



How to make Timestamp Work with ProSigner

Table of Contents

<u>1</u>	<u>INTRODUCTION</u>	<u>3</u>
<u>2</u>	<u>REQUIREMENTS</u>	<u>3</u>
<u>3</u>	<u>STEPS TO BE FOLLOWED</u>	<u>3</u>
3.1	STEP 1: CREATION OF THE TIMESTAMP POLICY	3
	CREATING A RULE FOR A MAJOR OPERATION WITH TIMESTAMPING AS A TRIGGERED OPERATION	3
	CREATING A RULE TO ENFORCE TIME STAMPING	7
3.2	STEP 2: EXPORTING THE POLICY FROM THE POLICY MANAGER	10
3.3	STEP 3: IMPORTING THE POLICY WHERE THE PROSIGNER IS INSTALLED	11
3.4	STEP 4: CHANGES IN CONFIGURATION SETTINGS TO ENUMERATE THE POLICY DURING SIGNING/ENCRYPTION OPERATION	12
3.5	STEP 5: ATTACHING THE POLICY DURING THE ACTUAL SIGNING/ENCRYPTION PROCEDURE	13
3.6	STEP 6: SIGNATURE VERIFICATION / DECRYPTION TO SEE THE TIMESTAMP DETAILS	14

1 INTRODUCTION

This document covers in detail the steps involved in making Timestamp work with ProSigner 6.1

The steps can be broadly classified into the following different sections:

- Creation of a timestamp policy using the Policy Manager
- Exporting the policy from the Policy Manager
- Importing the Policy to the computer on which ProSigner is installed
- Enabling the display of policies (when signing) from the Configuration Manager
- Attaching the policy to a document during the actual signing/encryption procedure
- Signature verification / decryption to see the timestamp details.

2 REQUIREMENTS

The following applications are required to make timestamping work with ProSigner. These applications can be installed on the same machine or on two different machines, per your requirements.

- Policy Manager 6.1
- ProSigner 6.1

3 STEPS TO BE FOLLOWED

3.1 STEP 1: CREATION OF THE TIMESTAMP POLICY

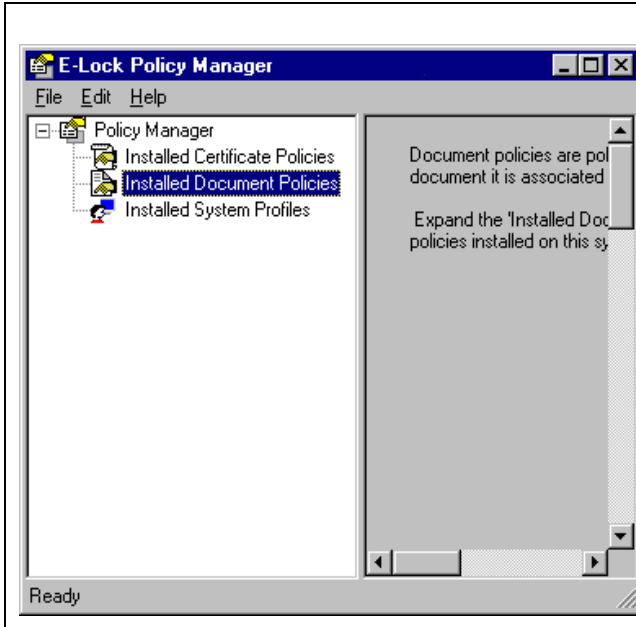
The first step is to create a timestamp policy using the Policy Manager. This creation of this policy can be divided into 2 parts:

- Create a rule for any major operation (signing or encryption) and define timestamping as a triggered operation.
- Create another rule which enforces timestamping
(In the rule define the operation as Timestamp and the Rule as Enforce)

CREATING A RULE FOR A MAJOR OPERATION WITH TIMESTAMPING AS A TRIGGERED OPERATION

On the machine where the Policy Manager application is installed, open the Policy Manager application.

