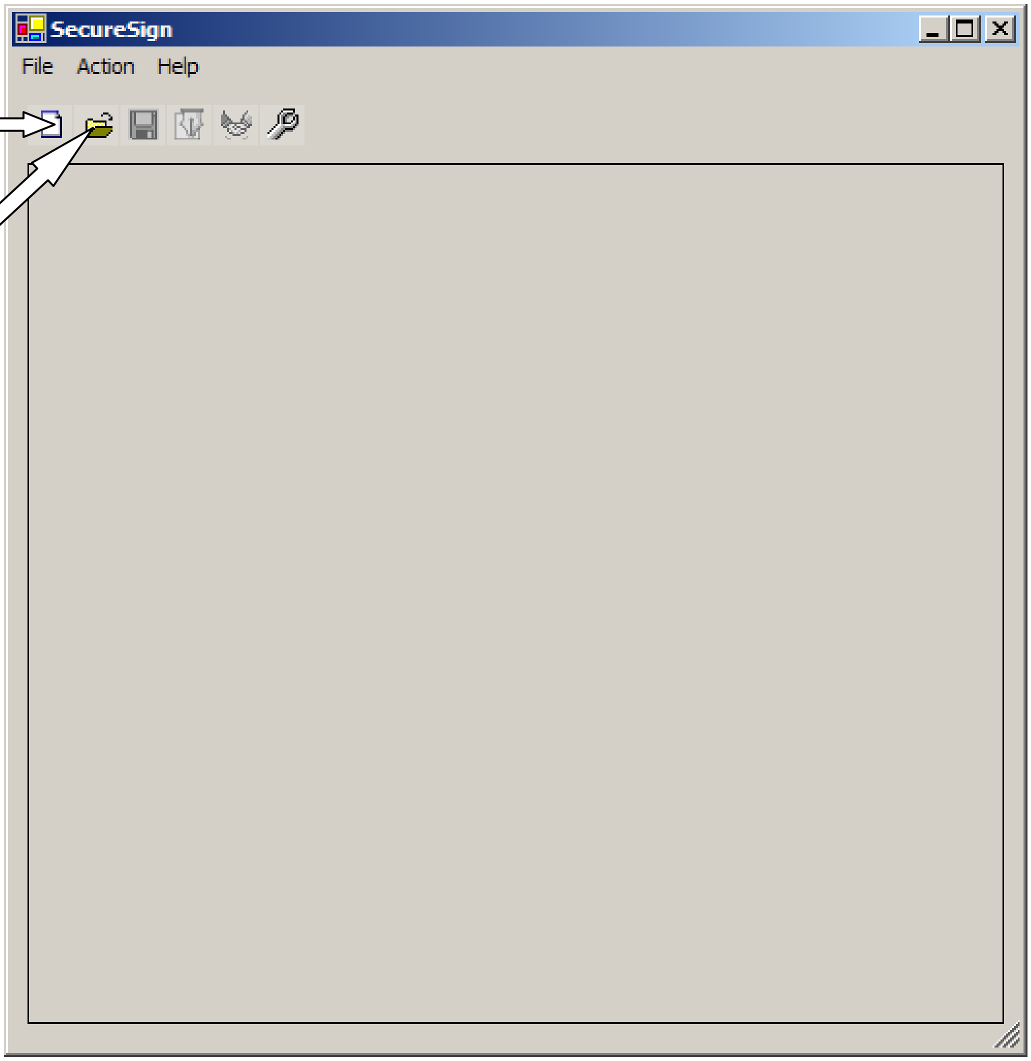
If you have your private key stored in a PKCS#12 file you can select that file here and specify the password used to access the private key. SecureSign does not remember this password and you must specify it every time.

Time Stamp Server Setup

SecureSign by default is setup to use the local system time for recording the signature creation date and time. It is also setup to use NIST time server for time stamping and you can enable the NIST time server usage by checking the Timestamp from URL checkbox. You can also specify a different time stamp server here if your organization is required to use a different time stamp server.

