eSigner 4.2 for Windows

Installation and User’s Guide
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms’ resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© Copyright 2008-12 Gemalto N.V. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

GEMALTO, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.
Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90


www.gemalto.com
# Contents

<table>
<thead>
<tr>
<th>Preface</th>
<th>vi</th>
</tr>
</thead>
<tbody>
<tr>
<td>eSigner</td>
<td>vi</td>
</tr>
<tr>
<td>Who Should Read This Book</td>
<td>vi</td>
</tr>
<tr>
<td>Documentation</td>
<td>vi</td>
</tr>
<tr>
<td>For Further Help</td>
<td>vi</td>
</tr>
<tr>
<td>If You Find an Error</td>
<td>vii</td>
</tr>
</tbody>
</table>

## Chapter 1  The eSigner 4 Plug-in  1

- About eSigner | 1
- The eSigner Plug-in | 1
- eSigner IdenTrust and/or Corporate Mode | 2
  - Corporate Mode | 2
  - IdenTrust Mode | 2
- The eSigner Graphical User Interface | 3
- About DDA Shortcuts | 5
- About Signing Documents | 6
  - What You See is What You Sign | 6
  - Signature Policy | 6
- About MIME Type Features | 7
- About PINs | 7
- About Certificates | 8
  - Certificate Validation | 8

## Chapter 2  Installation  9

- System Requirements | 9
- Before Installing | 9
- Installation Methods | 9
  - Network Availability | 9
  - “Silent” Installation | 9
- Installation | 10
  - Installing eSigner at the Administrator Level | 10
  - Installing eSigner at the User Level | 10
- Uninstalling eSigner | 13

## Chapter 3  User Tasks  14

- Using the DDA Shortcuts | 14
- Making the eSigner Window Active in Order to Enter a Shortcut Sequence | 14
- Using Shortcuts to Choose Options in Menus | 15
- Using Shortcuts in the Select Certificate Window | 16
- Using Shortcuts With the Virtual PIN Pad | 16
- Entering the User PIN | 17
- Using a Regular Smart Card Reader | 17
<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using a PIN Pad Reader</td>
</tr>
<tr>
<td>Entering an Incorrect PIN</td>
</tr>
<tr>
<td>Changing the User PIN</td>
</tr>
<tr>
<td>Finding Out Which Version of eSigner You Are Using</td>
</tr>
<tr>
<td>Changing Modes in the IdenTrust Version of eSigner</td>
</tr>
<tr>
<td>Signing Documents</td>
</tr>
<tr>
<td>Signing Text and Other Document Files in the eSigner Window</td>
</tr>
<tr>
<td>Signing Text and Other Document Files in an External Window</td>
</tr>
<tr>
<td>Signing Text and Other Document Files in Button Mode</td>
</tr>
<tr>
<td>Uploading Signed Local Documents</td>
</tr>
<tr>
<td>Saving Documents</td>
</tr>
<tr>
<td>Selecting Smart Card Slots</td>
</tr>
<tr>
<td>Printing Documents</td>
</tr>
<tr>
<td>Selecting Certificates</td>
</tr>
<tr>
<td>Viewing Certificates</td>
</tr>
<tr>
<td>Chapter 4 Troubleshooting</td>
</tr>
<tr>
<td>Initialization Problem</td>
</tr>
<tr>
<td>Certificate Problems</td>
</tr>
<tr>
<td>Software Problems</td>
</tr>
<tr>
<td>System Problems</td>
</tr>
<tr>
<td>Appendix A Security Basics</td>
</tr>
<tr>
<td>Certificates</td>
</tr>
<tr>
<td>What is a digital certificate?</td>
</tr>
<tr>
<td>What is a Certificate Authority?</td>
</tr>
<tr>
<td>Signatures</td>
</tr>
<tr>
<td>What is a digital signature?</td>
</tr>
<tr>
<td>PKCS# 11 Libraries</td>
</tr>
<tr>
<td>What is a PKCS# 11 Library?</td>
</tr>
<tr>
<td>Smart Cards</td>
</tr>
<tr>
<td>What is a Smart Card?</td>
</tr>
<tr>
<td>What Is the Classic TPC Smart Card?</td>
</tr>
<tr>
<td>What is On Board Key Generation?</td>
</tr>
<tr>
<td>Increased Certificate Storage</td>
</tr>
<tr>
<td>Terminology</td>
</tr>
<tr>
<td>Abbreviations</td>
</tr>
<tr>
<td>Glossary</td>
</tr>
</tbody>
</table>
List of Figures

Figure 1 - eSigner Displayed Inside Web Browser ........................................... 3
Figure 2 - eSigner Displayed in a Pop-up Window ............................................. 4
Figure 3 - General View ...................................................................................... 5
Figure 4 - Viewer Error Message ......................................................................... 6
Figure 5 - Add or Remove Programs Window .................................................... 13
Figure 6 - DDA Shortcuts for Menus .................................................................. 15
Figure 7 - DDA Shortcut for Menu Options ....................................................... 15
Figure 8 - Select Certificate Dialog Box ............................................................... 16
Figure 9 - Keyboard PIN Entry Dialog Box ......................................................... 16
Figure 10 - Keyboard PIN Entry Dialog Box ...................................................... 17
Figure 11 - Keyboard PIN Entry Dialog Box ...................................................... 17
Figure 12 - PC Pinpad Secure PIN Entry Window ............................................... 18
Figure 13 - PIN Entry - Out of Time Message .................................................... 18
Figure 14 - Incorrect PIN Entry Using PIN Pad .................................................. 19
Figure 15 - About eSigner Information ................................................................. 20
Figure 16 - Signing a Document ......................................................................... 21
Figure 17 - Data Too Large to Display - Sign Button Disabled ............................. 22
Figure 18 - External Window With View Data Button ......................................... 22
Figure 19 - External Window With Hyperlink ..................................................... 23
Figure 20 - Uploading Signed Local Documents ................................................ 24
Figure 21 - Uploading Signed Local Documents (eSigner Window) .................... 25
Figure 22 - Uploading Signed Local Documents (Hyperlink for External Window) 25
Figure 23 - Save File Window ............................................................................. 26
Figure 24 - Save after Signing Icon ..................................................................... 27
Figure 25 - Saving Signature File Window ............................................................ 27
Figure 26 - Select a Reader ................................................................................ 28
Figure 27 - Select Certificate Dialog Box ............................................................. 29
Figure 28 - Certificate Viewer - General Tab ...................................................... 30
Figure 29 - Certificate Viewer - Details Tab ........................................................ 31
Figure 30 - Certificate Viewer - Certification Path ............................................. 31
Figure 31 - Viewer Error Message ...................................................................... 34
Figure 32 - PKCS#11 Error - Web Site Not Trusted ........................................... 36

List of Tables

Table 1 - MIME Types Available in Corporate Mode ........................................... 2
Table 2 - MIME Types Available in IdenTrust Mode ......................................... 3
Table 3 - DDA Shortcut Sequences .................................................................. 15
eSigner

eSigner is a multi-faceted software solution that addresses the needs of the business world and the stand-alone end user in guaranteeing the security of Internet transactions.