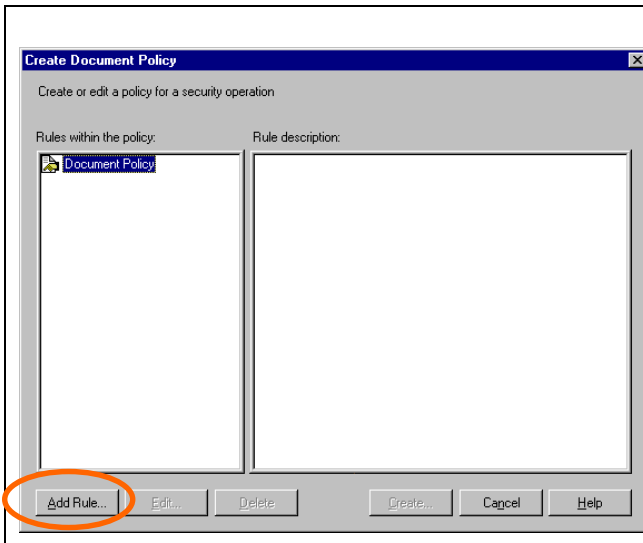
How to make Timestamp Work



Go to the File menu and select “New Document Policy”

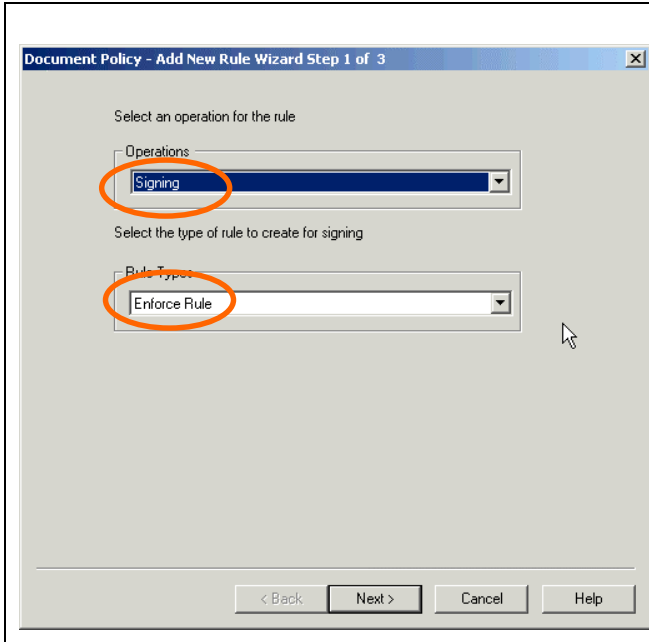
OR

Expand **Policy Manager**, right click **Installed Document Policies** and select **New Document Policy**



The **Create Document Policy** Wizard will open up. Click the “Add Rule” button

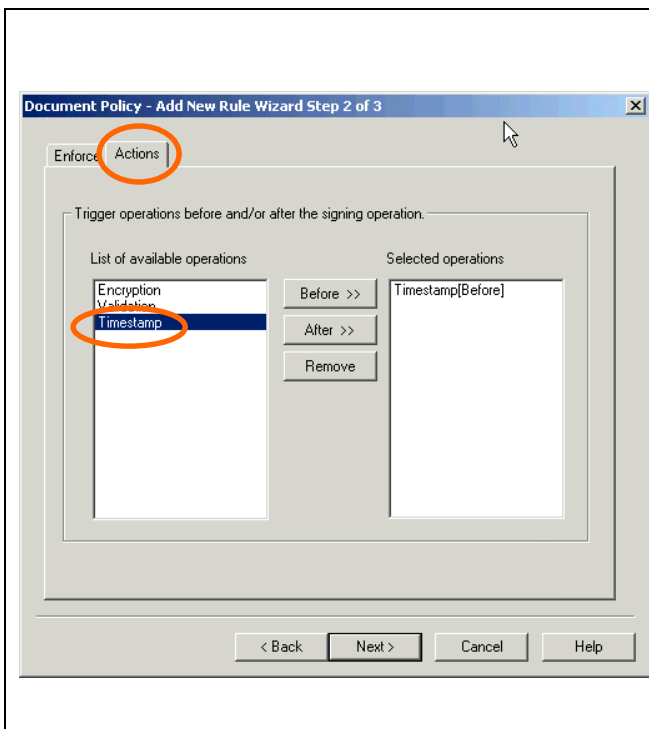
How to make Timestamp Work



(In this example, we will define **Signing** as the operation and **Enforce** as the Rule Type)

In the Add New Rule Wizard, select the operation as "Signing", and the Rule Type as "Enforce Rule"