Chapter 3

Signing Documents

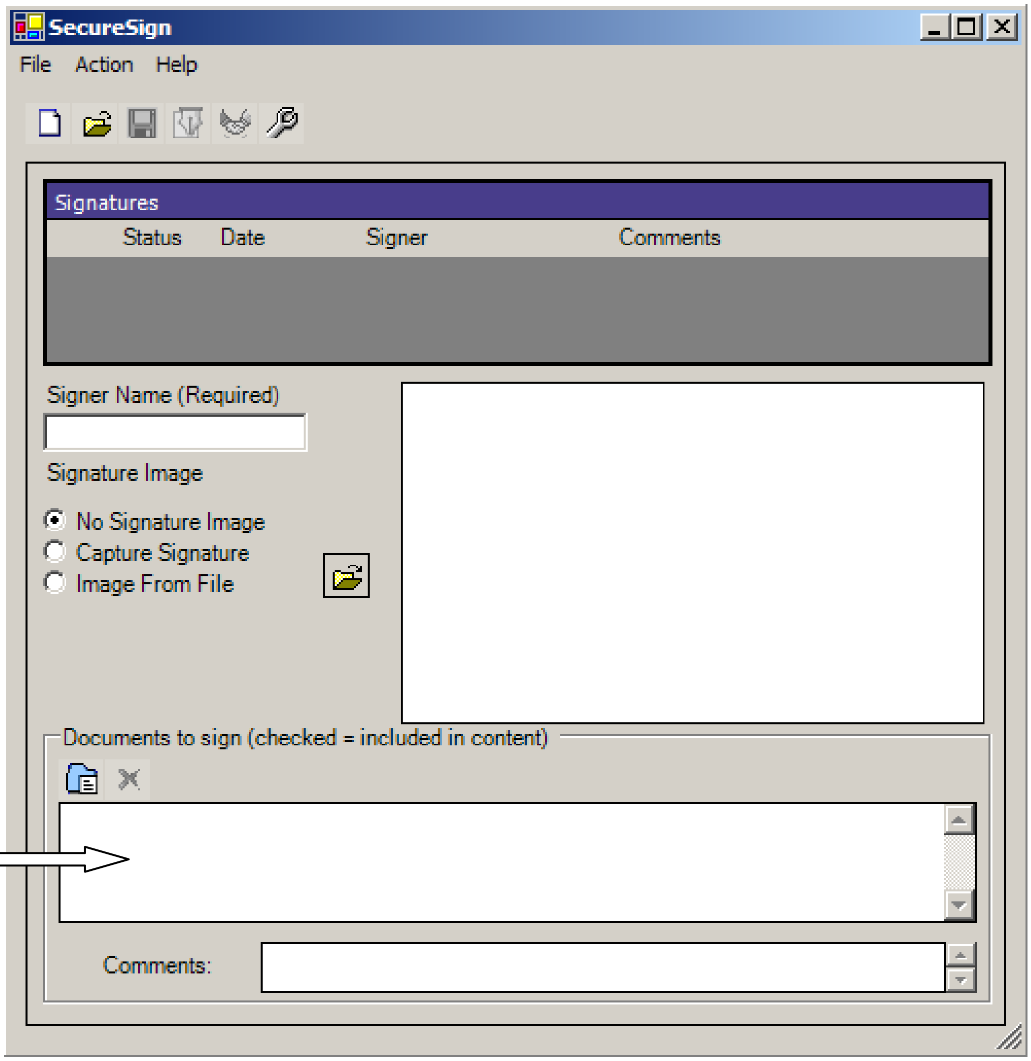


Click the new document button for creating a new signature

Click the open signed document button for verifying signature and accessing the content of the signed documents.

Before creating any signature, please make sure that all the initial setup has been completed and that you have access to a PKI certificate with a private key and you know whether it is in a PKCS#12 file, a smart card, a USB token or in your local Windows certificate store. In the case of a smart card or a USB token, you still need the certificate imported into the Windows certificate store (it will not import the private key so it will remain safely in the hardware device).

SecureSign allows you to either drag and drop documents onto the document to sign panel or select them by clicking on the document selection icon. First you click on the new document button. Now you can see the document reference panel and associated icons.



● No Signature Image
○ Capture Signature
○ Image From File

Drag and drop files here from your desktop or Windows Explorer

Please go ahead and type your name in the Signer Name text box. Next you need to specify whether to include a signature image with the digital signature. You can either capture a live signature or use a previously saved/scanned signature image. Please make your selection by clicking on the appropriate radio button. If you chose to include a file signature, please click on the Open File icon next to the radio button and select your signature image file.