When installed as a plug-in in the user's Internet browser, it allows a Web site to submit data that is to be signed to the user. The digital certificates stored in the user’s smart card can:

- Display data on a computer and sign it
- Generate digital signatures S/MIME PKCS#7 format
- Perform some verifications locally on the client side:
  - Check hashes
  - Check certificate expiration
  - Check certificate chain

eSigner supports Gemalto Smart Cards and Readers. It also supports the following plug-ins:

- Netscape Plug-in Application Programming Interface (NPAPI)
- ActiveX (IdenTrust version in IdenTrust mode only)
- Java (IdenTrust version in IdenTrust mode only)

Who Should Read This Book

The eSigner Installation and User Guide is intended for users of the software who will be performing the common tasks of end users. It may also be used by an administrator, who may wish to install the software.

Documentation

eSigner documentation includes:

- eSigner for Windows Installation and User’s Guide (this document)
- eSigner for Windows Integration Guide (not useful for end users)
- Classic Client User Guide
- ReleaseNotes.pdf. A separate file is included with each eSigner software release version and contains the complete version history.

eSigner documentation is available as .pdf document files. These .pdf files are provided alongside the eSigner package.

These files can be printed out or read on screen using the Adobe Acrobat Reader.

To obtain the Adobe Acrobat Reader, you can download it from Adobe’s Web site at: www.adobe.com.

These files are best viewed with the Acrobat Reader, version 7.0 or later.
Typographical Conventions
This documentation uses the following typographical conventions to assist the reader of this document.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Courier</td>
<td>transaction</td>
<td>Code examples.</td>
</tr>
<tr>
<td>Bold</td>
<td>Enter myscript.dll</td>
<td>Actual user input or screen output.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Select File &gt; Open</td>
<td>Indicates a menu selection. In this example you are instructed to select the “Open” option from the “File” menu.</td>
</tr>
</tbody>
</table>

Additional Resources
See your sales representative or contact Gemalto Support directly for information about how to obtain additional documentation.
For technical support, contact your Gemalto representative or consult the Gemalto customer support Web site.

For Further Help
If you received eSigner from a distributor or a bank, as is typically the case, you should first contact the company who supplied the eSigner software to you. If you purchased eSigner directly from Gemalto, the support procedures should be described in your Support and Maintenance contract.
Otherwise you can find information on how to contact your Gemalto representative by clicking Contact Us at the Gemalto web site, www.gemalto.com.

If You Find an Error
Gemalto makes every effort to prevent errors in its documentation. However, if you discover any errors or inaccuracies in this document, please inform your Gemalto representative. Please quote the document reference number found at the bottom of the legal notice on the inside front cover.
The eSigner 4 Plug-in

About eSigner

eSigner is a digital signature–based software solution designed to protect and secure Internet transactions.

With the increase in important business and financial transactions being conducted via the Internet, the need for safe and secure communication is fundamental to the success of individuals and enterprises.

eSigner provides the security of cryptographic algorithms in the software with the simplicity and convenience of hardware based information securely stored in a token, for example, a smart card. This additional hardware-based security is a principal advantage that is significantly more secure than software-only solutions.

The eSigner Plug-in

eSigner is installed as a plug-in to your browser. As such you will not have to launch it as an application, it will be launched by the Web site that you are navigating.

The eSigner plug-in opens inside a regular Web browser. It is launched by specific tags and embedded parameters in HTML pages loaded from the web application through a standard browser. These tags trigger a request to sign data that is either embedded in the HTML page or contained in a remote document, referenced by the page.

A mime-type parameter in the HTML page specifies which type of viewer engine the eSigner plug-in should launch to view the data; either the eSigner viewer or an external application (for example Adobe reader for a .pdf).

Once activated, the eSigner plug-in uses certificates to sign the requested data and transmit it securely using any PKCS#11 middleware module, for example Classic Client with a Gemalto Java-based PKI card such as the EZIO PKI smart card or Classic TPC smart card. eSigner then returns the signed data to the Web server for verification and further processing.

Note:

- eSigner satisfies both IdenTrust Signing Interface Requirements (IT SIR 3.2) and non-IdenTrust requirements and is therefore suitable for IdenTrust and non-IdenTrust use.

- The size of data that the eSigner plug-in is able to sign may be limited by the server settings.
eSigner IdenTrust and/or Corporate Mode

There are two versions of eSigner 4 for Windows; an IdenTrust version (also known as IS) and a Corporate version. The version provided to you depends on how your bank intends to use eSigner.

The two versions provide very similar features, however the IdenTrust version supports an additional specific IdenTrust-compliant interface with the bank Web site that is required in certain business environments.

The Corporate version can operate in Corporate mode only.

The IdenTrust version can operate in one of three modes:

- Corporate mode
- IdenTrust mode with ActiveX technology
- IdenTrust mode with Java technology

In the IdenTrust version, the mode used depends upon the parameters used when calling up a document for signing.

Many features in this document are available for all three modes. However where there are differences between the modes, this is indicated, for example by a note saying “Not available for the IdenTrust mode with Java technology”.

To find out which version you have, please refer to “Finding Out Which Version of eSigner You Are Using” on page 19.

Corporate Mode

In the corporate mode, eSigner is not IdenTrust-compliant and does not support Java technology, but it does support the text/signature MIME type that is not supported in the IdenTrust package.

The following table shows the MIME types supported in corporate mode and whether they are displayed in the eSigner window or an external application available on your PC.

Table 1 - MIME Types Available in Corporate Mode

<table>
<thead>
<tr>
<th>MIME Type</th>
<th>File Type</th>
<th>eSigner Window</th>
<th>External Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>text/Plain</td>
<td>Simple Text</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>text/HTML</td>
<td>Hypertext Markup Language</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>application/PDF</td>
<td>Adobe Acrobat</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>application/msword</td>
<td>Microsoft Word</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>application/vnd.ms-excel</td>
<td>Microsoft Excel</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>text/signature</td>
<td>Combined Signed Data</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

IdenTrust Mode

In the IdenTrust mode (both Java and ActiveX technologies), the interface with the server is a standard that belongs to IdenTrust. The use of this environment is legally restricted to IdenTrust systems and participants, but is compatible with eSigner, which can use Java applets as a plug-in.

Note: eSigner IdenTrust version is compliant with IdenTrust specifications 3.2 and in particular with IT-SIR v3.2.
The following table shows the MIME types supported in IdenTrust mode and whether they are displayed in the eSigner window or an external application available on your PC.

**Table 2 - MIME Types Available in IdenTrust Mode**

<table>
<thead>
<tr>
<th>MIME Type</th>
<th>File Type</th>
<th>eSigner Window</th>
<th>External Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>text/Plain</td>
<td>Simple Text</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>text/HTML</td>
<td>Hypertext Markup Language</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>application/PDF</td>
<td>Adobe Acrobat</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>application/msword</td>
<td>Microsoft Word</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>application/vnd.ms-excel</td>
<td>Microsoft Excel</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

*Note: Microsoft Word and Excel are not supported with Java.*

**The eSigner Graphical User Interface**

Depending on your eSigner configuration and the Web site calling parameters, when you call up a text document to be signed, the eSigner window may either appear in its own window inside the viewed Web page (embedded mode as shown in “Figure 1”), or in a separate pop-up window (as shown in “Figure 2” on page 4). In both cases it provides the same functionality.

