User's Guide to

iD2 Personal

Version 2.8

iD2 Technologies

October, 2000

Document number: UG-PE-020800-WIN-ENG-100

Contents

About this Guide

Intended Audience

This User's Guide is intended for those who want to install, configure and use iD2 Personal, with their security-enabled applications, on a PC.

The Product

iD2 Personal is a unique software product that brings security and smart card functionality to standard software.

iD2 Personal includes an SSL proxy, for access to secure web sites, from Microsoft Internet Explorer or Netscape Communicator, with full-length encryption, and a digital signature module for signing electronic documents. Access to secure web sites may be performed without the SSL proxy, although with weak encryption. Full-length encryption may be achieved in combination with a step-up certificate on the server side.

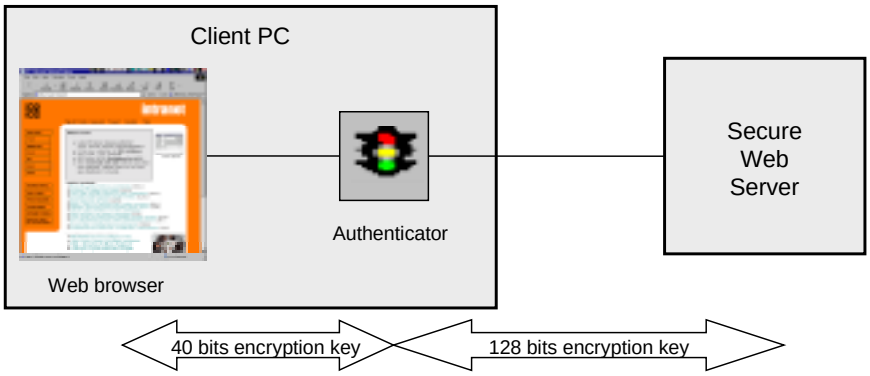
In addition, iD2 Personal can be used for secure and smart card based mail, either in Microsoft Outlook 98/Express or Netscape Messenger.

iD2 Personal includes these components:

- Authenticator
- WebSigner
- Cryptographic Service Provider (CSP) including the iD2 CSP Certificate Utility
- Cryptographic Module
- Cryptographic Library including the Administration Utility

Authenticator

Authenticator interacts with the web browser to improve the security of the Internet transactions exchanged with secure web servers. From the browser's point of view, Authenticator acts as a security proxy. This means that the web browser is configured to route all secured transactions via Authenticator. The following figure illustrates how Authenticator interacts with HTTPS transactions.



WebSigner

WebSigner is a browser add-in that is used to create digital signatures.

Cryptographic Service Provider

iD2 Personal may be used as a Microsoft Cryptographic Service Provider (CSP). This makes it possible for you to use your smart card in Microsoft Outlook 98/Outlook Express and Internet Explorer.

iD2 CSP Certificate Utility is a required utility program that moves certificate data from a smart card into the Registry where it can be accessed by various application programs e.g., Internet Explorer and Outlook 98.

Cryptographic Module

Cryptographic Module allows you to use your smart card in Netscape Communicator and Messenger. This module is not selectable during installation but it will be installed automatically if a Netscape browser is selected.

Cryptographic Library

Cryptographic Library is the part of iD2 Personal that implements the cryptographic standard interface Cryptoki (PKCS #11). Cryptographic Library also contains the Administration Utility that is used to configure the tokens performing the cryptographic functions. A token may be either a smart card or a virtual smart card (i.e., a system file that replicates the information held in a smart card).

What is New in This Version

This version of iD2 Personal introduces, in WebSigner, the capability to sign file contents in addition to signing plain text. The dialog boxes used for signing have been slightly changed.

In addition to the support for new types of smart cards, (specified in the `readme.htm` file accompanying iD2 Personal) there is also support for so called PIN-pad devices based on CT-API.

The existence of a PIN-pad will effect some dialog boxes in Administration Utility, Authenticator and WebSigner. Whenever the user is prompted for his PIN code the corresponding text boxes will be unavailable, (i.e., grayed), but instead, the PIN-pad will signal that the PIN should be entered at the device.

Where to Find the Information

This guide is divided into two parts. The first part gets you started with the iD2 Personal software, and covers installation and initial troubleshooting of the product:

- "Installation" on page 5
- "Troubleshooting" on page 13

The second part is the reference section of the guide, and provides descriptions and operating instructions for the various components of the product:

- "Administration Utility" on page 17
- "Authenticator" on page 29
- "CSP" on page 43
- "Cryptographic Module" on page 59
- "WebSigner" on page 67
- "iD2 CSP Certificate Utility Functions" on page 73
- "Glossary of Terms" on page 75

References

In addition to this manual, there is another one covering the more technical aspects of customization and programming

[1] *iD2 Personal Technical Description*, by iD2 Technologies.

Conventions Used in This Guide

To help you locate and interpret the information easily, the following conventions are used throughout this guide.

Italic text is used for:

- labels in dialog boxes when data entries in the corresponding text boxes are explained,
- check box text,
- titles of external references,
- variables in commands and configuration files.

Bold text is used to emphasize words of extra significance.

`Courier` is used for:

- file names and paths,
- command line commands,
- text file examples.

Arial is used for:

- menu and dialog box selections,
- button text.

Underlined text is used for URLs.

Note: Notes contain helpful suggestions, or references to information not contained in this guide.

Warning: The reader should be careful. Warnings contain important information on how to avoid errors or loss of data.

How to Contact Us

To provide feedback about our products or to suggest product enhancements, please send an e-mail to feedback@id2tech.com.

Installation

System Requirements

iD2 Personal will run under the following operating systems

- Windows 95 and Windows 98
- Windows 2000
- Windows NT 4.0

Detailed information on supported operating system versions is available in the file `README.HTM`.

6 MB of free disk storage is required.

Browser versions

iD2 Personal requires that your browser supports JavaScript. Versions later than Netscape Communicator 4.05 and Internet Explorer 4.0 are acceptable.

Installing iD2 Personal

Installation of iD2 Personal is a simple operation where an installation wizard guides you through the procedure, on-screen. Should you require further information, the various steps in the procedure are detailed below, for your guidance. If problems are encountered in the initial use of iD2 Personal please refer to “Troubleshooting” on page 13.

iD2 Personal can be installed from a CD or from files downloaded from the Internet.

Note: Your version of iD2 Personal may have been customized before it was delivered to you, and the installation procedure may differ slightly from the default installation described below.

Some of the components (listed in “The Product” on page 1) may be excluded in a customized installation.

Installing from the CD

To install iD2 Personal you should follow this procedure step-by-step:

1. Insert the iD2 Personal CD into the computer’s CD-ROM drive.

2. Click the **Start** button and select **Run**.
3. Enter `d:\setup` (where `d:` is the drive containing the iD2 Personal CD) or click the **Browse** button to locate the setup file.
4. Click **OK** to start the installation. The Welcome dialog box is displayed.

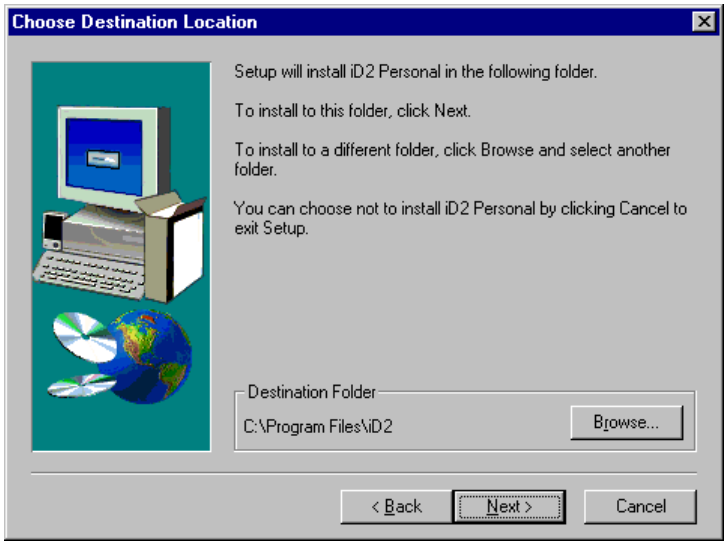
   Read the text in the dialog boxes carefully, at each step, before continuing.

Note: To stop the installation at any time, click **Cancel** and **Exit Setup**.