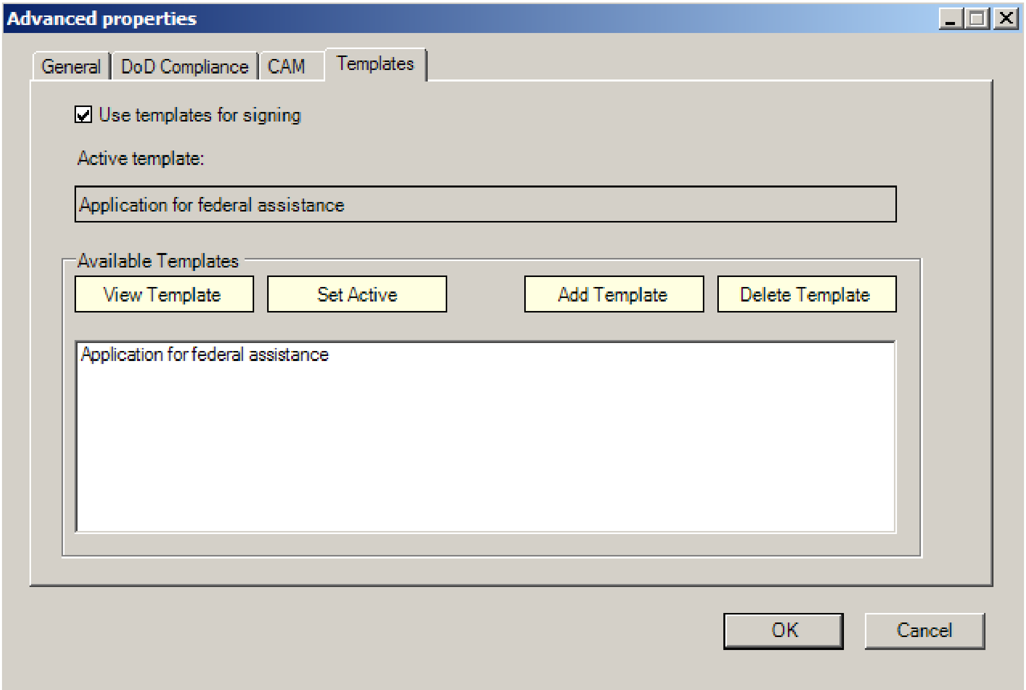
Once you have specified your signature image preference, please select files you would like to sign either by dragging them from your desktop and dropping them onto the "Document to sign" panel or by clicking on the document selection icon in the "Document to sign" panel. Once you have added all the documents you want signed, you are ready for the final step.

Please click on the "Sign" icon on the top toolbar. This will invoke additional GUI components as needed. You will see a signature image capture window or approval of file signature window if a signature image option was selected. If a PFX/P12 file or a default signer certificate was not selected in the advanced panel, you will see a certificate selection window where you must select a certificate before the signature creation will proceed. If your private key resides on a hardware device such as a smart card or a USB token, you may see additional GUI from their CSP layer components asking you to provide your password for accessing the private key.

After you have selected a certificate, SecureSign will verify its validity as per the options specified on the advanced panel. If the certificate passes this verification, a signature is created and then immediately verified. This signed document currently resides only in the computer's memory and you must save it to the hard disk in order to access it at a later time or to send it to another person for cosigning.

Signing Template Based Forms

Before you can sign a SecureSign template based form, you need to add it to your system by selecting the Templates tab in the advanced panel.