*Note: The user interface in eSigner 4 is considerably different to that in eSigner 3.*

**Figure 1 - eSigner Displayed Inside Web Browser**

![Figure 1 - eSigner Displayed Inside Web Browser](image-url)
Figure 2 - eSigner Displayed in a Pop-up Window

Normally, an eSigner pop-up window opens with sufficient size to be used easily. Nevertheless if for any reason the pop-up window is too small you can use the mouse to resize it or the "maximize" button.

Note: The menu bar shown in “Figure 3” does not appear in the IdenTrust version of eSigner when used in IdenTrust mode with Java technology. This is not dependent on your PC’s configuration or the configuration of eSigner but on the bank’s Web site invoking eSigner.

A summary of the items found in the interface and their use is found in “Figure 3” on page 5

Note: eSigner uses the Windows “hourglass” to indicate when it is processing data. Wait for the hourglass to disappear before continuing.
eSigner 4 includes Disability Discrimination Act (DDA) shortcuts designed to make using the software easier for a disabled person.

The principle of these shortcuts is to be able to access functions by issuing a sequence of single keystrokes, beginning with the <Alt> key. The menus indicate the keystrokes that correspond to each function by underlining the keystroke character.

The DDA shortcut features are not available if eSigner is invoked in Java mode in the IdenTrust version. In that version the menu bar (shown in “Figure 3”) does not appear at the top of the eSigner window.

If this is what you experience it is not linked to you PC or eSigner configuration but on the bank’s Web site you are using. You cannot change this.

If you can see the menu bar, you can access the shortcuts.

The DDA Shortcut features are fully available in:

- The Corporate version
- The IdenTrust version in either Corporate mode or IdenTrust mode with Active-x technology

To use DDA shortcut keys, the eSigner window must be selected or focused, so that the menu bar is active, that is the menu titles appear in black. In many use cases, the eSigner window will be the selected or focused window by default when it opens either in embedded mode or in pop-up mode.

For details on tasks on how to use the DDA shortcuts, please refer to “Using the DDA Shortcuts” on page 14.
About Signing Documents

When a page in a Web site triggers a request to sign documents, the eSigner plug-in is launched to allow you to sign the document. A multipurpose internet mail extensions (MIME)-type parameter in the page specifies which type of file is to be signed, and depending on the mime-type, the document may be displayed for signing.

Once activated, the eSigner plug-in uses certificates to sign the requested data using Classic Client, which prompts you to enter a personal identification number (PIN). eSigner then returns the signed data to the Web server for verification and further processing.

The procedure for signing documents is basically the same, regardless of the MIME type, which is in any case not always recognizable to the user. Once the document is displayed in the browser, it is ready for signing.

**Note:** A Web site may call eSigner in such a way that it prompts you to sign a document that you have locally stored on your PC. This is indicated by the presence of the **Browse** button in the eSigner window.

What You See is What You Sign

This feature compares the data that you see, with the data in the memory, so that you can be sure that the data that you see is the same as what you sign. To take full advantage of this feature, it is important to try and display all of the document or data in the eSigner window. Maximize your browser window if necessary.

**Caution:** If the data is too large to fit entirely in the eSigner window, make sure that the most sensitive part is visible, for example the amount in a transaction.

**Note:** The entire document or data is signed, not just the part that is visible in the eSigner window.

eSigner warns you if the eSigner window is not fully on the screen or if the window of another application overlaps it. In such a case, the following message appears:

*Figure 4 - Viewer Error Message*

If you click **Yes**, the signature is performed. If you click **No**, you are returned to the eSigner window where you can adjust it to make sure that all the data is visible.

Signature Policy

The signature policy is a set of rules for the creation and validation of an electronic signature, which is then used to determine if a signature is valid.
A given legal/contractual context may recognize a particular signature policy as meeting its requirements. A signature policy may be issued, for example, by a party relying on the electronic signatures and selected by the signer for use with the other party. Alternatively, a signature policy may be established through an electronic trading association for use amongst its members. The signature policy may be explicitly identified or may be implied by the semantics of the data being signed and other external data, such as a contract being referenced which refers to a signature policy.

### About MIME Type Features

MIME is a specification for formatting documents that are not sent in a typical text format. The MIME type allows different types of documents to be sent over the Internet and determines how a text or other type of document will be displayed.

Many e-mail clients now support MIME, which enables them to send and receive text documents as well as graphics, audio, and video files via the Internet mail system. There are many predefined MIME types. A newer version, called S/MIME, supports encrypted messages. Web browsers also support various MIME types, which enable the browser to display or output files that are not in HTML format.

The MIME types supported by eSigner vary according to the eSigner mode. To know which MIME types are supported for each mode, please refer to “Table 1 - MIME Types Available in Corporate Mode” on page 2 or “Table 2 - MIME Types Available in IdenTrust Mode” on page 3 as appropriate.

### About PINs

A PIN is a private code. It can be a sequence of numeric or alphanumeric characters, or a mix of the two, and it operates as a password. The PIN should be known only to you and must be verified before you can perform security tasks, such as digitally signing a document.

**Note:** In some cases, the PIN may need to be made up of numerical characters only, for example when using a PIN Pad reader, or the virtual PIN Pad reader.

To perform a security operation, you must demonstrate knowledge of the PIN. Software that performs security operations usually displays a window requesting you to enter the PIN before performing the security operation, or there is another area where you can enter the PIN.

**Note:** Other user tasks, such as working with PINs, are covered by the documentation of whatever PKCS#11 module is used with eSigner. If this module is Classic Client, please refer to the Classic Client User Guide for more information about PIN use.
About Certificates

A digital certificate contains information about the user and the user’s public key, and is used to authenticate the user’s identity during secure transactions. The certificate identifying the user must be registered with a certificate authority and this information must be available to both parties.

To use eSigner, your smart card must already contain a certificate available for use with its associated private key.

Note: Certificate storage, management and card use are handled by the middleware being used with eSigner. If the smart card you are using does not have certificates already on it, or certificates are not available from another source, refer to the documentation that accompanies your PKCS#11 for information about how to obtain, store, and manage certificates. When using Classic Client as the PKCS#11 middleware module, for example, this information can be found in the Classic Client User Guide.

Certificate Validation

A certificate is considered to be valid if:

- The time used to validate the document lies within the certificate’s validity period. Local system time is used.

- The validity period of the client certificate lies within the validity period of the issuer certificate. Note, however, that a client certificate that is valid to exactly the same time or longer than one of its issuer certificates (CA certificate), is not accepted.
Installation

This chapter contains information related to the installation of eSigner. Check that the system has all the requirements necessary to support this installation, including the installation or uninstallation of any other software used with eSigner.

System Requirements

The workstation must meet the normal system requirements to run the version of Windows OS installed.

Each user workstation must have at least:

- 50 MB of available hard disk space
- An Internet connection

For details about the versions of Windows, cards, readers and applications supported by eSigner, please refer to the accompanying Release Notes.