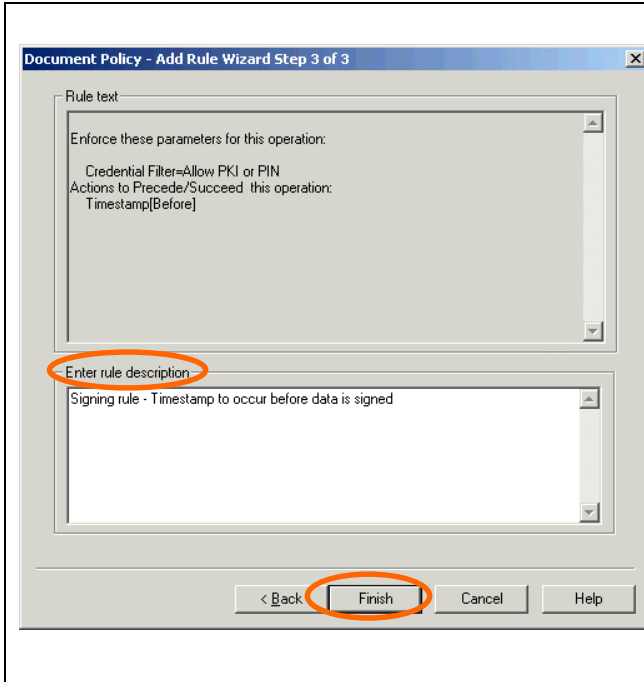
Click the Next button.



Click the Action Tab. In the list of available operations, **Timestamp** will be listed. Select this and click either **Before** or **After** per your requirements.

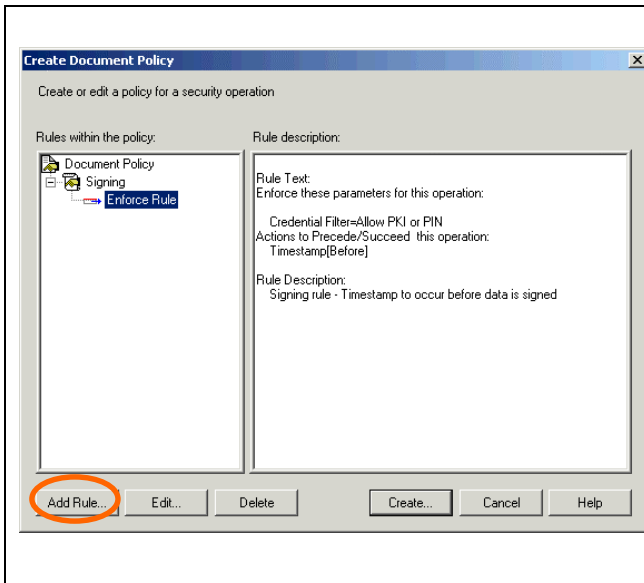
If **Before** is selected, Timestamp will occur before the data is signed, and if **After** is selected, Timestamp will occur after the data is signed. Click Next once the type of operation has been selected.

How to make Timestamp Work



In this screen, the **Rule text** will be displayed.
You can also enter a description for the Rule.

Click the “Finish” button.

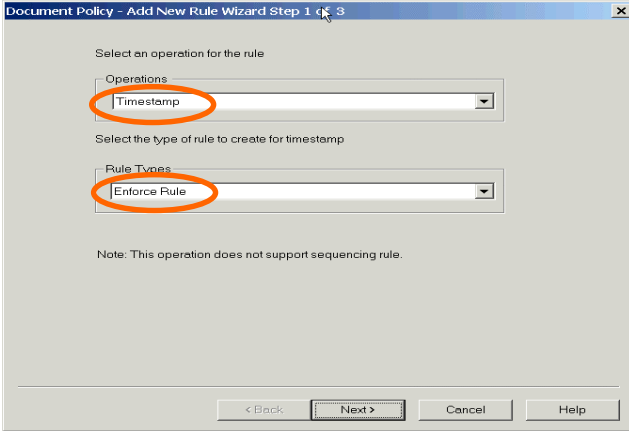


On clicking “Finish”, an **Enforce Rule** will be created for the **Signing** operation.

Now click **Add Rule** again to create a Time Stamp rule (that enforces timestamping).