☑ Use templates for signing

Active template:

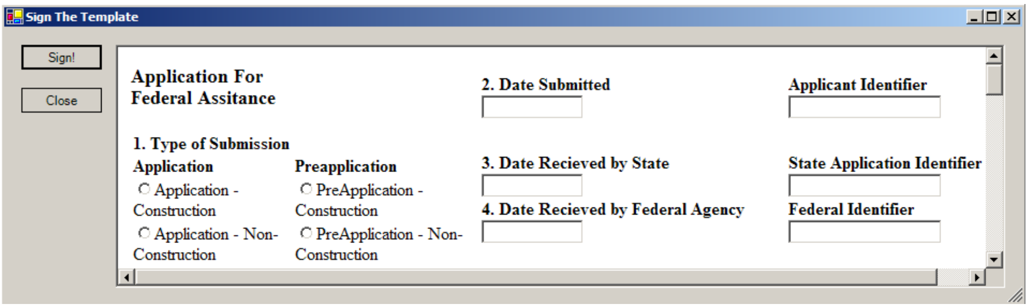
Application for federal assistance

Available Templates

Application for federal assistance

In order to add a template to your system, please click on the *Add Template* button and select the template file from your hard disk which you would like to use. Once added, the template will be available for use during all future sessions of SecureSign. After adding a template, please select it in the template list panel by clicking on its name once and then click on the *Set Active* button in order to make it the active template. Next please check the *Use templates for signing* check box. The template will now be used on the next click on the sign button in the main panel.

The following is an example of what a template based form might look like. Please note your actual form make differ considerably from this illustration.



Application For Federal Assitance

2. Date Submitted □

Applicant Identifier □

1. Type of Submission

Application	**Preapplication**
○ Application - Construction	○ PreApplication - Construction
○ Application - Non-Construction	○ PreApplication - Non-Construction

