



Running E-Lock ProSigner on a Windows 2000 Terminal Server

Table of Contents

1	<u>INTRODUCTION.....</u>	<u>2</u>
2	<u>INSTALLING USER DIGITAL CERTIFICATES ON WINDOWS 2000 SERVER</u>	<u>2</u>
3	<u>CONFIGURING E-LOCK PROSIGNER FOR INDIVIDUAL USERS</u>	<u>3</u>
4	<u>USING INDIVIDUAL PROFILES IN E-LOCK PROSIGNER</u>	<u>3</u>
5	<u>ASSOCIATING HANDWRITTEN SIGNATURES WITH DIGITAL SIGNATURES FOR INDIVIDUAL USERS.....</u>	<u>3</u>
6	<u>VERIFYING DOCUMENTS IN E-LOCK PROSIGNER THROUGH A TERMINAL SESSION.....</u>	<u>4</u>
7	<u>USING POLICIES IN E-LOCK PROSIGNER ON WINDOWS 2000 TERMINAL SERVER</u>	<u>4</u>

1 INTRODUCTION

Windows 2000 Server includes terminal services for the purpose of remote administration of servers as well as the ability to provide centralized access to software and the Windows 2000 desktop.

Terminal services provide an environment that is often referred to as 'thin client' (not installed by default). In this environment (also provided by third-party products such as Citrix Metaframe), only screen-shots, keyboard strokes, and mouse movements are passed between the server and the client. All processing actually takes place on the server, which greatly reduces the computing requirements on the client side. As such, even Intel 386 running Windows 3.11 can provide users with access to the Windows 2000 environment and associated applications. Terminal services use the **Remote Desktop Protocol** (RDP) to pass data between the terminal service client and server.

E-Lock ProSigner as an application can be used on a Windows 2000 Terminal Server and be accessed by multiple users simultaneously to perform digital signature operations on different files and through Office and Adobe applications

2 INSTALLING E-LOCK PROSIGNER ON WINDOWS 2000 SERVER

It is important to note that the Windows 2000 Server should be configured as a Terminal Server **before** installing E-Lock ProSigner. A user that has administrative rights on the server should install E-Lock ProSigner on the server.

3 INSTALLING USER DIGITAL CERTIFICATES ON WINDOWS 2000 SERVER

Users' certificates can reside either in the **Microsoft Certificate store or the Netscape Certificate store**. In case of Microsoft Certificate Store, each logged on user will be able to access only certificates installed for them. This means that digital certificates should be installed on the server after logging in as that particular user. This provides safety in a shared environment, whereby users will not have access to each other's private keys.

In case of **Netscape Certificate Store**, a different profile should be created for each user. The users should install their certificates from within their own profiles. Each profile is password protected and as a result, different users will not have access to other users certificates.

Since E-Lock ProSigner directly picks up certificates from the security framework certificate stores, it provides a greater level of security as compared to other products, which store their certificates in a file-based system.

4 CONFIGURING E-LOCK PROSIGNER FOR INDIVIDUAL USERS

E-Lock ProSigner's configuration manager stores each user's settings individually. So a particular user may have a setting to insert bitmaps in Word documents on signing of such documents while another may set it to not insert bitmaps in Word documents. Again, E-Lock ProSigner is the only product, which allows for configuring the user of ProSigner per individual needs.

5 USING INDIVIDUAL PROFILES IN E-LOCK PROSIGNER

E-Lock ProSigner allows for creation of user profiles, which enable using stored or pre-selected settings for signing and encryption for each user. Such profiles, again, are stored in users' individual profile folders and can be accessed only by the associated user.

Administrators can create such profiles for each user (to make it simple for the user to perform these operations) and the user can then just select the profile while signing or encrypting.

6 ASSOCIATING HANDWRITTEN SIGNATURES WITH DIGITAL SIGNATURES FOR INDIVIDUAL USERS

E-Lock ProSigner Add-On allows for associating handwritten signatures with digital signatures. This is done through the E-Mark Capture component of the E-Mark application (part of the ProSigner Add-On).

To create handwritten signatures using Wintab compliant devices, users need to have access to a machine where E-Lock ProSigner is installed with the Wintab compliant device. Users can then create the handwritten signature files (.esg) on that machine and then copy these files on the Windows Terminal Server. While signing, users can then select these signature files (.esg) to associate them with their digital signatures.

To provide extra security, these signature files can be encrypted using the public certificates of individual users so only that user will be able to decrypt and use the file while signing. Please

note that for obvious reasons, live (at runtime during signing) handwritten signatures cannot be created with Wintab compliant devices used in a Windows Terminal Server environment.

7 VERIFYING DOCUMENTS IN E-LOCK PROSIGNER THROUGH A TERMINAL SESSION

E-Lock ProSigner creates a folder called 'crlcache' to store CRLs (till their expiry) to prevent unnecessary fetching of CRLs. This allows users to perform Offline verification. This folder is created under the Winnt\System32 folder. Since by default users do not have write permission to this folder, offline verification will not work for users through terminal sessions.

To overcome this problem, after installation of E-Lock ProSigner, the administrator can create a folder called 'crlcache' under winnt\system32 folder. Users should be given the rights to modify this folder. Now users will be able to perform offline verification through the terminal session.

8 USING POLICIES IN E-LOCK PROSIGNER ON WINDOWS 2000 TERMINAL SERVER

Policies are created using E-Lock Policy Manager. These policies can be imported using E-Lock ProSigner through the Profile Manager. Since policies are usually made for enforcing enterprise rules, they are common across all the users and made available to all by storing them in a common folder – ATS Policies under winnt\system32.

Again, users will not be able to import policies since they do not have rights to this folder for writing. But they will be able to use policies that are imported and stored here. It is recommended that the administrator for use should import policies by all the users.