How to make Timestamp Work

CREATING A RULE TO ENFORCE TIME STAMPING



Document Policy - Add New Rule Wizard Step 1 of 3

Select an operation for the rule

Operations
Timestamp

Select the type of rule to create for timestamp

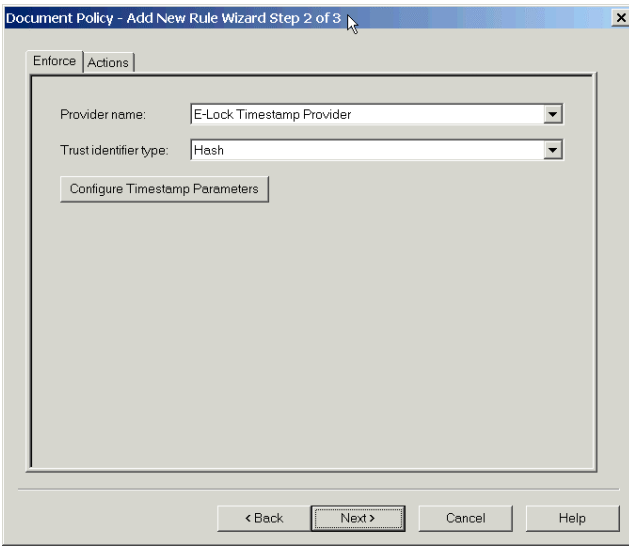
Rule Types
Enforce Rule

Note: This operation does not support sequencing rule.

< Back Next > Cancel Help

In the **Add New Rule Wizard**, select the operation as **Timestamp**, and the Rule Type as **Enforce Rule**.

Click Next.



Document Policy - Add New Rule Wizard Step 2 of 3

Enforce Actions

Provider name: E-Lock Timestamp Provider

Trust identifier type: Hash

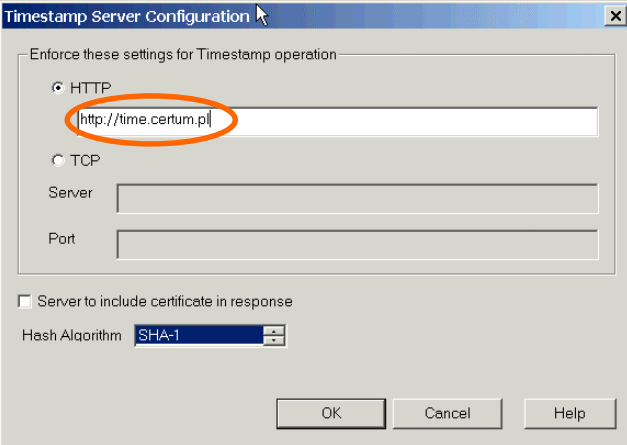
Configure Timestamp Parameters

< Back Next > Cancel Help

Select the timestamp provider and the trust identifier type.

Click on the “Configure Timestamp Parameters” to enter the Timestamp Server details.

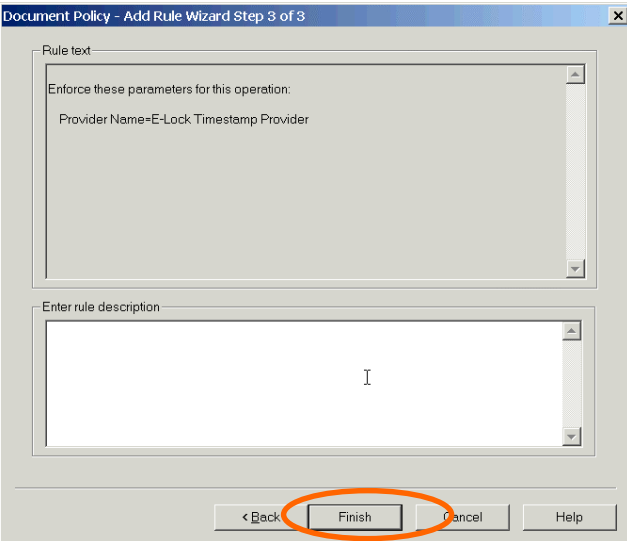
How to make Timestamp Work



The screenshot shows the "Timestamp Server Configuration" dialog box. It has a title bar with a close button. The main area is titled "Enforce these settings for Timestamp operation". There are two radio buttons: "HTTP" (selected) and "TCP". Below the radio buttons is a text input field containing "http://time.certum.pl", which is circled in orange. Below that are two empty text input fields labeled "Server" and "Port". At the bottom left, there is a checkbox labeled "Server to include certificate in response" which is unchecked. Below the checkbox is a dropdown menu for "Hash Algorithm" with "SHA-1" selected. At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

Choose the protocol (HTTP or TCP) and provide the server URL/name. Also select whichever hash algorithm is required and click OK.

Click Next when the "Add New Rule Wizard Step 2 of 3" comes up to complete the timestamp rule creation.