3. Date Recieved by State □

State Application Identifier □

4. Date Recieved by Federal Agency □

Federal Identifier □

Chapter

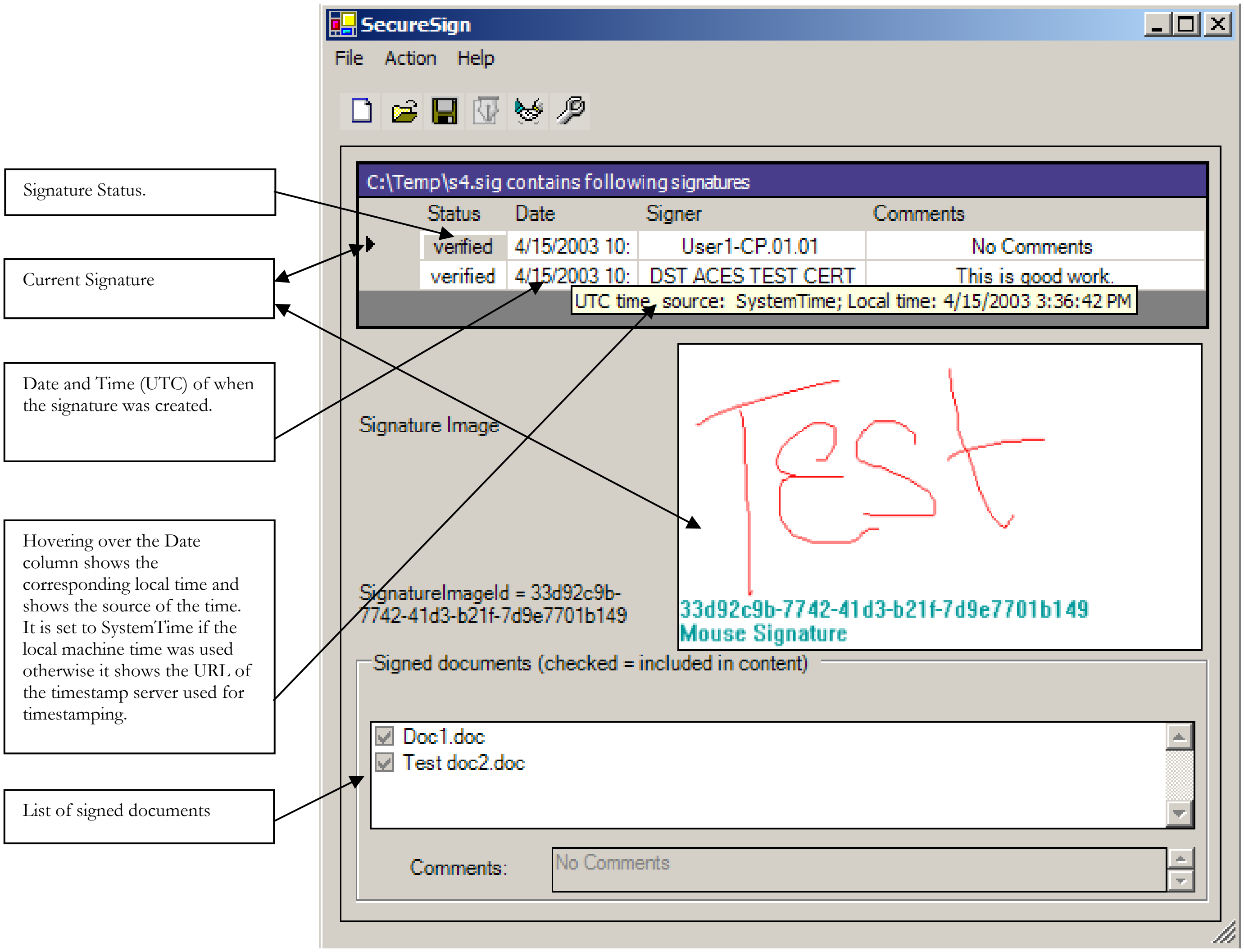
4

Verifying Signed Documents

There are two ways to open a signed document and verify the validity of its content. You can either double click a signed document (a .sig file) or select open from the file menu to open the signed document. Either way, SecureSign will verify the signatures and populate the reference list showing all the documents and form that were included during signing.

Viewing Signature and Signer Details

The following image shows what the main panel looks like when a signed document is opened. The top panel shows the list of signatures present in the opened document. The panel below that shows signature image if one was included during the signature creation process. Next you see a panel containing the list of documents that were signed by each signer. This will also include any template based forms.



C:\Temp\s4.sig contains following signatures

Status	Date	Signer	Comments
verified	4/15/2003 10:	User1-CP.01.01	No Comments
verified	4/15/2003 10:	DST ACES TEST CERT	This is good work.

UTC time source: SystemTime; Local time: 4/15/2003 3:36:42 PM

Signature Image

SignatureImageId = 33d92c9b-7742-41d3-b21f-7d9e7701b149

33d92c9b-7742-41d3-b21f-7d9e7701b149
Mouse Signature

Signed documents (checked = included in content)

☑ Doc1.doc
☑ Test doc2.doc

Comments: No Comments

Signature Status.

