E-Lock Policy Manager
White Paper

Table of Contents

1 INTRODUCTION

In business, security forms a major concern for any organization. With the economy shifting towards e-business, the use of digital signature technology has become imperative for providing the necessary trust and security. Depending on the transaction or the value of the electronic business process, organizations may have set rules or policies for security.

It is necessary that users comply with these policies. E-Lock's Policy Manager helps organizations to define policies for digital signatures and attach them to the transactions, which enforces user compliance with set rules.

2 ABOUT THE POLICY MANAGER

E-Lock Policy Manager is a component that works in conjunction with E-Lock ProSigner. Using the Policy Manager you can define policies and attach them to documents. When documents are signed using ProSigner, users will be forced to comply with the conditions in the policy. Policy Manager also allows you to create enterprise-wide user settings – System Profiles – that can be used by all users in an organization when they perform security (signing/encryption) operations.

For example if a Policy states that users can sign using only certificates from particular CSP, they will not be able to sign with any other certificates. This ensures that organizational procedures are enforced without having to depend on user compliance.

Policies can be created by the Policy Administrator and exported, and then imported by the person responsible for the document. That person can then attach the policy to the document, and route it.

3 HOW E-LOCK POLICY MANAGER WORKS

The Policy Manager lets you define "Rules" which comprise the policy. There are 2 types of Rules:

- **Enforce Rules** – through which you can enforce parameters for signing, encryption, validation and time stamping. You also trigger operations through the Enforce Rule.
- **Sequence Rules** – through which you can define the signing sequence.

Enforce Rules ensure that conditions specified are enforced during a security operation. For example, an enforce rule could require a signature image (digitized signature) be included with the digital signature in order for the signing operation to be accepted. It is important to note that multiple attributes can be selected within an enforce rule, and implemented for a particular user or group of users conducting security operations.

Sequence Rules specify a particular sequence of users to conduct a signing operation and ensures the process will not be completed unless the defined sequence is followed. For instance, in the case of a large commercial loan, a sequence rule could dictate that a loan officer not be allowed to approve the loan unless authorized by the loan issuance manager. In other words, E-Lock ProSigner would not allow the loan officer to sign the document until the loan issuance manager had already signed it.

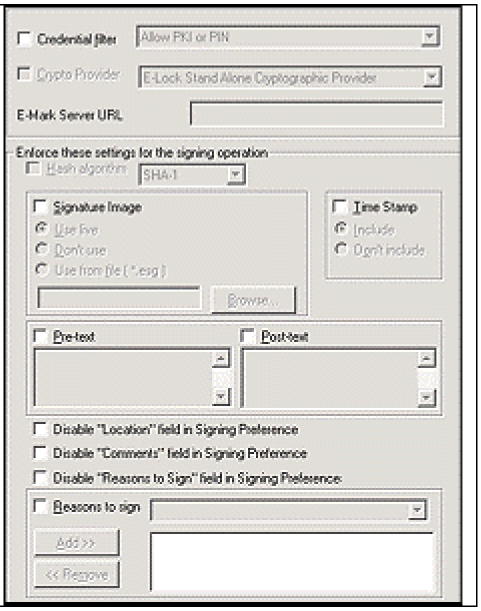
4 WHAT CAN I DO WITH THE POLICY MANAGER?

Using the Policy Manager you can control the following operations:

- Signing
- Encryption
- Validation
- Time Stamping

4.1 THINGS YOU CONTROL IN SIGNING

- The Signing Sequence
- The Signing Parameters
  - Hash algorithm
  - Signature image
  - Defining Reasons to Sign
  - Disabling Signing Reasons, Comments and Location (enabled by default)
  - Pre and Post Text
  - Allowing users to sign using certificates, credentials (Non-PKI) or both