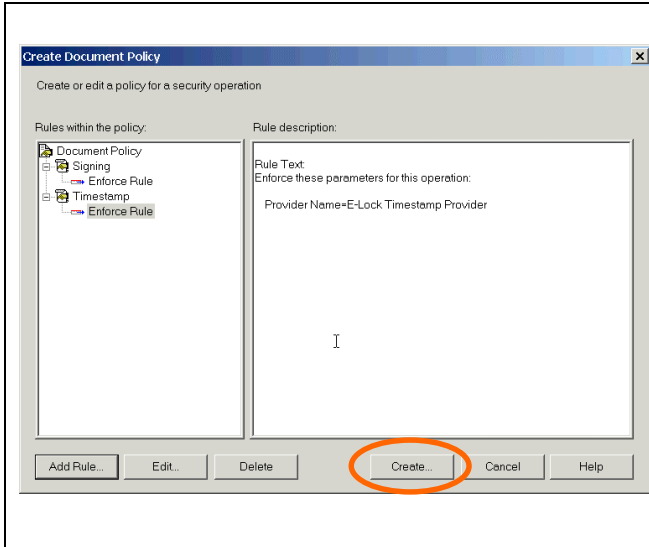


The screenshot shows the "Document Policy - Add Rule Wizard Step 3 of 3" dialog box. It has a title bar with a close button. The main area is titled "Rule text" and contains a text area with the text "Enforce these parameters for this operation:" and "Provider Name=E-Lock Timestamp Provider". Below this is another text area titled "Enter rule description" which is empty. At the bottom, there are four buttons: "< Back", "Finish" (circled in orange), "Cancel", and "Help".

In this screen, the policy rule text will be displayed, and also, you can enter any description for the policy if you want to.

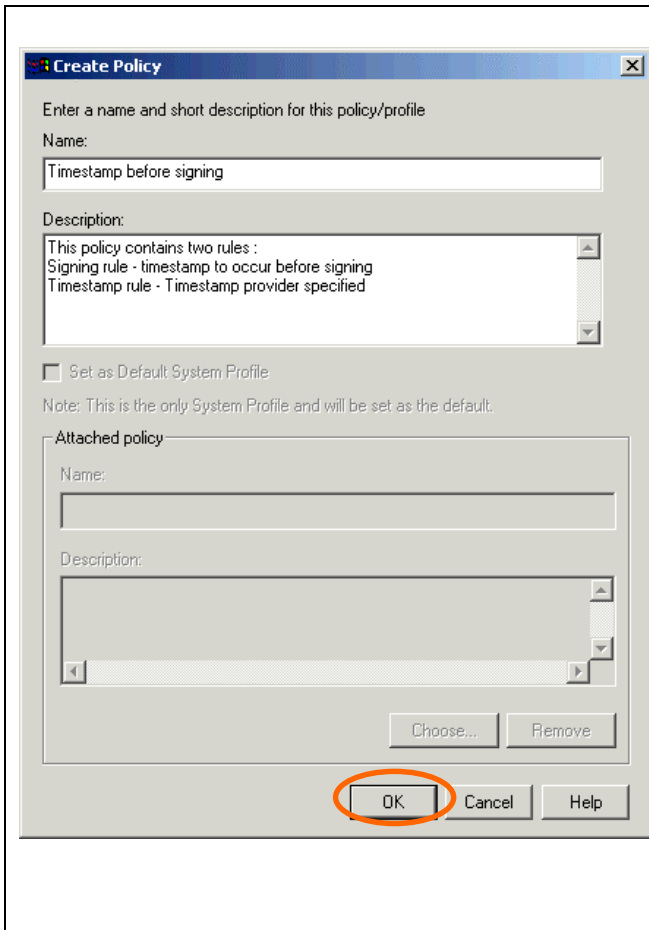
Click the "Finish" button.

How to make Timestamp Work



Now both the Signing Rule as well as the Timestamp rule has been added to the policy.

Click on the Create button to create the policy.



Give some name to the policy.

You can optionally also enter some description for the policy that is being created.

Click on the OK button

How to make Timestamp Work

Certificate Name	Issuer	Cryptographic Provider
Signer 1	E-Lock Demo Certificatio...	Microsoft Base Cryptographic...

Certificate details:

Subject: Signer 1
E-Lock Demo
Frontier Technologies Corporation
McLean, VA
US

OK Cancel Help

The policy is digitally signed. You will need to select the Certificate with which to sign the policy.