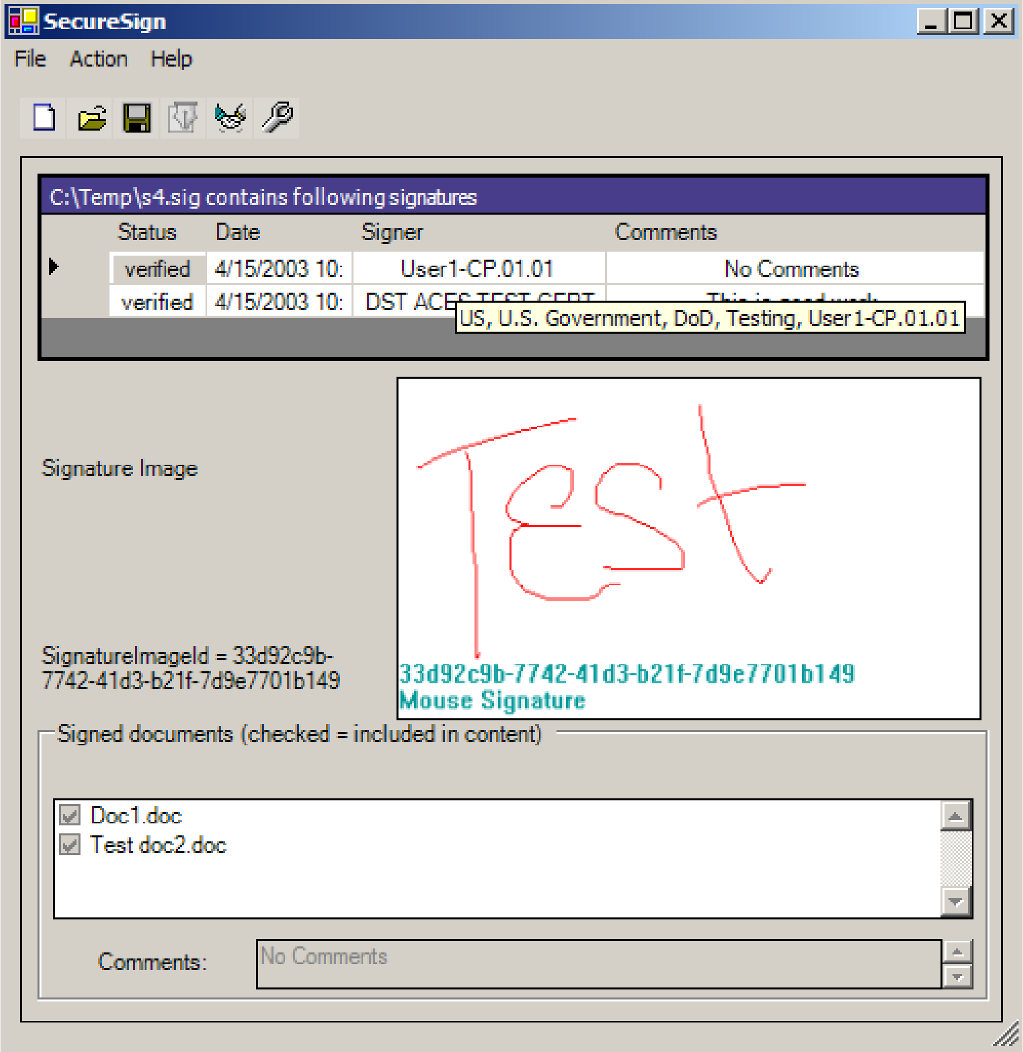
Current Signature

Date and Time (UTC) of when the signature was created.

Hovering over the Date column shows the corresponding local time and shows the source of the time. It is set to SystemTime if the local machine time was used otherwise it shows the URL of the timestamp server used for timestamping.

List of signed documents

When you hover over the Signer column, SecureSign shows you full signer subject information as shown below.



C:\Temp\s4.sig contains following signatures

Status	Date	Signer	Comments
verified	4/15/2003 10:	User1-CP.01.01	No Comments
verified	4/15/2003 10:	DST ACES TEST CERT	This is good work

US, U.S. Government, DoD, Testing, User1-CP.01.01

Signature Image

SignatureImageId = 33d92c9b-7742-41d3-b21f-7d9e7701b149

33d92c9b-7742-41d3-b21f-7d9e7701b149
Mouse Signature

Signed documents (checked = included in content)