Before Installing

Before installing eSigner, check the installation of the PKCS #11 module you will be using with eSigner. Classic Client is such a PKCS#11 module and is recommended by Gemalto to use with eSigner. The PKCS #11 module must be installed before you install eSigner. This may require uninstalling an older version and installing a newer version.

Installation Methods

Network Availability

The end user setup is made available to the user on a local network. In order to install eSigner, perform the following steps:

1. Navigate to the folder on the local network in which the user setup has been stored.
2. Click on the setup executable and the installation automatically begins.

“Silent” Installation

In the “silent” installation, the user installation is deployed to the user’s computer by the administrator using the command line prompt. This procedure is described in "Installing eSigner at the Administrator Level".
Installation

The following sections describe how to:

- Install the eSigner at the administrator level
- Install the eSigner at the user level
- Uninstall eSigner

**Note:** If you are upgrading from an older version of eSigner, first **uninstall** the existing version before installing the new version. Instructions on how to remove the software can be found later in “Uninstalling eSigner” on page 13.

### Installing eSigner at the Administrator Level

The administrator can configure the user setup to install eSigner in the user’s computer without any action on the part of the end user. This installation method is also known as “silent” installation. The administrator configures this installation by entering the following command in the **Command Prompt** dialog box:

```msiexec “Path to eSigner msi” /qn INSTALLDIR=“Path for Install”```

**Note:** The quotes and spaces used in the above code are necessary for correct implementation.

The following is an example for the Corporate version:

```msiexec “c:\templeSignerV4_CORP.msi” /qn INSTALLDIR=“C:\Program Files\Gemalto\eSigner”```