You can use any certificate ID to the sign this policy.

Click OK after selecting the signer certificate.

The timestamp policy has been successfully created.

3.2 STEP 2: EXPORTING THE POLICY FROM THE POLICY MANAGER

NOTE: This step needs to be performed only if the Policy Manager and the ProSigner applications reside on two different machines.

If the Policy Manager and the ProSigner applications are installed on two separate machines, then to use the policy created in the Step 1 of this document, it will need to be exported from the Policy Manager and then imported on the machine where the ProSigner is installed.

File Edit Help

New Certificate Policy...
New Document Policy...
New System Profile...
Refresh FS
Import Policies...
Export Policies...
Import System Information...
Refresh Crypto Information
Exit

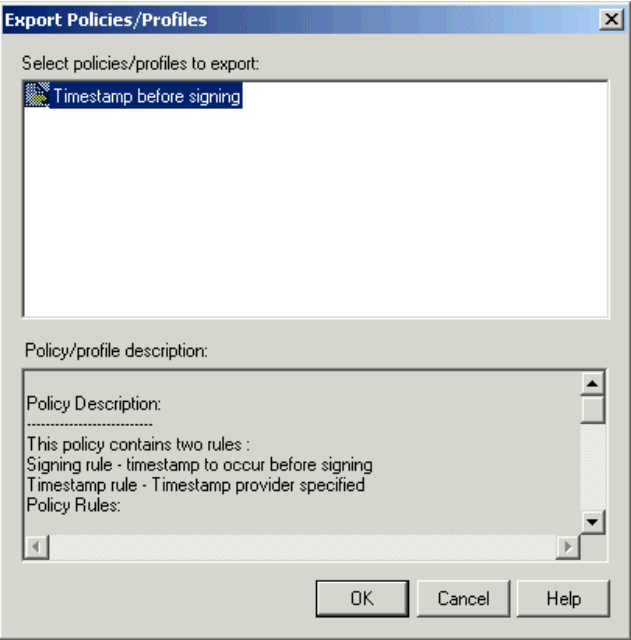
Policy Description:
This policy contains two rules:
Signing rule - timestamp to occur before signing
Timestamp rule - Timestamp provider specified

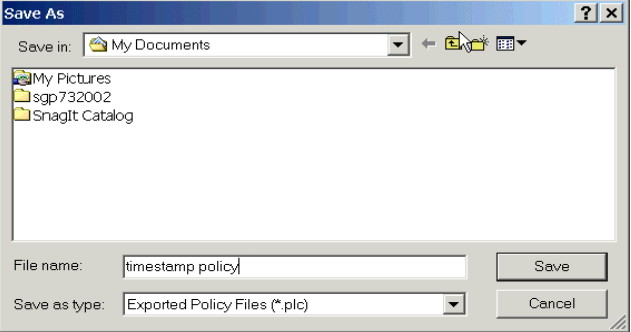
Policy Rules:
1 Rule List for the Signing Operation:
Rule Text:
Enforce these parameters for this operation:
Credential Filter=Allow PKI or PIN
Actions to Precede/Succeed this operation:
Timestamp[Before]

2 Rule List for the Timestamp Operation:
Rule Text:
Enforce these parameters for this operation:
Provider Name=E-Lock Timestamp Provider

Once the policy is created, click on File -> Export Policies in the Policy Manager application.

How to make Timestamp Work

	<p>Select the timestamp policy that was created in the Step 1 of this document.</p> <p>Click on OK.</p>
---	---

	<p>Select the folder where you want the exported policy to be saved, give some name to the exported policy file and click on Save.</p> <p>The policy will be exported and saved in the .plc format.</p> <p>A confirmatory message that the policy has been exported successfully is shown.</p>
---	--

3.3 STEP 3: IMPORTING THE POLICY WHERE THE PROSIGNER IS INSTALLED


NOTE: This step needs to be performed only if the Policy Manager and the ProSigner applications reside on two different machines.

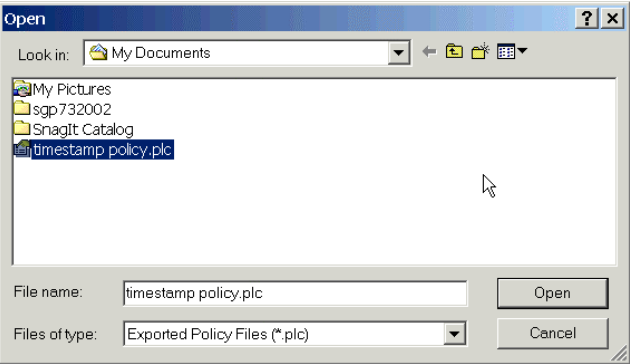
Once the policy has been exported successfully, it will have to be imported on the machine where the ProSigner is installed.