☑ Doc1.doc
☑ Test doc2.doc

Comments: No Comments

Viewing Signed Document Contents

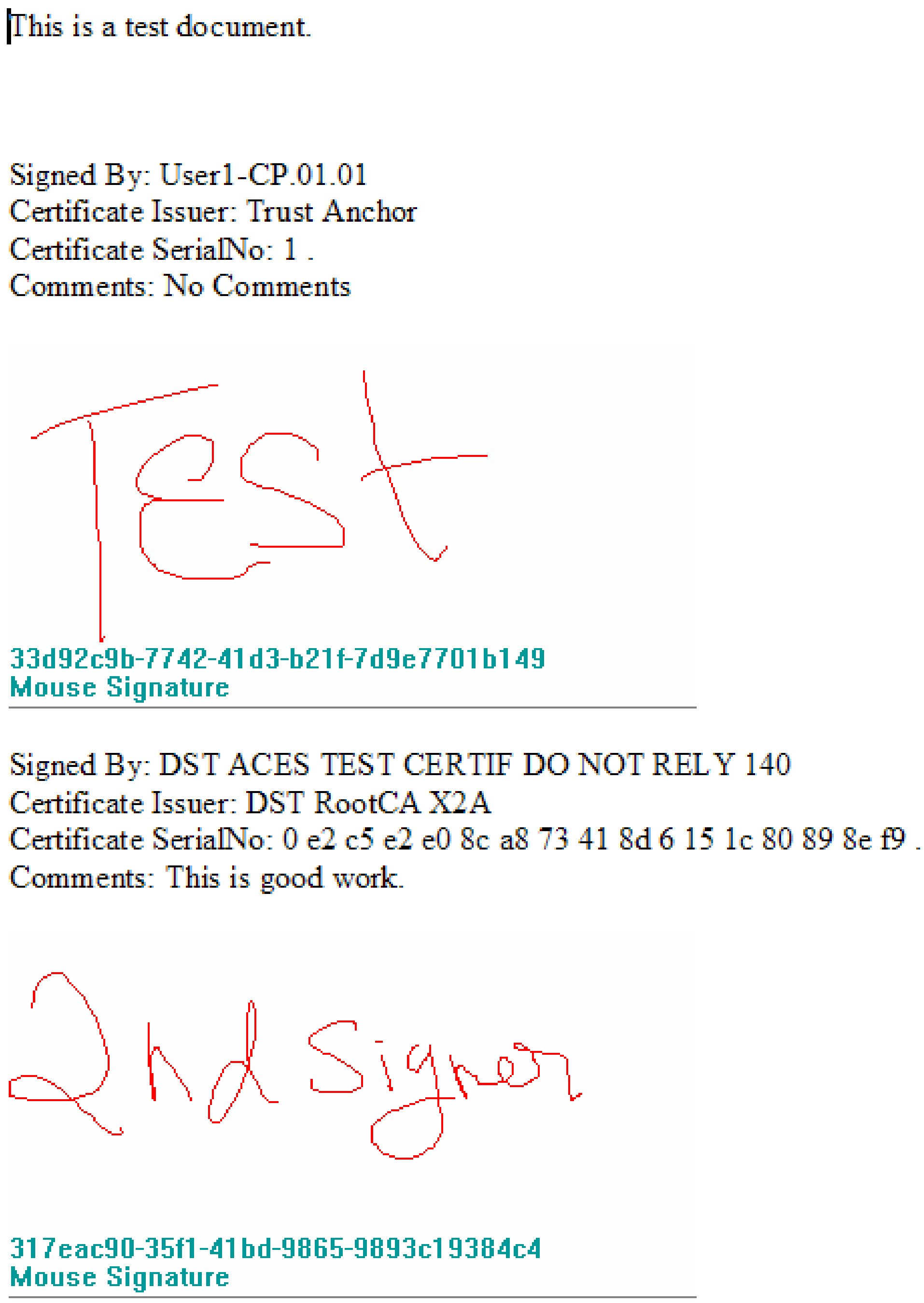
In order to access individual signed files and form, you can simply double click the item shown in the reference list panel. You can also select an item and right click to access the context menu for opening the file or viewing the form.

If the content of the .sig file was tampered with, the signature verification will fail. If the tampering was specific to a signed reference such as a signed file or a form, the reference list will tell you which of the signed references were tampered.

Special Features for Signed MS Word File Viewing

If the recipient of the signed file has MS Word XP installed on his/her computer, SecureSign puts the signer details in the signed file when opened for viewing. It allows for printing word documents with signer information in them. The following illustrations show what it may look like. The first image shows how signer information is added at the end of the signed document while the second image shows how it is added to the footer of the signed document.

Document Body Signer Annotation:



This is a test document.

Signed By: User1-CP.01.01
Certificate Issuer: Trust Anchor
Certificate SerialNo: 1 .
Comments: No Comments

Test

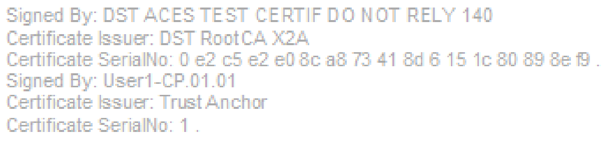
33d92c9b-7742-41d3-b21f-7d9e7701b149
Mouse Signature

Signed By: DST ACES TEST CERTIF DO NOT RELY 140
Certificate Issuer: DST RootCA X2A
Certificate SerialNo: 0 e2 c5 e2 e0 8c a8 73 41 8d 6 15 1c 80 89 8e f9 .
Comments: This is good work.

2nd Signer

317eac90-35f1-41bd-9865-9893c19384c4
Mouse Signature

Document Footer Annotation:



Signed By: DST ACES TEST CERTIF DO NOT RELY 140
Certificate Issuer: DST RootCA X2A
Certificate SerialNo: 0 e2 c5 e2 e0 8c a8 73 41 8d 6 15 1c 80 89 8e f9 .
Signed By: User1-CP.01.01
Certificate Issuer: Trust Anchor
Certificate SerialNo: 1 .