Note: If setup finds a previous installation of this product or any of its components, you will be asked if you want to uninstall the old version before you continue the installation. It is recommended that you uninstall the old version.

---

5. Click **Next >**. The Choose Destination Location dialog box is displayed.

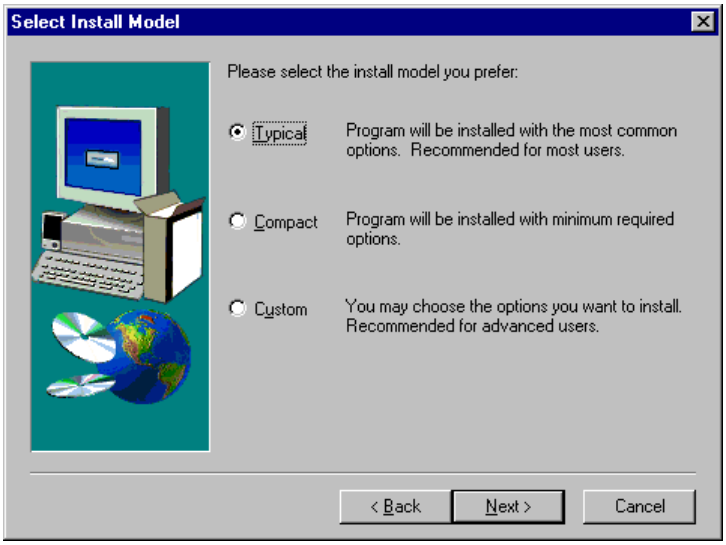


6. Specify the destination folder. The default is:

   `C:\Program Files\iD2`

   If you want to change this, use the **Browse** button. If necessary, the new folder will be created.

   Click **Next >**. The Select Install Model dialog box is displayed.

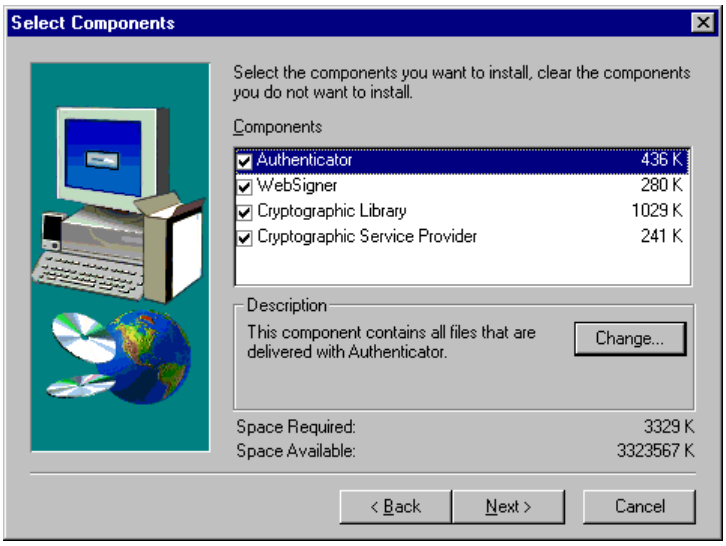


7. Select the type of installation you prefer:

   - **Typical** - means a default installation where you have a minimum of interaction until the setup is completed.
   - **Compact** - means a default installation without help files.
   - **Custom** - gives you the options to control which components and sub-components should be installed.

   Click **Next >**. If you have selected the Custom installation the Select Components dialog box is displayed. Otherwise the Installed Browsers dialog box will appear.

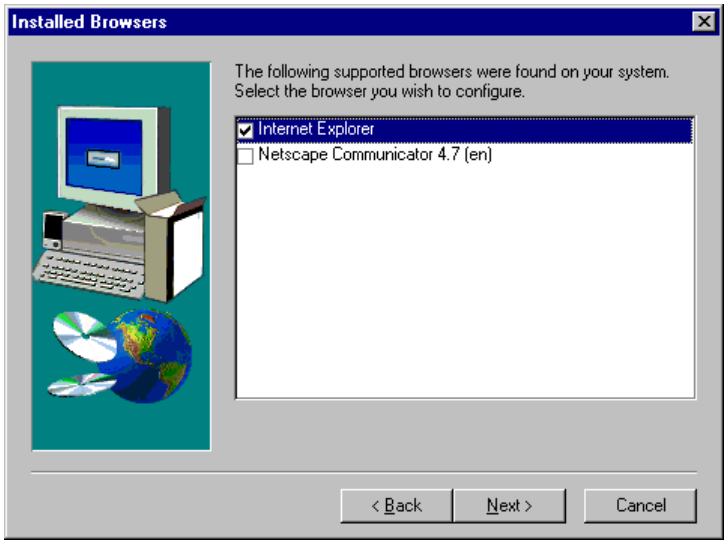
Note: Step 8 only applies to Custom installations.



8. Select the components you want to install using the checkboxes.

If you want to see which sub-components belong to a component, highlight the component and click the **Change** button.
The Select Sub-components dialog box appears. Now you can see the amount of space required for the individual sub-components. You may clear the checkboxes for the sub-components you do not want to install. When you have completed your sub-component selections, click **Continue** to return to the Select Components dialog box.
When you have finished component selection, click **Next >**.

Note: The installation program will detect if any component is missing or has an old version number. If so, the component will be selected for installation. It is recommended that you install the suggested component(s).

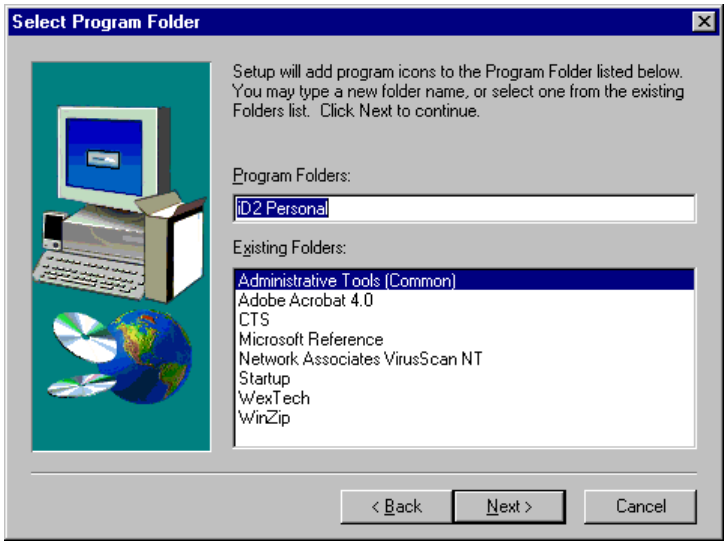


9. Select the browser(s) you want to configure for iD2 Personal and then click **Next >**.

Note: If Authenticator is selected for installation you can only select one browser. If you want to configure iD2 Personal for more than one browser, you will have to run the installation again.

Note: If you have an instance of Netscape running and you have selected to install iD2 Personal for this browser, it will be closed down automatically and a warning message will be shown.

10. If you selected Custom installation the Select Program Folder dialog box will be displayed. Otherwise, the installation program will run automatically until a message dialog appears (see step 12, 13 or 14).



By default iD2 Personal will be installed in the iD2 Personal program group. To specify another program group, select it from the list of program groups.
Click **Next >**. The Start Copying Files dialog box is displayed to show the current settings before you continue.

11. Click **< Back** if you want to return to a previous dialog box to make any changes.
    When you click **Next >**, the files will be copied to the target location and the Registry will be updated accordingly.
12. When you are installing an iD2 Personal version that contains Authenticator, the message **Do you want to add Authenticator to your Startup program folder?** will be shown. It is recommended that you answer **Yes** and have Authenticator automatically activated when you restart your PC.

Warning: When iD2 Personal has been installed and configured in your browser, HTTPS connections will only work correctly when Authenticator is running. (See “Troubleshooting” on page 13.)

---

13. If you chose to configure Netscape for iD2 Personal, then the message **Are you sure you want to install this security module? Module Name: iD2 Cryptographic Library** appears. Click **OK** to install the Cryptographic Module required for access to secure web servers. The message **A new security module has been installed** appears. Click **OK** to continue.
14. Your system will be updated and the Setup Complete dialog box will appear. You can choose to view the ReadMe file.
    Click **Finish** to complete the installation.
15. Finally, when you install an iD2 Personal version containing Authenticator, an information message is displayed to inform you that Authenticator’s CA certificate has to be installed.