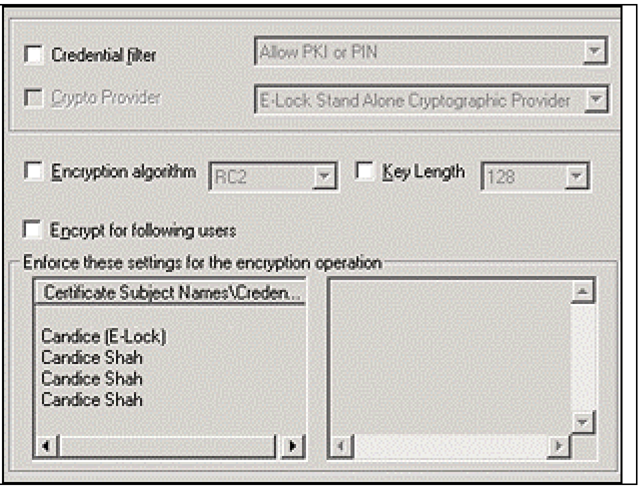


☐ Credential filter: Allow PKI or PIN
☐ Crypto Provider: E-Lock Stand Alone Cryptographic Provider
E-Mark Server URL:

Enforce these settings for the signing operation
☐ Hash algorithm: SHA-1
☐ Signature Image: ● Use live ○ Don't use ○ Use from file (*.esg)
☐ Time Stamp: ● Include ○ Don't include
☐ Pre-text
☐ Post-text
☐ Disable "Location" field in Signing Preference
☐ Disable "Comments" field in Signing Preference
☐ Disable "Reasons to Sign" field in Signing Preference
☐ Reasons to sign

4.2 THINGS YOU CAN CONTROL IN ENCRYPTION

- Encryption Parameters
  - Allowing users to encrypt using certificates, credentials (Non-PKI) or both
  - Crypto Provider
  - Encryption algorithm and key length
  - The persons to encrypt for

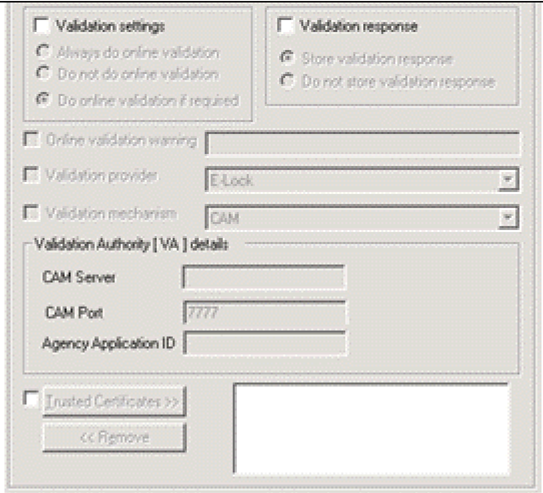


☐ Credential filter: Allow PKI or PIN
☐ Crypto Provider: E-Lock Stand Alone Cryptographic Provider
☐ Encryption algorithm: RC2 ☐ Key Length: 128
☐ Encrypt for following users

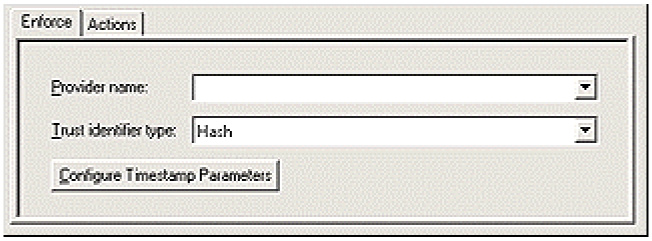
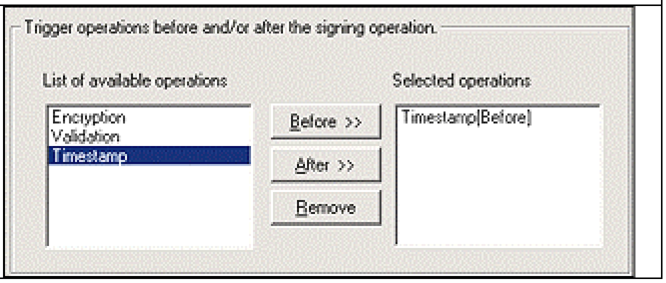
Enforce these settings for the encryption operation

Certificate Subject Names\Creden...
Candice (E-Lock)
Candice Shah
Candice Shah
Candice Shah

4.3 THINGS YOU CAN ENFORCE IN VALIDATION

• Whether to perform online validation always, never or if necessary • The validation provider • Whether to store validation responses • Validation warnings • The validation mechanism • The VA Details • Trusted Certificates	 ☐ Validation settings ○ Always do online validation ○ Do not do online validation ● Do online validation if required ☐ Validation response ● Store validation response ○ Do not store validation response ☐ Online validation warning ☐ Validation provider E-Lock ☐ Validation mechanism CAM Validation Authority [VA] details CAM Server CAM Port 7777 Agency Application ID ☐ Trusted Certificates >> << Remove