For the IdenTrust version, the equivalent line is:

```msiexec “c:\templeSignerV4_IS.msi” /qn INSTALLDIR=“C:\Program Files\Gemalto\eSigner”```

**Note:** If you are installing the 32-bit version of eSigner on a machine running a 64-bit version of Windows, the directories in the above lines will be C:\Program Files (x86).... instead of C:\Program Files.

If you are installing the 64-bit version of eSigner the names of the .msi in the above lines are eSignerV4_CORP_x64.msi and eSignerV4_IS_x64.msi.

### Installing eSigner at the User Level

**Note:** If you are installing eSigner as a user, you must have the administrator rights to your machine.

**To start the installation process**

1. Begin in one of the following ways.
   - If the setup is available on a network, locate the eSigner .msi file and double-click it.
   - If the setup has been provided in a .zip file, unzip the file, locate the eSigner .msi file and double-click it.

   The **InstallShield Wizard** dialog opens to assist you throughout the installation process.
2 Click **Next** to begin installing eSigner. The eSigner **License Agreement** is displayed.

3 Read the **License Agreement**, and if you understand and agree with the License Agreement, select **I accept the terms in the license agreement** and click **Next**. The following dialog appears.
In the **Destination Folder** dialog, you can optionally click the **Change** button to install the eSigner in a different folder and select the chosen folder. However, Gemalto recommends that you keep to the default directory as this will make it easier to investigate any problems if they occur.

Click on **Next** to proceed with the installation. The following dialog appears:

![Image of Ready to Install the Program dialog]

If you want to change the destination folder (the directory where you want to install eSigner), click **Back** to return to the previous dialog.

If you are ready to begin the installation, click **Install**.

A progress bar appears to track the progress of the installation.

When the eSigner installation has successfully completed, the following dialog appears:

![Image of InstallShield Wizard Completed dialog]

Click **Finish** to exit the **InstallShield Wizard**.

The software is now installed and you may now begin using eSigner.
Uninstalling eSigner

If you have installed both the 32-bit and 64-bit versions of eSigner on the computer, you must uninstall both versions before you can re-install eSigner.

To uninstall eSigner from a computer in Windows XP:

1. From Start, choose Settings > Control Panel > Add or Remove Programs, then select eSigner from the list of programs (some earlier versions were called GemSAFE eSigner and Classic eSigner). Naturally if both the 32-bit and 64-bit versions are installed on the machine, then both appear in the Add or Remove Programs window. The 64-bit version of eSigner is indicated as “64 bits”.

2. Click Remove.

   A window opens asking you to confirm the uninstall operation.

3. Click Yes to continue with the uninstallation of the software.

   When the uninstallation finishes, eSigner no longer appears in the Add or Remove Programs window.

   The eSigner uninstallation does not uninstall the PKCS#11 used with eSigner.

To uninstall eSigner from a computer in Windows Vista and Seven:

1. Open the Control Panel (Start > Control Panel).

2. Double-click Programs and Features.

3. Select eSigner in the list and click Uninstall (the Uninstall button appears when you select eSigner).

4. Click Yes in the confirmation box that appears.

5. If User Account Control is activated, the warning “An unidentified program wants access to your computer” appears. Choose Allow.

6. Again, if User Account Control is activated, a message may appear to tell you to close certain applications. If it does, choose the Automatically close applications option and click OK.

7. A progress bar displays during the removal. At the end of the removal, the progress bar closes, removal is complete and eSigner is removed from your computer.

8. If prompted, restart your computer.
User Tasks

This chapter explains how to perform user tasks associated with eSigner. These tasks include:

- Using the DDA shortcuts
- Entering the User PIN
- Signing documents
- Saving and printing documents
- Viewing certificates
- Displaying and saving a software information report of particular software versions using the eSigner Software Information feature.

Using the DDA Shortcuts

You need to make the eSigner window active in order to enter a shortcut sequence.

Making the eSigner Window Active in Order to Enter a Shortcut Sequence

If the menu titles appear in gray font, you will need to select the eSigner window to make it the active window.

You can do this in one of the following ways:

- If eSigner is embedded in the internet browser:
  - If you have access to the mouse, click the mouse on an inactive part of the eSigner window, such as the display area.
  - If you do not have access to the mouse, first make the internet browser the active application by using the keyboard shortcuts corresponding to your operating system, for example, <ALT> + <TAB> in windows XP. Once the internet browser is the active application, press the <Tab> key as many times as necessary until the eSigner window is selected.

- If eSigner was open in a pop-up window:
  The menu is always active when the eSigner pop-up window is the active application in Windows. If you need to make the internet browser the active application use the keyboard shortcuts corresponding to your operating system, for example, <ALT> + <TAB> in windows XP, as many times as necessary.
Using Shortcuts to Choose Options in Menus

After typing <Alt>, the menu bar underlines the keystrokes for the shortcuts to select each menu, as shown in “Figure 6”.

**Figure 6 - DDA Shortcuts for Menus**

You enter the Post menu by typing <P> and the Actions menu by typing <A>.

When you then enter a menu the shortcut options are underlined and also indicated to the right of each option. For example, “Figure 7” shows that the shortcut for Print is P (underlined and to the right of “Print”). To print, type <P>.

**Figure 7 - DDA Shortcut for Menu Options**

The following table lists all the available DDA shortcuts in the standard Gemalto eSigner package.

**Table 3 - DDA Shortcut Sequences**

<table>
<thead>
<tr>
<th>Key Sequence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Alt&gt;</td>
<td>Enters shortcut sequence</td>
</tr>
<tr>
<td>P</td>
<td>Enters Post menu</td>
</tr>
<tr>
<td>S</td>
<td>Sign</td>
</tr>
<tr>
<td>V</td>
<td>Verify</td>
</tr>
<tr>
<td>C</td>
<td>Cancel</td>
</tr>
<tr>
<td>A</td>
<td>Enters Actions menu</td>
</tr>
<tr>
<td>P</td>
<td>Print</td>
</tr>
<tr>
<td>S</td>
<td>Save</td>
</tr>
<tr>
<td>V</td>
<td>View</td>
</tr>
<tr>
<td>A</td>
<td>About</td>
</tr>
</tbody>
</table>

For example: the single keystroke sequence needed to start a signature is:

<Alt> <P> <S>

Type each key one at a time in the right sequence.

**Note:** The displayed DDA shortcut menus can be customized by the bank distributing eSigner. It’s thus possible that the menus are different to those described in this document. Nevertheless the way to enter menus and select an action remains as described in the previous sections.
Using Shortcuts in the Select Certificate Window

*Figure 8 - Select Certificate Dialog Box*

To scroll up and down the certificate list, use the up and down arrows on the keyboard. To switch to the buttons at the bottom, use the right or left arrow on the keyboard. To return to the certificate list, either click the right button when View Certificate is active, or the left button when OK is active.

Using Shortcuts With the Virtual PIN Pad

*Figure 9 - Keyboard PIN Entry Dialog Box*

Use the four arrow keys (up, down, left and right) on the PC keyboard to move around the numbers and the Clear, Erase, OK and Cancel buttons on the virtual Pin Pad. For these purposes, the buttons are a continuation of the numbers. For example if the number 1 is highlighted, then pressing the down arrow highlights the Erase button. Pressing the down arrow again highlights the Cancel button.

To select the number or button that is highlighted, hit the space bar. For example “Figure 9” shows that the number 9 is selected, so hitting the space bar enters 9 as the first digit of the PIN.
Entering the User PIN

At various times, for example when signing a document, you are asked to enter the User PIN of your smart card. The way you do this varies according to whether you are using a regular smart card reader, or a PIN Pad reader. This section explains the different ways of entering the user PIN.

Using a Regular Smart Card Reader

With a regular smart card reader, the way of entering the PIN depends on your eSigner setup, as defined by your bank. There are three different modes:

Mode 1 - Keyboard Entry

In this mode the following window displays when you are prompted to enter the user PIN.

Figure 10 - Keyboard PIN Entry Dialog Box

Enter the PIN using your PC keyboard and then press <Enter> or click OK.

Mode 2 - Virtual Scrambled PIN Pad Entry

In this mode the following window displays when you are prompted to enter the user PIN.

Figure 11 - Keyboard PIN Entry Dialog Box

Enter the PIN by clicking on each digit the PIN and then click OK (or press <Enter>). Entering the digits using your PC keyboard has no effect.
DDA shortcuts are available with this window to allow entering the PIN. For specific detail, please refer to “Using Shortcuts With the Virtual PIN Pad” on page 16.

**Mode 3 - Virtual Scrambled PIN Pad and Keyboard Entry**

In this mode, the virtual scrambled PIN pad displays as in mode 2, but entry from the keyboard is accepted. Both entry methods are available.

**Using a PIN Pad Reader**

When using a PIN pad reader, the following window appears when you need to enter a PIN.

*Figure 12 - PC Pinpad Secure PIN Entry Window*

Enter the current User PIN in the PIN Pad, then press the confirmation button, for example **OK** or **Enter**.

If the PIN is correct, you will be able to continue following the steps to perform a signature. A message appears on the PIN Pad’s display to tell you that the PIN is correct.