Install the CA certificate in the browser that you selected in step 9 above.
The procedure will differ depending on the browser. Refer to your browser documentation for any further information you may need while performing this procedure.

Installing from Downloaded File

1. Click the **Start** button and select **Run**.
2. Browse to locate the downloaded file:
   `setupiD2Personal.exe`

Continue with steps 4 - 15 in section “Installing from the CD” on page 5.

After Installation

iD2 Personal may require the iD2 Technologies’ CA certificate to be available to your browser. If this is the case this certificate will be automatically installed with iD2 Personal.

The installation program should create the necessary settings in the browser configuration. It is recommended that you check that certificate installation was successfully completed.

The handling and inspection of CA certificates varies between different browsers and also between different versions of the same browser. Refer to your browser documentation for more information.

Configuring iD2 Personal

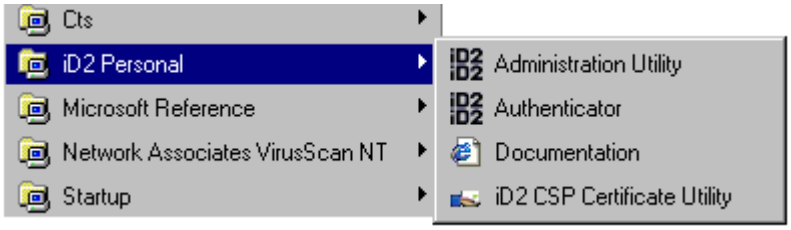
The necessary settings for the security proxy server will be created in your browser during the installation, if Authenticator has been installed. You can see the result if you open the option dialog box in your browser. The proxy server information may be found in different locations depending on which browser you are using. The Internet address and the port number are shown in the Security Proxy server configuration.

It is not normally necessary to change these settings. If, for some reason, your port is occupied for any other purpose, you may alter the port number. The port number in Authenticator must then be set to the same value.

iD2 Personal is now installed and configured.

Start Menu Program Group

When the installation procedure has been completed the iD2 Personal Start menu program group should contain the following selections:



Note: Authenticator will only be available if the installed iD2 Personal version contained that component.

For further information on the selections available in the program group refer to the reference section of this guide.

Starting iD2 Personal

Authenticator can be put in your startup folder during the installation (see “Installing from the CD” on page 5) to allow automatic start whenever your PC is started.

To manually start the program, click the **Start** button and select the Authenticator icon located in the iD2 Personal program group.

System Tray Icons

New icons will have appeared in your system tray:

The icon resembling a traffic light is the Authenticator icon, which will only be visible if Authenticator has been installed and started up. The other new icon is the iD2 CSP Certificate utility.

Further information on Authenticator and iD2 CSP Certificate Utility can be found in the reference section of this guide.

Troubleshooting

Troubleshooting after Installation

This section contains some simple troubleshooting procedures to help you solve any problems you may encounter after installation of iD2 Personal. Further troubleshooting information can be found in the on-line documentation, located in the iD2 Personal program group of the Start menu.

Smart Card and Smart Card Readers

The easiest way to verify that your card reader works is to follow this procedure:

1. Insert your smart card in the reader.
2. Start the iD2 Personal Administration Utility, found in the iD2 Personal program group.
3. Verify that the correct card reader is displayed in the list.
4. Click the **Change PIN** button. If the Change PIN dialog is displayed you have contact with both the reader and the card, and all is fine. Click **Cancel**.
   If a message **No token present** is displayed there is a problem accessing your smart card.
5. Check that the reader is properly connected to your computer.
6. Check that the reader power supply is connected.
7. Check that the smart card you are using is of a supported type (listed in the `readme.htm` file).

If the problem persists, refer to the “Troubleshooting” section of the on-line documentation, found in the iD2 Personal program group.

Secure Transactions

Authenticator is installed and configured as a proxy in your browser. This means that secure transactions from your browser will only work as long as Authenticator is active.

If HTTPS does not function correctly you should perform the following checks:

1. Make sure that Authenticator is running. The program icon that looks like a traffic light should be visible in the system tray.
2. Check the settings for the security proxy in your browser. The IP address should be 127.0.0.1 and port number should be 9999. Refer to your browser documentation for more information on this topic.
3. Check that the iD2 Technologies certificate is correctly installed. The name of this certificate is shown in "Certificates and Temporary Certificates" on page 31. Refer to your browser documentation for more information on this topic.

If the problem persists, refer to the “Troubleshooting” section of the on-line documentation, found in the iD2 Personal program group.

Microsoft CSP

If you have no certificates available to select, follow this procedure:

1. Check “Smart Card and Smart Card Readers” on page 13, to be sure that you can access your smart card and reader.
2. Check that you have the iD2 CSP Certificate Utility application icon in your system tray:

3. Remove and insert your smart card. The iD2 CSP Certificate Utility icon in the system tray should change to a spinning wheel as it reads the certificates from the smart card:

If you can not find the iD2 CSP Certificate Utility icon, or if it doesn't work correctly although you can access your smart card, it is recommended you reinstall iD2 Personal.

WebSigner

There are problems with loading plugins (i.e. WebSigner) in Windows 95 when you have several browsers installed. Thus, it is recommended you install the WebSigner component of iD2 Personal in one selected browser only.

Windows 2000

If you are unable to logon to Windows 2000 using a smart card, you should check that the physical connection of your card and card reader are working properly. To do this, start the Administration Utility in the

iD2 Personal program folder and insert the smart card. The card and its certificates should now appear in the list shown in the General tab of the Administration Utility.

If the certificates on the card are displayed under the General tab, the Administration Utility has been able to read the card. The problem is then probably related to the specific certificate being used or the authority of the certificate owner. Contact your domain or system administrator to find out.

Warning: Windows 2000 logon only supports card readers of type PC/SC.

Administration Utility

Utility Functions

The Administration Utility is a stand-alone application. Its purpose is to configure tokens to be used by various iD2 products. The application enables the user to specify whether the cryptographic functions should be performed by a real smart card token and/or by a virtual smart card token.

The Administration Utility is used to manage the following tasks:

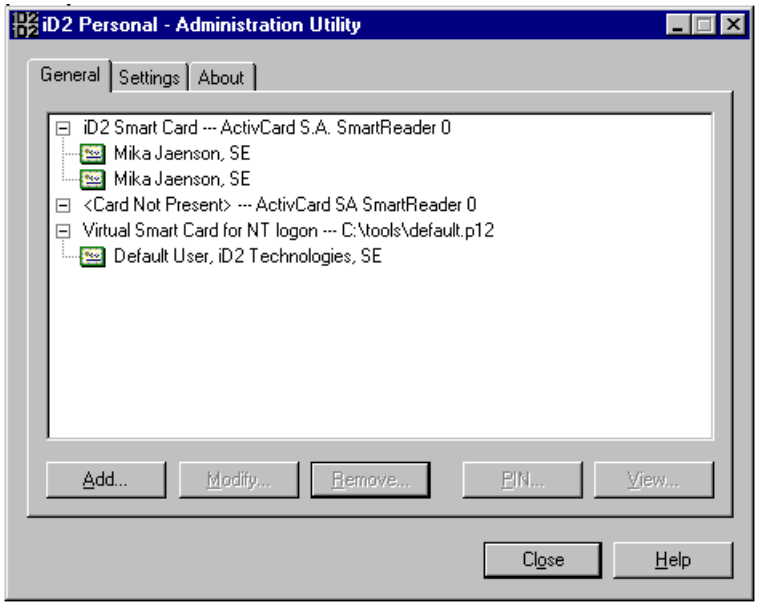
- view tokens
- configuring virtual smart cards and defining their properties, i.e., file locations
- changing PIN codes
- to do the necessary settings

Starting the Administration Utility

Warning: If you want to change the properties of a token, make sure that no active applications are currently using that token.

Click the **Start** button and select Administration Utility from the iD2 Personal program group. The program window with its three tabbed pages appears.

Administration Utility General Tab



Selecting the **General** tab displays all the active tokens. You may add, modify and remove tokens or change the PIN codes. It is also possible to look at the details of the individual tokens. At least one token must be configured before you can use any of its cryptographic functions.

For each token there is a description. Smart cards get their names from the card reader type. You set your own description when you define a virtual smart card. The tokens are listed alphabetically by their descriptions. The corresponding certificates are listed under each token.