4.4 THINGS YOU CAN ENFORCE IN TIMESTAMPING

You first need to create a rule to define the timestamp provider and optionally check for the authenticity of the time stamp client.	 Enforce | Actions Provider name: Trust identifier type: Hash Configure Timestamp Parameters
Once you create this rule, you can trigger time stamping on or before signing / encryption.	 Trigger operations before and/or after the signing operation. List of available operations Encryption Validation Timestamp Before >> After >> Remove Selected operations Timestamp[Before]

4.5 TRIGGERED OPERATIONS

Certain security operations can be specified as triggered operations. What this means is that operation will be performed automatically on performing some other operation. For example you can specify that after a certain document is signed, it needs to be encrypted for confidentially – in this case, encryption is the operation triggered on signing.

Also, validation or time stamping can be specified as the operation triggered on signing. Therefore, whenever a signing operation occurs, validation or time stamping will follow.

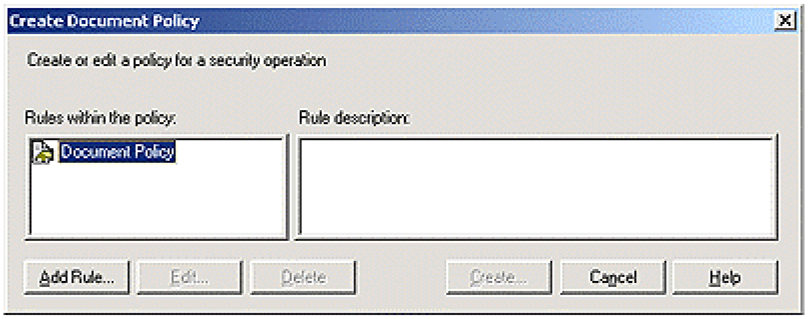
The triggered operation can be specified as either a pre or post operation.

5 TYPES OF POLICIES THAT CAN BE CREATED

E-Lock Policy Manager allows you to create two types of policies:

5.1 DOCUMENT POLICIES

Policies created and attached to electronic documents. Attaching these policies ensures that whenever a security operation is performed on the document or the transaction, it is governed by the rules and statements defined within the policy. This makes certain that the document or transaction follows the security life cycle as defined by the organization.

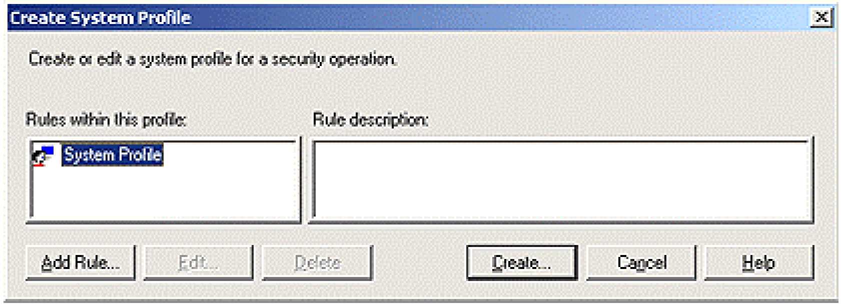


Create or edit a policy for a security operation

5.2 SYSTEM PROFILES

System Profiles provide a pre-selection of settings based on the settings defined in the profile. The purpose of a system profile is to pre select and store some settings that will be used as default, in the absence of a defined user profile or policy. User Profiles take precedence over System Profiles, and Policies take precedence over User Profiles.

The settings defined in the system profile will be pre-selected and displayed to the user when signing or encrypting, but the user has the choice to change any of the settings. If you always want these settings to be used, without giving the user the option to make any changes, you can set rules for these settings in a Policy and attach it to a System Profile.



Create or edit a system profile for a security operation.

Note: System Profiles differ from User Profiles created using the Profile Manager. While user profiles are a collection of commonly used settings for a particular user, the system profile contains settings that will be default if no user profile or policy is selected.

6 DEPLOYMENT OF POLICIES

The following are options for deployment of the policy manager:

- The Policy Administrator can create the policy, export it and send it to the user(s) who can then import the policy and attach it to the document.

- The Policy Administrator can create policies and store them on a shared network drive. In an enterprise-wide deployment, ProSigner can be installed in such a way that it always refers to the shared network drive to locate the polices to be used.