**Timeout**

If you do not enter the PIN after a certain time duration eSigner considers that you have canceled the operation and you will get the following message. In addition, a “timeout” message appears on the reader’s display. Press **Close**. Request the signature again by pressing **Sign**. Make sure that you enter the PIN before the allowed time elapses.

*Figure 13 - PIN Entry - Out of Time Message*
Entering an Incorrect PIN

If the PIN is incorrect, the following message appears in the eSigner window. Press Close. Request the signature again by pressing Sign.

*Figure 14 - Incorrect PIN Entry Using PIN Pad*

If using a PIN Pad reader, the message in “Figure 14” appears and in addition, an “incorrect PIN” message appears on the reader’s display.

**Caution:** This window displays the number of attempts remaining to enter the PIN. If you exceed this number, your card becomes blocked. Make sure that you know the correct PIN before trying again.

Changing the User PIN

For security reasons, some cards force you to change the PIN the first time you use the card. If your PKCS#11 is Classic Client, it is the Registration Tool in Classic Client that manages this operation. Please refer to the *Classic Client User Guide* for more information.

If your PKCS#11 is Classic Client, you can change the User PIN or IdenTrust PIN yourself through the Classic Client toolbox. Please refer to the *Classic Client User Guide* for more information.

Finding Out Which Version of eSigner You Are Using

To find out whether your version is the Corporate Version or the IdenTrust Version:

From Start, choose Settings > Control Panel > Add or Remove Programs. This displays the window in “Figure 5” on page 13.

If you are using the IdenTrust version, eSigner appears as “eSigner 4.x IS” as seen in the example in “Figure 5”.

If you are using the Corporate version, eSigner appears as “eSigner 4.x CORP”.

To find out the exact version number of the software:

1. Do one of the following:
   - Click the About icon 📈.
   - From the Actions menu, choose About.
   - Use the following DDA shortcut sequence: <Alt> then <A> then <A> again.
     
     An information window appears like the one shown in “Figure 15”.

2 Click Close to close the window.

Changing Modes in the IdenTrust Version of eSigner

The operating mode (Corporate or IdenTrust) and technology (Java or ActiveX) are determined by the bank's Web server and cannot be changed by yourself.

Signing Documents

When a document to be signed is available, eSigner is triggered to open in its own window — either within a regular Web browser or as a separate pop-up window — to display the document. You view the document, if possible, and proceed to sign it.

You can sign documents of various MIME types with eSigner. To see if a MIME type is supported by your version or in the mode you are using, please refer to Table 1, "MIME Types Available in Corporate Mode", on page 2 or Table 2, "MIME Types Available in IdenTrust Mode", on page 3 accordingly. The procedure for all MIME types is essentially the same.

You may be prompted to enter a PIN or insert a smart card in the process of signing if this has not already been done before signing.

Signing Text and Other Document Files in the eSigner Window

As an end-user, you do not initiate a signature sequence. It is the Web site that initiates the signature sequence by calling eSigner. Your browser then displays the eSigner window.

Caution: Make sure that you view all the document before signing, especially if some of it is not immediately visible in the eSigner window.
To sign text and other types of document files using the eSigner plug-in

Figure 16 - Signing a Document

1. When the document appears in the eSigner window, sign it by doing one of the following:
   - Click **Sign**.
   - From the **Post** menu, choose **Sign**.
   - Use the following DDA shortcut sequence: <Alt> then <P> then <S>.

   **Note:** For simplicity, this document will just say “Click Sign” for other use cases but you should remember that all three of these methods can be used.

   If there is more than one certificate in the certificate store, the **Select Certificate** dialog box opens. Select a certificate as described in “Selecting Certificates” on page 29.

2. When the document has been successfully signed, it is automatically sent to the server for verification and further processing. If no error messages appear, the signature operation is successful.

   Typically, the eBanking Web site will direct you to a page confirming the success of the transaction.

If the Data is Too Large

If the data is too large to be displayed by eSigner, the following message appears and the **Sign** button is disabled as shown in the following figure:
Figure 17 - Data Too Large to Display - Sign Button Disabled

Note: If this occurs and if the used web application allows it, you may retry a full signature transaction sequence by selecting less data or less objects to be signed. If you cannot manage to split your data into smaller packages using the web application, please contact your e-banking application support.

Signing Text and Other Document Files in an External Window

Some documents may not directly be displayed in the eSigner window but are viewable via another application residing on your PC. Depending on how your version of eSigner is configured, one of the following windows displays.

Figure 18 - External Window With View Data Button
Figure 19 - External Window With Hyperlink

The hyperlink in “Figure 19” could equally be configured to display the filename only.

Click View Data or on the hyperlink as appropriate, to open the document in its corresponding application. You must of course have the appropriate application on your computer.

This display mode is applicable to the following types of files:

■ Adobe pdf
■ Microsoft Word
■ Microsoft Excel

Signing Text and Other Document Files in Button Mode

It is possible that your administrator will have configured eSigner in “button mode”. In this case, a Sign button displays instead of the data. Just click Sign and continue as you would for signing a document in standard mode.
Uploading Signed Local Documents

In some cases the bank's Web site will ask you to sign documents that are stored locally on the hard disk of your computer and then send them to the server.

Figure 20 - Uploading Signed Local Documents

To upload a document to be signed

1. In the case where you are prompted to find the document on your hard disk, use the Browse button in eSigner to locate the file and click Open.
If the file’s MIME type is supported by eSigner, it appears in the eSigner plug-in window and a “hyperlink” appears next to the **Browse** button (as shown in “Figure 21”). In fact this hyperlink is not active and is for information only.

**Figure 21 - Uploading Signed Local Documents (eSigner Window)**

If it is a MIME type that can be viewed by an external window, a hyperlink appears in the panel to the right of the **Browse** button. Click this link to view the document in the external window.

**Figure 22 - Uploading Signed Local Documents (Hyperlink for External Window)**

If the MIME type is not supported, an error appears to tell you this.

1. Click **Sign** to continue with the signing process as with other types of files.
Saving Documents

You can use eSigner to save documents, both before and after they are signed to an authorized local hard disk or other document storage area.

By default, the files in plain text are saved in text format (*.txt) and HTML files are saved in HTML format (*.htm).

To save documents before signing:

1. Save the document by doing one of the following:
   - Click the **Save** icon at the top of the window.
   - From the **Actions** menu, choose **Save**.
   - Use the following DDA shortcut sequence: <Alt> then <A> then <S>.

   The **Save file** dialog box opens as shown in “Figure 23”.

**Figure 23 - Save File Window**

1. In **File name**, enter the name for your file.
2. In **Save as type**, select a format for the file.

**Note**: If the format for your file is not present in the list for **Save as type**, enter the file extension manually in **File name**.

4. Click **Save**.
To save documents after signing

Note: This option is available only if activated in the configuration file.

1. When you see the eSigner signing window, click the **Save After Signing** icon that is to the left of the **Sign** button in order to activate the feature. The icon changes from gray to orange as shown in “Figure 24” on page 27.

*Figure 24 - Save after Signing Icon*

2. Click **Sign**. The **Saving Signature File** Window opens as shown in “Figure 25”.

*Figure 25 - Saving Signature File Window*
3 Navigate to the directory where you want to save the file.

4 In File name, enter the name for your file.

5 In Save as type, select a format for the file.

6 Click Save. The document is saved as an HTML page including a call to eSigner n verify mode with the PKCS#7 signature included.

If there is more than one certificate in the certificate store, the Select Certificate dialog box opens. Select a certificate as described in “Selecting Certificates” on page 29.

7 When the document has been successfully signed, it is automatically sent to the server for verification and further processing. If no error messages appear, the signature operation is successful. The signed file is saved to the location you specified.

Selecting Smart Card Slots

If you have more than one smart card reader and one card inserted in your PC, then you may have to select the reader with the select reader dialog box. This select reader may also appear if you have only one card but featuring multiple virtual slots.

*Figure 26 - Select a Reader*

![Select a Reader](image)

Simply select your reader or slot and click OK.

*Note:* To use DDA shortcuts in this window, please refer to “Using Shortcuts in the Select Certificate Window” on page 16. (The shortcuts work in the same way as the Select Certificate window.)

Printing Documents

*To print a signed or unsigned document,*

Do one of the following:

- Click the Print icon.
- From the Actions menu, choose Print.
- Use the following DDA shortcut sequence: <Alt> then <A> then <P>.

This opens the Windows Print dialog box where you select a printer.
Selecting Certificates

If your card has more than one certificate inside, for certain tasks such as signing a document, the window in “Figure 27” appears, asking you to choose a certificate.