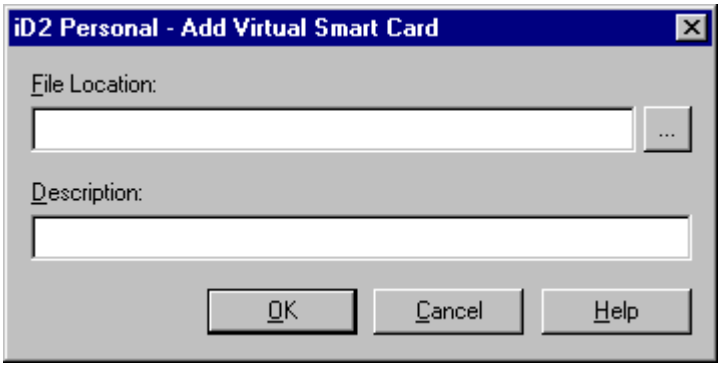
When you select a virtual smart card token, the **Modify** and the **Remove** buttons will be selectable.

Warning: The changes you make to a token will not take effect until you have restarted the application using that token.

Adding a Token

Smart card readers are automatically detected and configured when iD2 Cryptographic Library is initialized, i.e., when the computer is restarted (See also the “Administration Utility Settings Tab” on page 24).

Click the **Add** button to add a virtual smart card token. The Add Virtual Smart Card dialog box will appear.



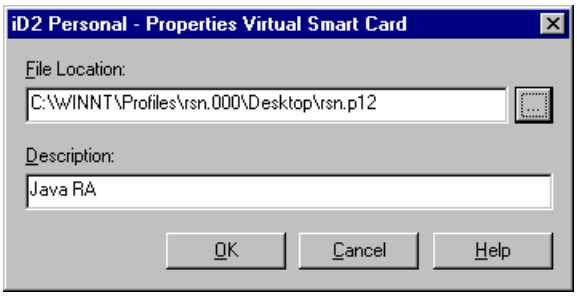
To complete this dialog box, you need a virtual smart card file of the correct type. Valid extensions are `*.pse` and `*.p12`. The default extension (`*.p12`) is assumed if no extension is present.

1. Enter the file name including the full path, or use the ... button to locate the virtual smart card file.
2. Give the virtual smart card a description that can be displayed in the list of available tokens.
3. Click **OK** to complete the dialog. The new token will appear in the list under the **General** tab.

Modifying a Token

To change the properties of a token, select the token in the list and click the **Modify** button. The Properties Virtual Smart Card dialog box will appear.

Note: Smart card readers are automatically detected and configured when the computer is restarted. Their properties cannot be changed.



To complete this dialog box, you need a virtual smart card file of the proper type. Valid extensions are `*.pse` and `*.p12`. The default extension (`*.p12`) is assumed if no extension is present.

1. Enter the file name including the full path, or use the ... button to locate virtual smart card file.
2. Give the virtual smart card a description that can be displayed in the list of available tokens.

3. Click **OK** to complete the dialog. The changed token will appear in the list under the **General** tab.

Removing a Token

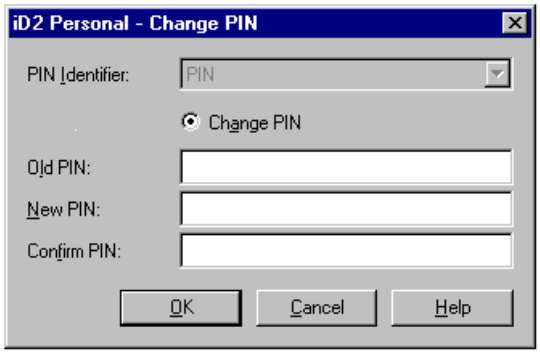
In the list under the **General** tab, select the token you want to remove. Click the **Remove** button. You will have to confirm the following message **Do you really want to delete the selected item?** before removal is carried out.

Note: A token associated with a smart card reader may not be removed.

Changing PIN

Note: If you are using a PIN-pad, the dialog box will look slightly different and you must enter the PIN codes at the device.

If you want to change the PIN codes of a smart card or a virtual smart card, click the **PIN** button. The Change PIN dialog box will appear.

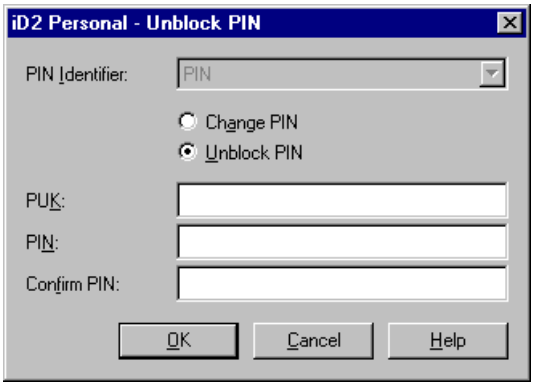


1. If the token currently selected has more than one PIN, you have to select the PIN identifier before changing the PIN. When only one PIN exists, the PIN identifier is not selectable.
2. Select option **Change PIN**.
3. Enter the old PIN and the new PIN and finally confirm the new one.
   - PIN codes for smart cards depend on the type of card. Normally they should be 4 - 8 characters long. All printable characters are accepted. Depending on the type of smart card in use, PIN codes may be case sensitive or not.
   - PIN codes for virtual smart cards can be of any length from 2 - 32 characters. All printable characters are accepted. PIN codes for virtual smart cards are case sensitive.
4. Click **OK** to complete the dialog.
5. The message **The PIN has been successfully changed** is confirmation of a successful change of PIN code.

Unblocking PIN

Note: The Unblocking PIN function may not be available at all since this option is configurable. If it is available and you are using a PIN-pad, the dialog box will look slightly different and you must enter the PIN codes at the device.

If your token has been blocked due to too many failed attempts to enter the correct PIN code, you may be able to unblock the PIN. Click the **PIN** button and select the **Unblock PIN** option. The Unblock PIN dialog box will appear.



1. If the token currently selected has more than one PIN, you have to select the *PIN identifier* before changing the PIN. When only one PIN exists, the *PIN identifier* is not selectable.
2. Enter the PUK code (i.e., the Personal Unblocking Key code).

Note: If you do not know the PUK code, you will have to contact your smart card supplier to get the information. You should also ask whether it is the current PIN or a new PIN that is required or if you need a new smart card. This may vary between different suppliers.

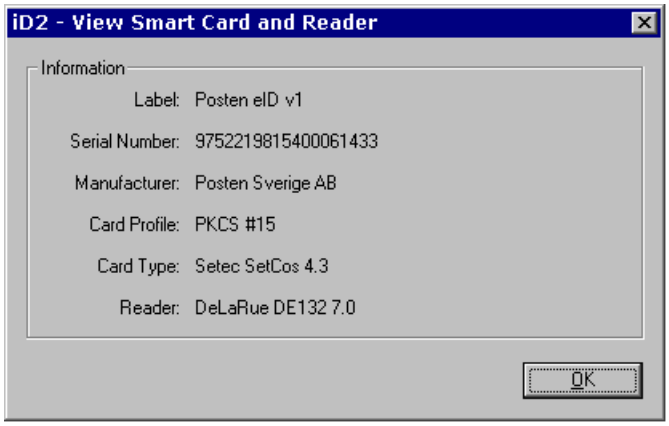
3. Enter the PIN twice to confirm it. Click **OK** to complete the dialog.

Viewing Details

It is possible to view token details as well as those of the certificates associated with the token.

View Token Details

To view the token detail information, select the token in the list and click **View**. Depending on the type of token the information displayed will vary. For a smart card, the information is presented like this.