  To do this: Install ProSigner with the following command line parameter
  setup.exe /z"-p<shared_path>"
  Where <shared_path> is the complete path (including the drive letter) to the shared location for policies.

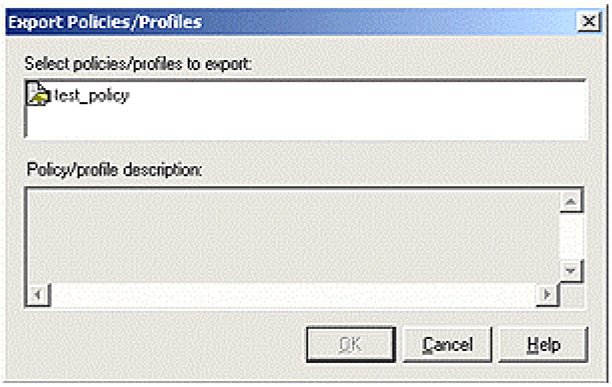
E-Lock Policy Manager is typically installed and used only on the Policy Administrator's machine. The administrator can then create policies and profiles that can be deployed on a per-user basis, or organizational-wide.

Once Administrators create policies, they need to distribute them to users in the organizations. To do so, the Administrator needs to export the policies, and users can then import them and start using them.

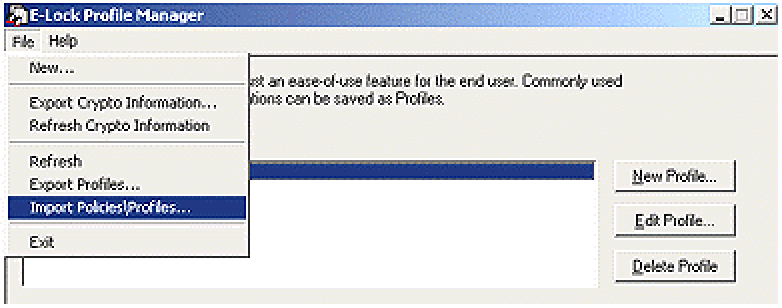
6.1 STEPS TO EXPORT POLICIES – FOR ADMINISTRATORS

- Open the Policy Manager, go to the File Menu
- Select Export Policies
- Select the Policy to export and Click OK
- You will then be promoted to choose a location to save the policy locally on your PC
- Save the Policy

You can either save the policy on a network drive or a location from where it will be accessible to users or you can email the policy to the user. If received via email., users need to save the policies locally on their PCs so they can later import them.


Export Policies/Profiles
Select policies/profiles to export:
test_policy
Policy/profile description:
OK
Cancel
Help

6.2 STEPS TO IMPORT POLICIES – FOR USERS

• Open the Profile Manager, go to the File Menu • Select Import Profiles/Policies • Chose the policy from your local computer • Click OK – you will then get a message that the policy has been installed	 E-Lock Profile Manager File Help New... Export Crypto Information... Refresh Crypto Information Refresh Export Profiles... Import Policies\Profiles... Exit New Profile... Edit Profile... Delete Profile st an ease-of-use feature for the end user. Commonly used tions can be saved as Profiles.

7 SUMMARY– POLICIES PROVIDING TAILORED SIGNING SOLUTIONS

Organizations adopting an E-Lock Digital Signature solution can confidently deploy the solution in a tailored fashion, with all of the security operations pre-configured by an administrator for individual users and/or groups of users. E-Lock Policy Manager also enables deployment and heightened adoption rates by end users as a result of the central administration and distribution of tailored signing processes.

Without use of a “Security Manager” such as the E-Lock Policy Manager, users are free to conduct a variety of security operations, creating legal and monetary implications for the organization or person(s) they represent. Even if no plausible harm or malicious tactics are meant by users conducting these security operations, without enforcement of any guidelines, the effect can be quite harmful, creating a costly barrier for organizations migrating to a paperless environment.

The E-Lock Policy Manager lifts this barrier through its enforcement of end-user compliance in conducting a variety of security operations, such as digital signatures and encryption.

E-Lock’s Digital Signature solutions operate based on rules enforced as E-Lock Policies – clearly instituting the key factors of data integrity, data confidentiality, non-repudiation, and above all, establishing a framework for “trust” in paperless transactions.

Please contact Sales@elock.com for more information.