*Figure 27 - Select Certificate Dialog Box*

To select a certificate:
1. Click on a certificate you want to select.
2. If you want to view the certificate details before choosing it, click **View Certificate**. For more a description of the certificate details, please refer to “Viewing Certificates”.
3. Click **OK** to select the certificate.
4. Depending on the type of certificate, you may be prompted to enter a PIN. If this happens, enter the PIN and click **OK**.

**Note:** To use DDA shortcuts in this window, please refer to “Using Shortcuts in the Select Certificate Window” on page 16.

Viewing Certificates

When eSigner has been invoked to sign a document, that is, when it is in the signing mode, you can use the eSigner plug-in to view details of certificates in the certificate store.

You can view the details of a certificate before you use it to make a signature.

*To view certificates before signing:*
1. Open the eSigner plug-in.
2. View the certificates by doing one of the following:
   - Click the **View Certificates** icon.
   - From the **Actions** menu, choose **View**.
   - Use the following DDA shortcut sequence: <Alt> then <A> then <V>.

**Note:** Depending on your eSigner configuration, you may be asked to enter your PIN.

3. The **Select Certificate** window shown in “Figure 27” on page 29 appears, even if there is only one certificate in the card:

**Note:** You will only see certificates that are available for signing even if there are others in the card.
4. Select the certificate you want to view and click **View Certificate**. This opens the Certificate Viewer. The **General** tab is active and shows information as shown in “Figure 28” on page 30.

**Figure 28 - Certificate Viewer - General Tab**

The **General** tab allows access to certificate information such as:

- for what purpose the certificate was issued,
- to whom the certificate was issued,
- the authority that issued the certificate,
- and the certificate validity period.

5. If you want to display the detailed information about the certificate, click the **Detail** tab. This displays the information shown in “Figure 29” on page 31.
6 Expand an individual data field, such as Issuer, to reveal its contents.

7 If you want to display the path and origin of a certificate, click the Certification Path tab. This displays the information shown in “Figure 30” on page 31.

*Figure 29 - Certificate Viewer - Details Tab*

![Certificate Viewer - Details Tab](image)

6 Expand an individual data field, such as Issuer, to reveal its contents.

7 If you want to display the path and origin of a certificate, click the Certification Path tab. This displays the information shown in “Figure 30” on page 31.

*Figure 30 - Certificate Viewer - Certification Path*

![Certificate Viewer - Certification Path](image)
Troubleshooting

Use this chapter to resolve any problems that may occur while you are using eSigner.

Initialization Problem

This error displays when you try to start eSigner.

Error during input parameters initialization: The configuration parameters file was not found

Description
The configuration parameters file, Config.reg is missing.

Solution
Make sure that the file is in the directory where you installed eSigner. If the file is not present on the computer at all, reinstall eSigner.

Certificate Problems

This section tells you what to do if the following certificate-related error messages appear:

No valid certificate found in card that matches the search criteria. Please use “View Certificate” for details

Description
This error occurs when eSigner finds one or more certificates in the card, but none are valid. This may be because the time of the operation is not within the validity period of the certificate “Certificate Validation” on page 8 or that the certificate is the wrong type (for example, not valid to perform signatures).

Solution
Insert a smart card that contains a valid certificate.

No certificate found in card

Solution
Insert a smart card that contains a certificate.
PKCS#11 dynamic library not found

Description
Either eSigner cannot find the PKCS#11 module (for example Classic Client) or it cannot find the certificate store in the module.

Solution
Reinstall the PKCS#11 module. Consult the documentation of your PKCS#11 for details on how to do this (for example, the Classic Client User Guide).

Software Problems

This section tells you what to do if the following software-related error messages appear:

No supported card found

Description
Either there is no card in the reader, or eSigner does not recognize or support the smart card.

Solution
Insert a supported smart card in the reader.

No reader found

Description
This message appears when the reader is not connected.

Solution
Make sure that your smart card reader is properly connected to the computer.

Device error

Description
An error occurred with either the smart card, reader, the smart card itself, or the smart card subsystem.

Solution
Check that the reader is correctly connected to the computer and that the smart card is correctly inserted in the reader.

Incorrect PIN

Description
The PIN you entered is incorrect.

Solution
Re-enter the PIN.
PIN is blocked

Description
The PIN has become blocked following too many consecutive presentations.

Solution
If the configuration of your card and your company’s security policy allows it, unblock the smart card’s User PIN and try again. For information about how to unblock the PIN of a smart card, refer to the Classic Client User Guide.

If you cannot unblock the PIN contact your administrator.

eSigner Viewer Error

Figure 31 - Viewer Error Message

This error may occur after you click Sign. It may be caused because another window is blocking the eSigner window and not all parts of the window that contains the data to be signed can be detected. Make sure that your window and all the data you want to sign in it is fully visible. Refer to “What You See is What You Sign” on page 6 for more details.

If the error persists, you may have a hardware problem caused by old graphic cards and/or drivers, or there may be a malicious program trying to change the content that is displayed. In this case, contact your Administrator.

Cannot read the file you have selected.

This error occurs because eSigner was unable to read the data to be signed from the selected file. Check that:

- You have read access to the file.
- The file is not locked by another application.
- The file has not been deleted.
System Problems

Unable to create thread.

Description
This error may occur because there not enough free resources in Windows to create a new thread.

Solution
Reboot the system and try again.

Error creating text window.

Description
This error can occur because there are not enough free resources in Windows to create a new text window.

Solution
Reboot the system and try again.

Error initializing HTML window.

Description
This error can occur because there are not enough free resources in Windows to create the HTML window.

Solution
Reboot the system and try again.

No HTML module installed!

Description
This error occurs because the component to display HTML data is not available.

Solution
Check to see if Ter32.dll and Hts32.dll are installed (its default location is C:\Program Files\Common Files\Gemalto\Viewer). If it is not, re-install eSigner with the HTML module.

Network error.

Description
If you receive this message, an error has occurred during the downloading of data from the network.

Solution
Check that the network server is available and try again. If you are still unsuccessful, contact your Administrator.

Data not completely received. Please wait....

Description
This message may occur if you attempt to sign data in eSigner before it is fully downloaded from the network.

Solution
Wait for the data to be completely downloaded and try again.
PKCS#11 Error - Trusted Web Site Problem

Description
This problem may occur when using Internet Explorer 8 or later with a version of Windows Vista or later. It is not systematic.

When trying to access a Web site, the following message appears:

*Figure 32 - PKCS#11 Error - Web Site Not Trusted*

Solution
Click **Close** to remove the message and follow these steps:

1. Make sure that the Web site is in Internet Explorer’s list of trusted Web sites.
   
   a) Open IE, and from the **Tools** menu, choose **Internet Options**, then click on the **Security** tab.
   
   b) In the **Security** tab, click the **Trusted Sites** icon, then click on **Sites**.

*Figure 33 - Trusted Sites in the Security Tab*
The Trusted Sites window opens as shown:

*Figure 34 - Trusted Sites Window*

![Trusted Sites Window]

c) If the site is not in the list, enter the URL in **Add this website to the zone** and click **Add**.

d) Click **Close**.

2 Back in the Security tab, set the security level for trusted Web site to **Medium**.

3 Disable the protected mode by clearing the check box **Enable Protected Mode**.

4 Click **OK** to close the Internet Options window.
This chapter provides some general background to some of the security concepts related to eSigner.

Certificates

What is a digital certificate?

A digital certificate is an electronic document that serves as your digital passport. Your digital certificate stores your public key and other personal information about you and the certificate.

The most widely accepted standard for digital certificates is defined by International Telecommunications Union standard ITU-T X.509. Version three is the most current version of X.509.

The X.509v3 certificate includes the following data:

- Version
- Serial number
- Signature algorithm ID
- Issuer name
- Expiration Date
- User name
- User public key information
- Issuer unique identifier
- User unique identifier
- Extensions
- Signature on the above fields

As a convenience to recipients, it is standard practice to attach your digital certificate to every secure e-mail that you send. The recipient uses your public key, included in your digital certificate, to encrypt e-mail addressed to you. If you do not attach your digital certificate to outgoing e-mails, recipients must retrieve your public key from a public directory if they want to reply to you with an encrypted e-mail.
What is a Certificate Authority?