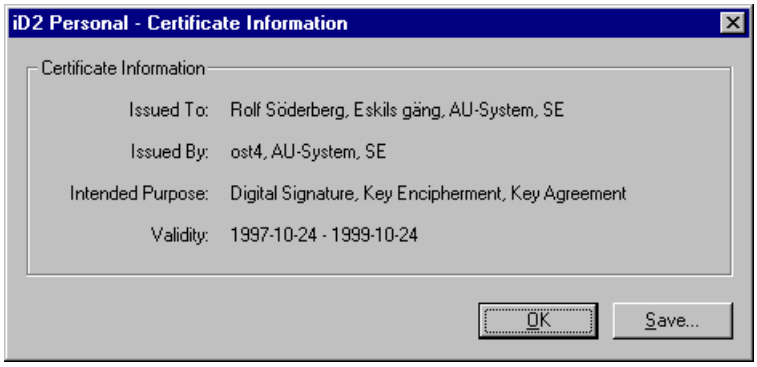


View certificate details

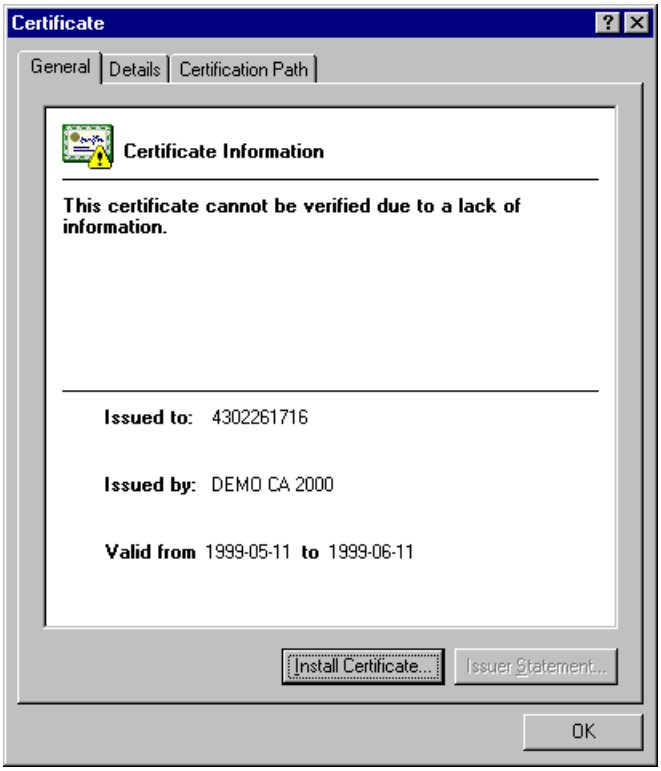
To view the certificate detail information, select the certificate in the list and click **View**.

A dialog box containing the certificate information will be displayed. The look may vary depending on your version of operating system.

One option is the following dialog box, where you may use the **Save** button to save the selected certificate to a file.

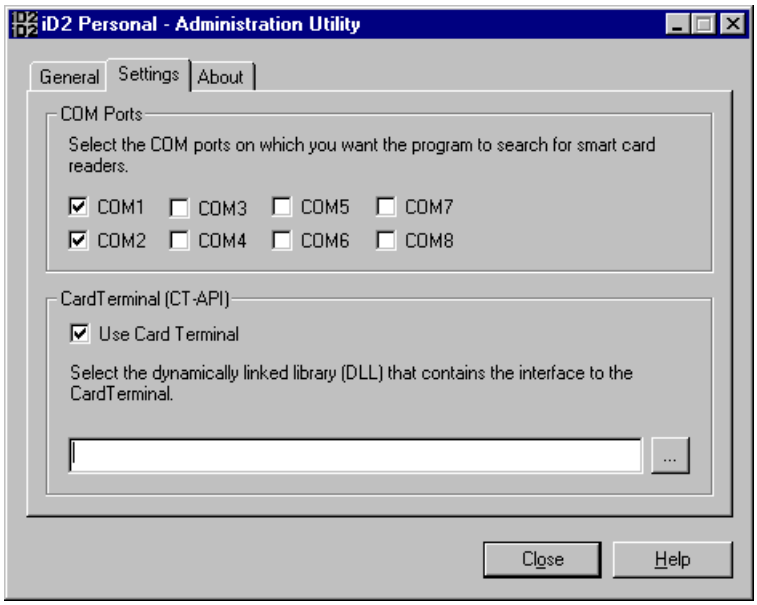


With Windows NT (Service Pack 4) as your operating system, the following alternative will be shown.



Certificate information is available under the various tabs. Click **OK** to return to the Administration Utility.

Administration Utility Settings Tab



The **Settings** tab has two purposes:

- To select the COM ports where the application should look for card readers.
- To configure a CardTerminal

COM Ports

The application will automatically search for smart card readers on all the COM ports selected in this dialog box. By deselecting COM ports, you can prevent the application mistaking any other device (e.g., a modem) for a smart card reader. For example, if you have problems locating your card reader, and you have a modem connected to COM port #1 with your card reader on COM port #2, simply select *COM2* and make sure all other COM ports are not selected.

CardTerminal

If you are using a smart card reader of the CardTerminal type you should select this option and then enter the path and file name of the DLL that contains the CT-API. Contact the supplier of your software for more information.

About Administration Utility

The **About** tab displays version information for the Administration Utility as well as for other components such as iD2 Cryptographic Library and iD2 Smart Card Server.

In addition, the operating system version is shown.

Messages from the Administration Utility

When working with the Administration Utility, there are a number of error messages that may appear.

File does not exist. Please enter an existing file.	
Cause:	You are trying to use a virtual smart card, but the file specified does not exist.
Action:	Specify a new name, for a valid file.
Incorrect PIN given	
Cause:	If you are using a smart card: Either an incorrect PIN has been entered, or the card may be locked due to too many incorrect PIN codes in a row. If you are using a virtual smart card: The PIN code is incorrect.
Action:	Enter the correct PIN code. If you are using a smart card: If the error remains you must unblock the card with the PIN unblocking code or obtain a new card.
Invalid PIN given	
Cause:	The format of the PIN is incorrect.
Action:	Enter the correct PIN code.
Operation failed	
Cause:	This message is displayed when you have tried to unblock a locked card and the unblocking operation has failed. An incorrect PUK (i.e., the personal unblocking key) has probably been used.
Action:	Check that you have entered the correct PUK code. **Note:** The PUK code is not your “normal” PIN code.
PIN is locked	
Cause:	This message is shown when too many incorrect PIN codes in a row have been entered and the card has been locked. The information on the card can no longer be accessed.
Action:	If you have the PUK code available, use it to unblock the card. Otherwise, call your customer support, to obtain a new card.
PIN length must be between %d and %d for this token.	
Cause:	You have typed a PIN code that is either too short or too long. %d is replaced by numeric values e.g., “between 2 and 32”.
Action:	Specify a new PIN code with the expected length.
Specified virtual smart card already exists.	

Cause:	You are trying to define a new virtual smart card, but it already exists. You are not allowed to specify a virtual smart card more than once.
Action:	Specify another name for the virtual smart card.
The PINs you typed do not match. Enter the new PIN in both text boxes.	
Cause:	You are trying to change PIN but the contents of the New PIN and the Confirm New PIN text boxes are not equal.
Action:	Specify the same PIN code in both text boxes.
The specified file is not a virtual smart card. Valid extensions are '.pse' or '.p12'.	
Cause:	This message is shown if an invalid file name is entered in a dialog box. Non-existent files are accepted to allow for token creation that has to be supplemented with a virtual smart card file at some other time.
Action:	Specify a file name with the extension .pse or .p12.
The specified library is not a valid CardTerminal library.	
Cause:	This error only occurs when you are trying to configure a card reader using the CT-API standard. You are specifying a DLL, but the file does not contain the functions required.
Action:	Specify the correct file name. Check with your card reader supplier for details.
Token not present	
Cause:	The token can not be found. If you are using a smart card, the card is not in the reader or cannot be used. If you are using a virtual smart card, the file specified can not be found or used.
Action:	If you are using a smart card: Insert the card into the reader and try again. Check the connection to the card reader. Try with another card, to make sure the card is all right. If you are using a virtual smart card: Check that the specified exists and that is has the correct file type.
Unexpected error (error code)	
Cause:	This message is used in various unexpected error situations. The error code gives the details.
Action:	Save the error code information, and call customer support.

Authenticator

Introducing Authenticator

Authenticator is client software for secure authentication of a user in a web environment. It is based on the standard client authentication procedure in the SSL protocol. This means that any standard web server that uses client authentication can interact with Authenticator and give selective access to information on the server. Secure document systems, electronic banking and electronic commerce are examples of applications where Authenticator could be used to improve security.

Authenticator, which can be integrated with any browser using the SSL security proxy protocol, uses smart cards to perform the authentication.