Exported policies can be imported in ProSigner using the Profile Manager application.

How to make Timestamp Work

Open the Profile Manager application from the Start, Programs, E-lock, E-Lock ProSigner menu.

	<p>In the Profile Manager application, select the File => Import Policies\Profiles option</p>
---	--

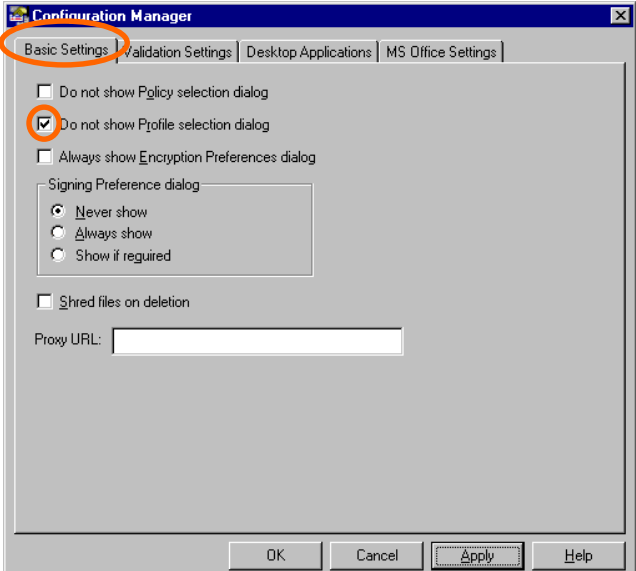
	<p>Go to the folder where the exported policy was saved, and select the exported policy file.</p> <p>The exported policy will be in a .plc format.</p> <p>A confirmatory message that the policy has been imported successfully is shown.</p>
---	---

3.4 STEP 4: CHANGES IN CONFIGURATION SETTINGS TO ENUMERATE THE POLICY DURING SIGNING/ENCRYPTION OPERATION

Now that the policy has been imported successfully, this policy can be used during the actual signing/encryption process. A small configuration change is required so that this policy can be selected during the signing process.

Open the Configuration Manager application from the Start—Programs—E-Lock—E-Lock ProSigner menu.

How to make Timestamp Work

 <p>The screenshot shows the 'Configuration Manager' dialog box with the 'Basic Settings' tab selected. The 'Do not show Policy selection dialog' checkbox is unchecked, and the 'Do not show Profile selection dialog' checkbox is checked. The 'Apply' button is highlighted with a red box.</p>	<p>On the “Basic Settings” Tab, de-select the option “Do not show policy selection dialog”.</p> <p>Click on the Apply button.</p> <p>Now during the signing operation, the policy selection dialog box will come up, and all the policies present on the system will be enumerated.</p>
---	---

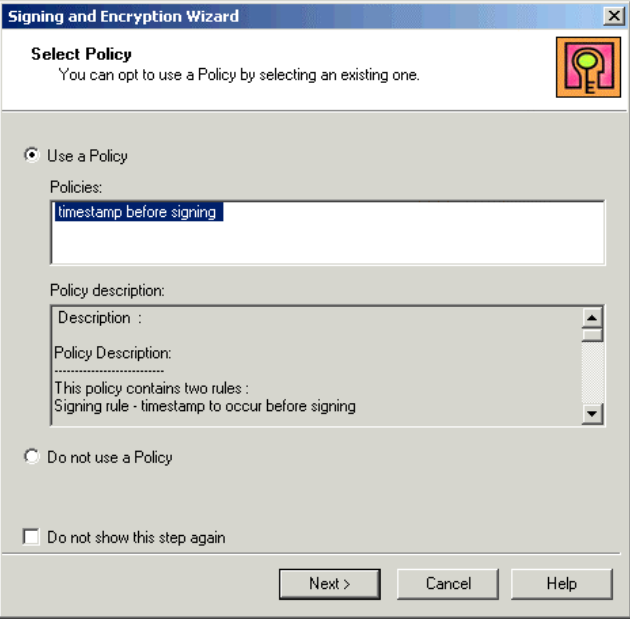
3.5 STEP 5: ATTACHING THE POLICY DURING THE ACTUAL SIGNING/ENCRYPTION PROCEDURE

The timestamp policy created in step 1 of this document can now be attaching during the signing/encryption operation.