Certificate Authorities (CAs) are trusted third parties that issue digital certificates. CAs vouch for the identity of the individual or enterprise to whom they are issuing a certificate. CAs provide a transfer of trust from CA to the individual or enterprise. When you trust the CA certificate, you can transfer that trust to all certificates published by that CA.

When you obtain your digital certificate, you provide the CA with your public key and any personal information requested by the CA. The CA verifies your personal information and the integrity of your public key. After the verification process, the CA signs your public key, stores appropriate personal information and your public key on the digital certificate, and issues your digital certificate to you.

CAs issue certificates with varying levels of identification requirements. CA policies and the level of identification of the digital certificate determine the method and requirements for proving your identity to the CA. The most simple digital certificate only requires your e-mail address and name. However, some CAs require a driver’s license, notarized certificate request form, or any other personal documentation attesting to your identity. Some CAs may even go as far as requiring biometric data such as fingerprints.

The CA public key must be widely available so that users can validate the authenticity of all certificates published by this CA.

Signatures

What is a digital signature?

A digital signature is a piece of information created using message data and the owner's private key. Digital signatures provide message authentication, non-repudiation of origin, and data integrity.

Digital signatures are created by mathematical, or hash, and private signing functions. The one-way hash function produces a message digest, a condensed version of the original message text. The message digest is encrypted using the sender's private key, turning it into a digital signature.

The digital signature can only be decrypted using the public key of the same sender. The recipient of the data decrypts the digital signature and compares the result with a message digest, recalculated from the original message text. If the two are identical, the message was not manipulated, thus is authentic.

The digital signatures performed by eSigner follow the PKCS#7 standard. For more information about this standard, see www.rsa.com.
PKCS# 11 Libraries

What Is a PKCS# 11 Library?

eSigner uses a PKCS #11 component to perform cryptographic functions. PKCS #11 refers to a standard that specifies an API, called Cryptoki, to devices which hold cryptographic information and perform cryptographic functions. Cryptoki, pronounced crypto-key and short for cryptographic token interface, follows a simple object-based approach, addressing the goals of technology independence (any kind of device) and resource sharing (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device called a cryptographic token.

While eSigner can use any PKCS #11 API, it is often used in conjunction with Classic Client, which is a smart card–based PKCS #11 API designed to secure e-mail communications and Internet transactions. Classic TPC smart cards support encryption/decryption and signature functions.

eSigner and a smart card provide the following advantages:

■ Your private key is never removed from your smart card.
■ The smart card is hardware-based security.
■ The PIN code protects key use.
■ eSigner is portable and convenient.

The encryption/decryption function enables you to send and receive secure e-mail to protect confidential or private information. You can use the signature function to sign your messages. By signing messages, you can prove to the recipient that you are who you claim to be.
Smart Cards

What Is a Smart Card?

The smart card is the size of a conventional credit card. But unlike the credit card, which has a magnetic stripe, the smart card has a silicon microprocessor chip to store and process electronic data and applications. The advantage of the smart card is security.

There are generally two types of smart cards: contact and contactless. Contact smart cards use a microprocessor chip to store and process data. They must be inserted into a smart card reader. Contactless smart cards use a microprocessor chip and antenna to store and process data.

What Is the Classic TPC Smart Card?

Your Classic TPC smart card stores your private key and digital certificate. In the past, your only option was to store your private key on your local hard drive, rendering it susceptible to theft and fraudulent use. With eSigner, your electronic identity is secure. You must have both the smart card and PIN code to use the smart card.

The Classic TPC smart card is tamper resistant. The structure and operating system of the smart card make it practically impossible to interrogate or pilfer smart card data.

Perhaps the most convenient aspect of the Classic TPC smart card is portability. With eSigner, you can carry your electronic passport with you at all times and use it on any eSigner–equipped computer in the world.

What is On Board Key Generation?

The Classic TPC smart card offers on-board key generation. With this feature, every time you enroll a new certificate on your smart card, a new key pair is generated on your smart card. In other words, you are not limited to using the same key pair for every certificate that you enroll.

One significant advantage of on board key generation is the ability to monitor and control the life span of your RSA key pairs and that the generated key pair is unique.

Increased Certificate Storage

You can store up to six key pairs and up to eight multiple digital certificates in your Classic TPC smart card depending upon the size of your certificates and space available in the card. The multiple digital certificates feature provides the convenience of using certificates for whatever purposes you want; for example, you can use certificates with varying degrees of encryption (1024–bit and 2048–bit RSA key pairs) to communicate securely with contacts in various parts of the world.

Another reason for obtaining more than one digital certificate is the level of certification that the Certificate Authority (CA) requires. You may want to obtain and use a digital certificate from a CA that requires stringent identity certification if you are using the certificate for sensitive business communications or financial transactions. However, if you want to encrypt/sign data for personal communications, you may decide that a certificate from a CA that requires minimal identity certification meets your needs.
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>DDA</td>
<td>Disability Discrimination Act</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HTML</td>
<td>Hyper Text Markup Language</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol</td>
</tr>
<tr>
<td>ISIL</td>
<td>IdenTrust Signing Interface Library</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>MIME</td>
<td>Multipurpose Internet Mail Extensions</td>
</tr>
<tr>
<td>NPAPI</td>
<td>Netscape Plug-in Application Programming Interface</td>
</tr>
<tr>
<td>NTLM</td>
<td>Windows NT LAN Manager</td>
</tr>
<tr>
<td>PC/SC</td>
<td>Personal Computer/Smart Card</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, Adleman (inventors of public key cryptography standards)</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure/Multipurpose Internet Mail Extensions</td>
</tr>
<tr>
<td>SIR</td>
<td>Signing Interface Requirements</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
</tbody>
</table>
# Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm</td>
<td>A mathematical formula used to perform computations that can be used for security purposes.</td>
</tr>
<tr>
<td>Certificate</td>
<td>A certificate provides identification for secure transactions. It consists of a public key and other data, all of which have been digitally signed by a CA. It is a condition of access to secure e-mail or to secure Web sites.</td>
</tr>
<tr>
<td>Certificate authority</td>
<td>An entity with the authority and methods to certify the identity of one or more parties in an exchange (an essential function in public key cryptographic systems).</td>
</tr>
<tr>
<td>Cryptography</td>
<td>The science of transforming confidential information to make it unreadable to unauthorized parties.</td>
</tr>
<tr>
<td>Digital signature</td>
<td>A data string produced using a public key cryptographic system to prove the identity of the sender and the integrity of the message.</td>
</tr>
<tr>
<td>Encryption</td>
<td>A cryptographic procedure whereby a legible message is encrypted and made illegible to all but the holder of the appropriate cryptographic key.</td>
</tr>
<tr>
<td>Interoperability</td>
<td>The ability of products manufactured by different companies to operate correctly with one another.</td>
</tr>
<tr>
<td>Key</td>
<td>A value that is used with a cryptographic algorithm to encrypt, decrypt, or sign data. Secret key cryptographic systems use only one secret key. Public key cryptographic systems use a public key to encrypt data and a private key to decrypt data.</td>
</tr>
<tr>
<td>Key length</td>
<td>The number of bits forming a key. The longer the key, the more secure the encryption. Government regulations limit the length of cryptographic keys.</td>
</tr>
<tr>
<td>Public key cryptographic system</td>
<td>A cryptographic system that uses two different keys (public and private) for encrypting data. The most well-known public key algorithm is RSA.</td>
</tr>
<tr>
<td>Secure sockets layer (SSL)</td>
<td>A security protocol used between servers and browsers for secure Web sessions.</td>
</tr>
<tr>
<td>SSL handshake</td>
<td>The SSL handshake, which takes place each time you start a secure Web session, identifies the server. This is automatically performed by your browser.</td>
</tr>
<tr>
<td>S/MIME</td>
<td>A Standard offline message format for use in secure e-mail applications.</td>
</tr>
<tr>
<td>Token</td>
<td>In a security context, a token is a hardware object like a smart card, but it could also be a pluggable software module designed to interact with a specific hardware module, such as a smart card. Token-based authentication provides enhanced security because success depends on a physical identifier (the smart card) and a personal identification number (PIN).</td>
</tr>
</tbody>
</table>