Common Authentication Procedures

Many systems perform some kind of access control before giving services to users. This access control is very often based on simple solutions with user-id and passwords. This kind of authentication involves a considerable amount of administration and it is also very insecure. Passwords can be copied or stolen. This means that user ID/password combinations do not give the necessary authentication needed in an open communication environment.

New authentication solutions based on asymmetric key systems are being developed. They have advanced security features that effectively hinder intruders from breaking into a system or faking the authentication procedure. The drawback with many of these solutions is that they often use keys stored in the computer when performing authentication. Practically, this means that the system will authenticate the computer, not the user.

Secure Authentication with Smart Cards

The most important concern in secure authentication is to be sure that the private key is really private to its owner. The key must be protected from illegal use and from other threats such as copying. This level of security can be added if the private key used in the authentication procedure is stored on a smart card. A key stored on a smart card can never be copied and a personal password, called the PIN code, protects its usage.

Securing the authentication procedure by means of a smart card is the best way to prove the true identity of the user.

One Identity for Mobile Users

The current implementations of client side authentication in browsers lack the capability of using only one identity. Since the identity is stored inside the browser it hinders the user from carrying his identity with him. If the user is mobile, this implies that he will have different identities at different locations. This is not very convenient. When smart cards are used for authentication, this problem does not exist. The smart card is the best way of securing the identity of a user and also results in mobility. Wherever he uses his card to identify himself, the identity will always be the same.

Client Authentication and SSL

The SSL protocol has become a standard for secure communication over the Internet. The protocol has the capability to authenticate both communicating parties and secure the communication against eavesdropping. The potential for client side authentication is however seldom exploited. The method used is the same as for the more commonly used server authentication, when the server verifies itself towards the user.

The user is in possession of a private key that is “challenged” by the server. The client software encrypts the challenge (a random number) with the private key and the response is sent back to the server. Since a correct response can only be achieved if the user is in the possession and control of the private key, the method can give very secure authentication.

Authenticator and Client Authentication

In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. Authenticator acts like a proxy server.

Socks (or "SOCKS") is a protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet. Authenticator can be configured to enable SOCKS.

Authenticator is installed in the client and plugs in to the traffic between the browser and a web server. When a server requests client authentication, Authenticator will respond with information retrieved from the user's smart card.

Since the private key used in the authentication procedure is protected by a PIN code, the user has to enter this PIN code in a dialog box before execution can take place. Authenticator handles the rest of the authentication procedure transparently.

Standard Web Server

Since Authenticator uses the SSL protocol to perform the authentication any standard web server that makes use of client side authentication can be used. This includes servers such as Apache, Microsoft IIS and Netscape Enterprise Server. All these servers include advanced capabilities to connect the proven user identity and to selectively present information to the user. A standard web server together with Authenticator means that current investments in servers can be protected.

Certificates and Temporary Certificates

Secure transactions are based on authentication of the two parties exchanging data. Authentication is performed by means of certificates that have been issued by Certifying Authorities (CAs).

Web browsers like Netscape and Internet Explorer contain CA certificates of all trusted CAs. During the installation of iD2 Personal a new CA certificate will be added. The name of this CA is “Authenticator Signature, iD2 Technologies AB, SE”.

Certificates are exchanged during the negotiation between Authenticator and a security server. An incoming certificate from a security server is examined by Authenticator, which has its own set of trusted CAs. When a certificate is accepted, a temporary certificate will be issued by Authenticator and sent to the web browser. This temporary certificate, has iD2 Technologies as CA. It contains information about the security server. Since iD2 Technologies is an accepted CA in the browser, the negotiations will succeed.

Strong Encryption

Due to export regulations in the U.S., web browsers from U.S. vendors have limited capacity for encryption. The length of the key used in the exported versions is so short, that even with low investment, the data can be cracked within hours. The SSL protocol however has the capability to use full-length ciphers. Authenticator makes full use of this.

Builds on Cryptographic Library

Authenticator builds on top of Cryptographic Library, which is used to perform the low-level cryptographic routines. All the features of Cryptographic Library, such as transparent handling of virtual smart cards, are therefore also included in Authenticator.

Starting Authenticator

If the autostart option was selected during installation, Authenticator will start automatically when you start your computer.

Use the **Start** button to launch the program manually. Normally, the program icon is found in the Start menu program group named iD2 Personal.

Running Authenticator

When Authenticator is active it runs minimized, i.e., without a window. The icon resembles a traffic light.

Authenticator automatically detects in which environment it is running. In Windows NT 4.0, Windows 95/98 and Windows 2000, the icon is displayed in the system tray.

The colors of the traffic light in the icon indicate the status of the SSL connections.

- **Idle**. No connection is established. In this state none of the lights are on.
- **Connecting**. **Red** and **yellow** lights indicate Authenticator is attempting to establish a connection.
- **Negotiating**. **Green** and **yellow** lights indicate the parameters of the SSL protocol are being negotiated.
- **Completed**. Negotiation and transfer is completed. This state is indicated by a **green** light.
- **Tunneling**. Authenticator is not able to negotiate a secure connection, as the server does not support SSL protocol version 3. Authenticator will pass data transparently between the server and the browser. This state is indicated by a **green** light.
- **Completed tunneling**. Transparent transfer, i.e., transfer without additional security from Authenticator, is completed. This state is indicated by a **green** light.
- **Error**. A **red** light indicates Authenticator failed to establish a secure connection. A timeout will occur if completion is not obtained within the maximum time allowed.

  Normally a browser message will indicate the reason for the failure. Use this message to correct the problem situation.

Note: The status can either be viewed in the **Status** tab of the Authenticator user interface, or by the control tip text displayed when the pointer is placed over the program icon.

Interacting with Authenticator

Interaction between Authenticator and the user can be divided into two categories:

1. **User initiated**. This happens, for example, when the user wants to change settings, or select ciphers. The user initiates the interaction

via the icon in the system tray and the Authenticator dialog box will be displayed.

2. **Authenticator initiated**. Different events occur when Authenticator is negotiating a secure SSL connection. These events are mainly related to identification of the user and his certificate(s). Some form of user interaction will be required to handle the situation. Information about the situation and optional user alternatives will be displayed in various dialog boxes.

Note: The dialog boxes and the available options are described in "Authenticator Initiated Dialog" on page 37.

System Tray Icon and Commands

Mouse commands can be used on the icon in the system tray. Click the right mouse button on the icon to open a popup menu that contains the following commands:

- **Open** to show the program's dialog box.
- **Quit** to stop the execution of the program.

You can also double-click the icon to open the dialog box that manages the application, and obtain access to the following tabbed pages:

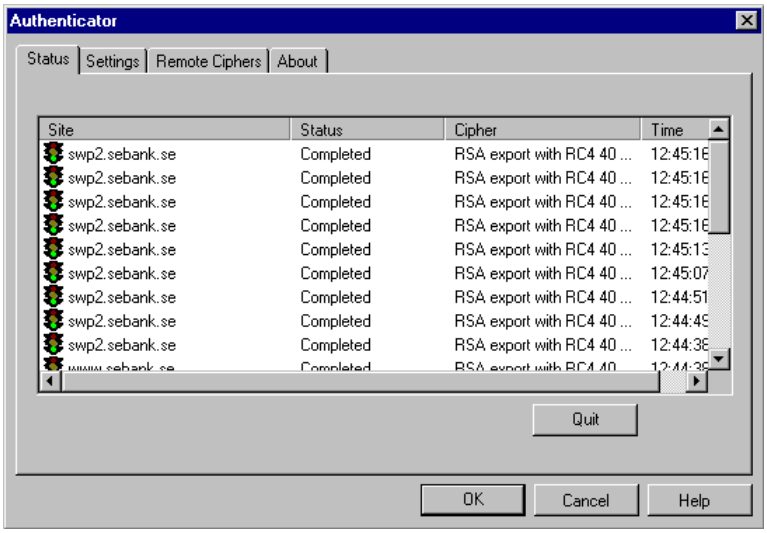
- Status
- Settings
- Remote Ciphers
- About

The Authenticator Dialog Box

When Authenticator is opened, the dialog box is displayed with its four tabbed pages.

Status

To follow the status of the SSL negotiation and the transfer of data in a secure transaction click on the **Status** tab. You can display this page while the browser is connecting to a secure server.