In your application (MS Word/Excel or e-Sign), select the file and start the signing process.

The select policy dialog comes up.

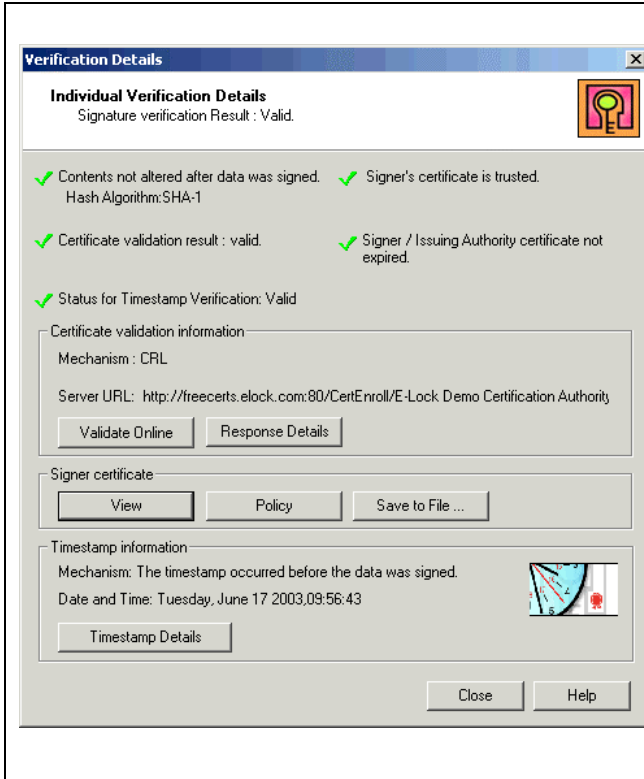
How to make Timestamp Work

	<p>During the Signing operation, the Select Policy option will come. Select the policy that you had earlier created in the Policy Manager. The description of the policy will be shown in the policy description part.</p> <p>Select this policy and click Next.</p> <p>Follow the Signing and Encryption Wizard and complete the signing process.</p>
---	--

3.6 STEP 6: SIGNATURE VERIFICATION / DECRYPTION TO SEE THE TIMESTAMP DETAILS

Now verify the document signed in step 5 to see the timestamp details.

How to make Timestamp Work



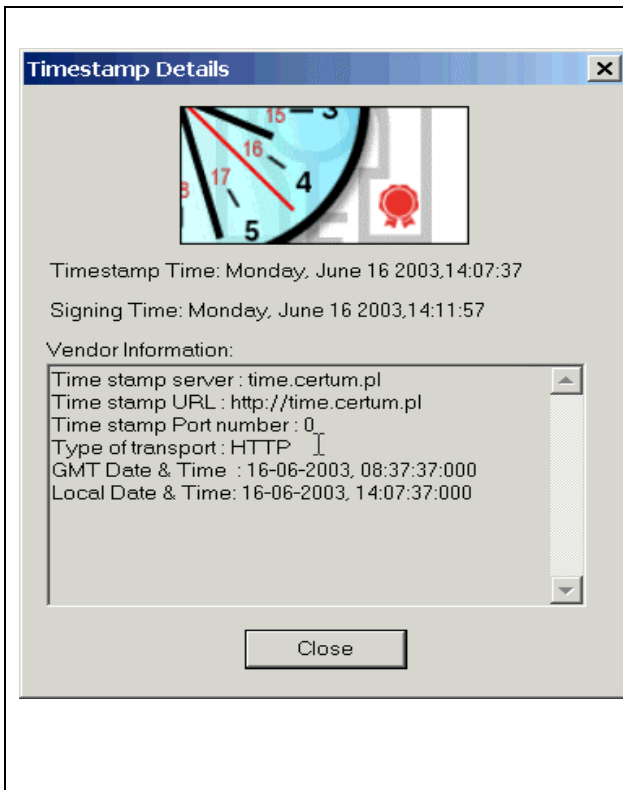
The verification result will come up.

Select the signature and click on Verification Details.

The Timestamp Verification shows as Valid

The mechanism specifies that the timestamp occurred before the data was signed.

In the "Timestamp Information", click on Timestamp Details to see additional information of the Timestamp Vendor



The Timestamp Details shows additional information including the Timestamp Vendor information.