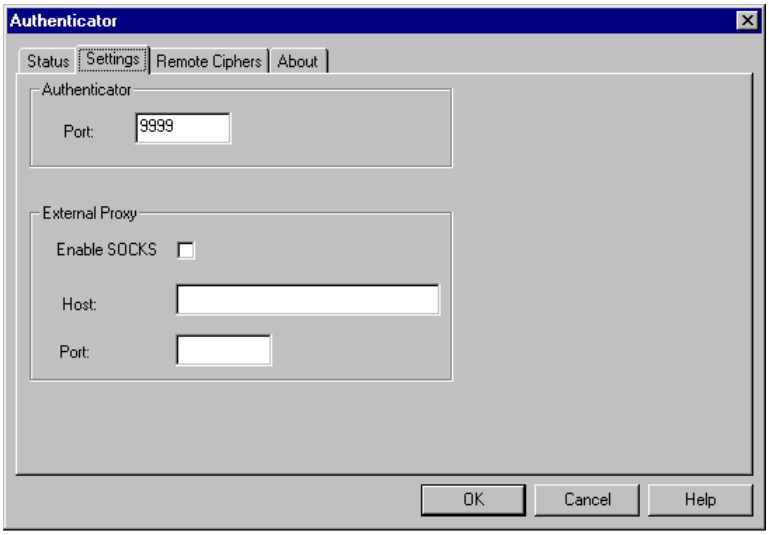
The HTML page loaded in this example contained several objects, (e.g., GIF or JPEG pictures). Authenticator performs a separate SSL negotiation for each object.

Possible status conditions are:

- **Idle**. No connection is established.
- **Connecting**. Attempting to establish a connection.
- **Negotiating**. The parameters of the SSL protocol are being negotiated.
- **Completed**. Negotiation and transfer is completed.
- **Tunneling**. Authenticator is unable to negotiate for a secure connection, as the server does not support SSL protocol version 3. Authenticator is passing data transparently between the server and the browser.
- **Completed tunneling**. Transparent transfer, i.e., transfer without additional security from Authenticator, is completed.
- **Error**. Failed to establish a secure connection.

Authenticator Settings

The proxy settings are stored in the `Authent.ini` file. When Authenticator is started the settings are loaded and, when quitting, the current settings are stored.



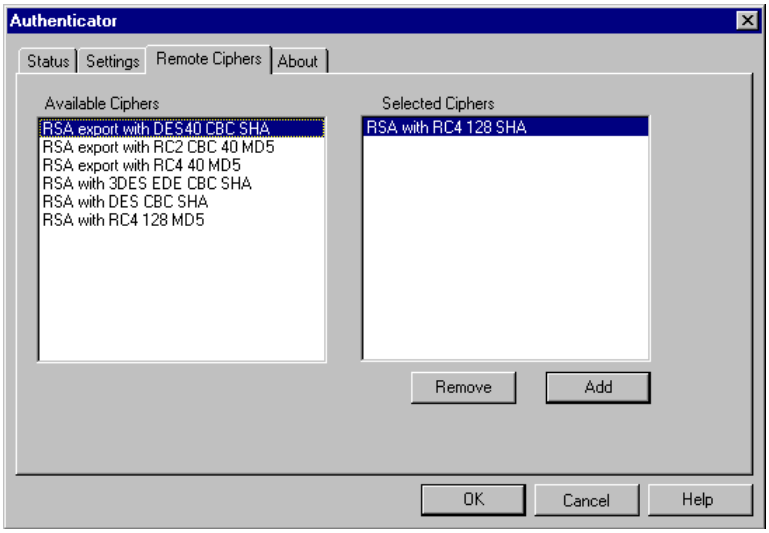
The available settings for Authenticator are accessible from the **Settings** tab in the dialog box.

- **Authenticator Port**. This text box indicates which port to use when Authenticator communicates with the web browser.
- **External Proxy**. If an external proxy, e.g., a firewall, is passed on the way to the server, its address and port number must be specified here. At installation, the proxy server settings of the default browser are checked. First, if a Security proxy is specified, its settings are automatically moved to the External Proxy in Authenticator. Secondly, if a SOCKS proxy is specified, its settings are moved to Authenticator and the *Enable SOCKS* checkbox is selected.

Authenticator Remote Ciphers

In the **Remote Cipher** page in the dialog box, the cipher(s) that Authenticator will present to the server, during the SSL negotiations, are listed.

Note: Due to export regulations in the U.S., all ciphers may not be available in exported versions of Authenticator.



When the list of selected ciphers is empty, the server and Authenticator will negotiate using the list of available ciphers, starting with the highest security level and working down. This will ensure that an agreement can be reached.

The list of selected items is empty after setup. It is not necessary to add ciphers to the list of selected ciphers.

Warning: If ciphers are added to the list of selected ciphers, negotiations between the server and Authenticator will use only those selected, so agreement may not be reached.

Add Ciphers

From the list of available ciphers, one or more ciphers can be added to the list of selected ciphers. Select the cipher and then click the **Add** button to move it to the list of selected ciphers. New ciphers are added to the bottom of the list.

Note: The order of the ciphers in the Selected Ciphers list is of great significance. The most secure cipher should be placed at the top of the list to ensure that it is negotiated first. If an agreement can be reached on this cipher, the highest level of security is obtained.

Remove Ciphers

To remove ciphers from the selected list, highlight the cipher and then click the **Remove** button. This moves the cipher back to the list of available ciphers.

Cipher Description

A variety of cryptographic algorithms are supported by SSL. During the handshake, the RSA public-key cryptographic system is used.

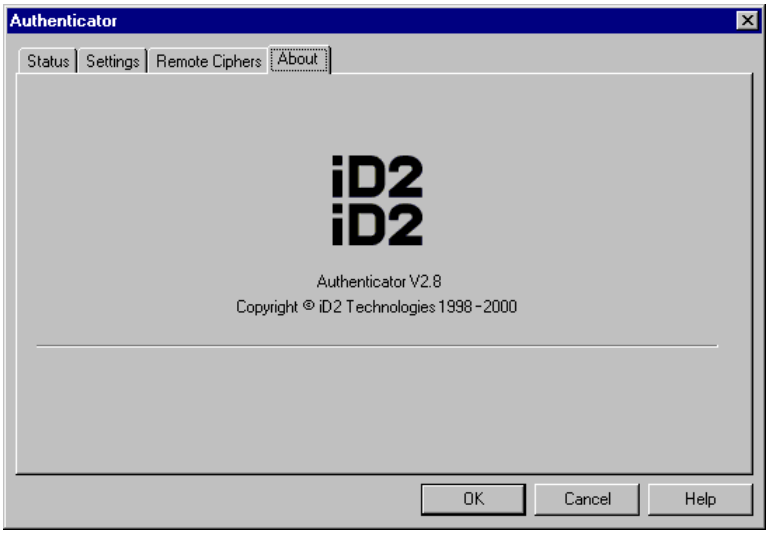
The server determines the types of cipher. Included are RC2, RC4, DES, and triple-DES. The SHA-1 and MD5 message-digest algorithms are also used. The public-key certificates are in accordance with the X.509 syntax.

The cipher names used indicate a combination of cipher methods, key lengths, and message-digest algorithms.

The following list presents the ciphers ordered by security level. The first item is the most secure and the last item is the least secure.

- RSA with 3DES EDE CBC SHA (key length 3*56)
- RSA with RC4 128 SHA (key length 128)
- RSA with RC4 128 MD5 (key length 128)
- RSA with DES CBC SHA (key length 56)
- RSA export with DES 40 CBC SHA (key length 40)
- RSA export with RC2 CBC 40 MD5 (key length 40)
- RSA export with RC4 40 MD5 (key length 40)

About Authenticator



Selecting the **About** tab in the dialog box displays the current version of Authenticator.

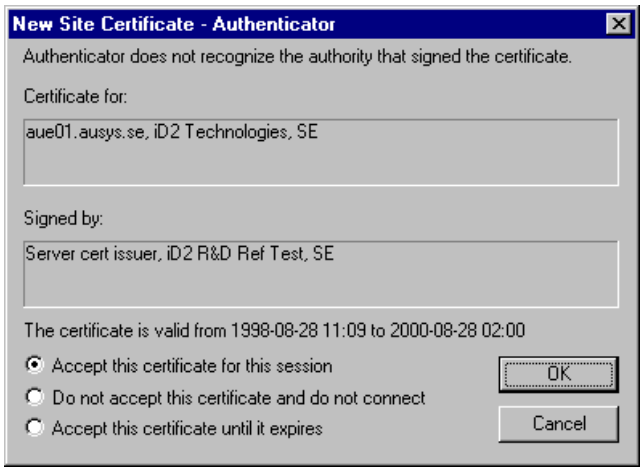
Authenticator Initiated Dialog

Events can occur when Authenticator is negotiating a secure SSL connection, and different interaction dialogs may be initiated. The interaction required is explained in the dialog boxes.

In addition, self-explanatory error messages are displayed when a problem occurs that cannot be resolved by user input.

New Site Certificate

When the server being contacted presents a certificate that is signed by an unknown Certification Authority, the New Site Certificate dialog box will appear.



The user has three options:

1. Accept the certificate for this session only. This dialog will then appear each time this server is contacted as long as the Certification Authority is not among those accepted in Authenticator's trusted server storage.

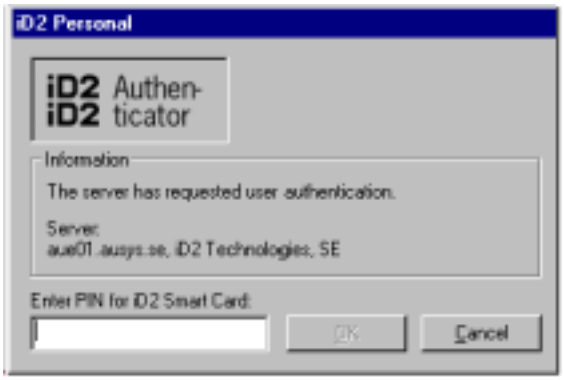
2. Do not accept, which will result in the connection being refused.

3. Accept the certificate and install it in Authenticator's trusted server storage.

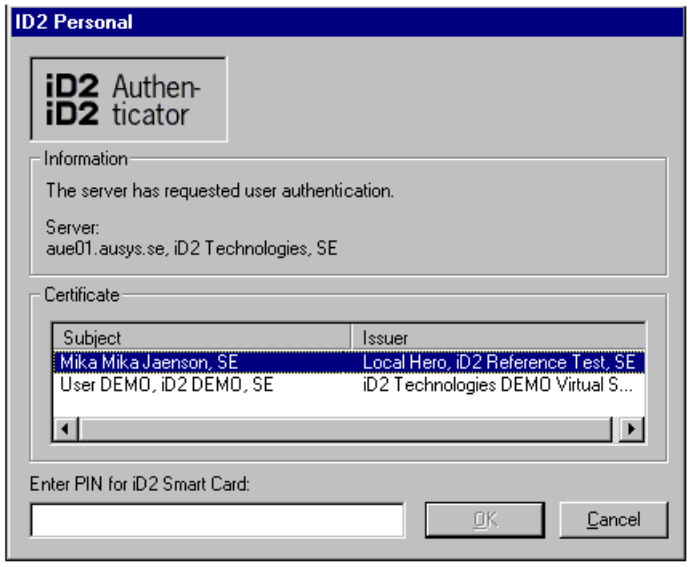
User Authentication

This dialog appears when the server being contacted requests client authentication. There are two different layouts of the dialog box depending on whether the user has one or more certificates installed.

Note: If you are using a PIN-pad, the dialog boxes will look slightly different and you must enter the PIN codes at the device.



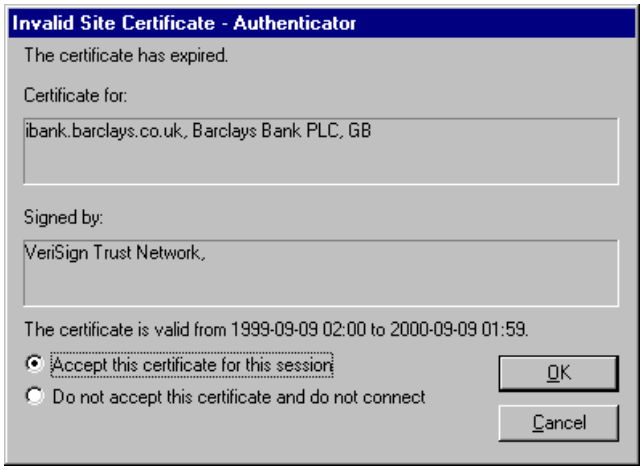
Only one certificate is installed. Enter the PIN and click **OK**.



More than one certificate is installed. Select a certificate, enter the corresponding PIN and click **OK**.

Invalid Site Certificate

The Invalid Site Certificate dialog box may appear for different reasons. Either the certificate has expired or it may have been revoked.



The user has two options:

1. Accept the certificate for this session only. This dialog will then appear each time this server is contacted as long as the server presents a certificate that has been revoked or that has expired.

2. Do not accept, which will result in the connection being refused.

CSP

Introduction to CSP

iD2 Personal may be used to add smart card support to Microsoft products such as Windows 2000, Internet Explorer, Outlook 98, and Outlook Express.

This section describes in detail how to configure CSP in the Microsoft environment after installation of iD2 Personal.

Note: If you are using a PIN-pad device, the standard dialog boxes requesting a PIN code may look different or not appear. Instead, you will get a signal from the PIN-pad.

Cryptographic Service Provider

iD2 Personal is installed as a Microsoft CSP (Cryptographic Service Provider) during the installation procedure. Through this API, various Microsoft products (Windows 2000, Internet Explorer, Outlook 98, and Outlook Express) can use the functions provided by the underlying product, iD2 Personal. Among the available functions are support for certificates and keys stored on smart cards and accessed via different smart card readers.

You can use the CSP to access secure web sites in Internet Explorer, and to sign and encrypt mail in Outlook 98 and Outlook Express.

Smart card logon to Windows 2000 is also supported by the CSP.

Note: This requires that a Windows 2000 server has issued a specific certificate for this purpose. The CSP supports the downloading of this certificate on to the smart card under certain conditions. You have to check with your system administrator or security manager that there is enough free space on the card and that your smart card can be updated.

Supported Products

Before using iD2 Personal you need to configure your applications. This document describes configuration and usage of iD2 Personal in the following products:

- Microsoft Internet Explorer

- Microsoft Outlook 98
- Microsoft Outlook Express
- Microsoft Windows 2000

Internet Explorer

You may use iD2 Personal in SSL negotiations in your Internet Explorer. When a secure site (https://……) requests client authentication, you may use the certificate on your smart card to connect to the server. This section describes this procedure.

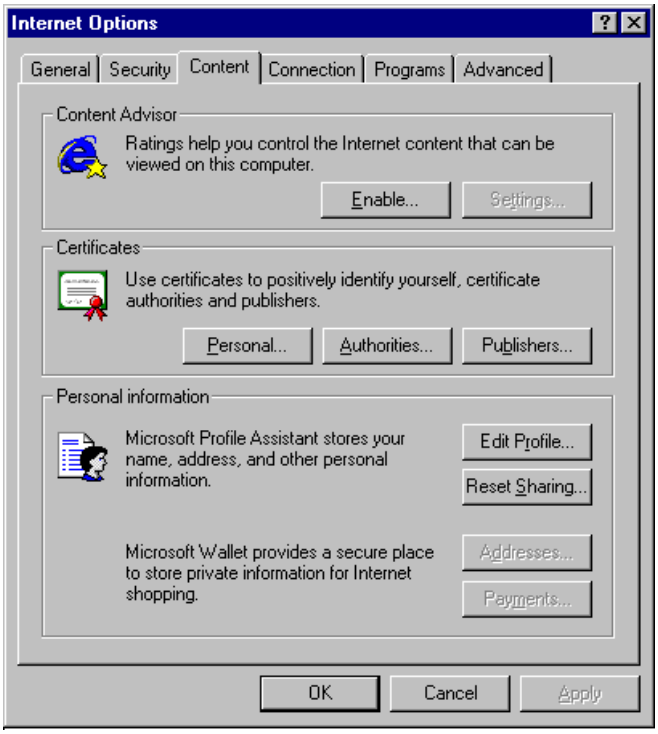
Warning: You cannot use this procedure in conjunction with Authenticator. If Authenticator has been installed, you must delete the browser Secure Proxy settings that point to Authenticator. If an external Proxy server is used, replace the Secure Proxy settings with those of the external server.

Configuration in Internet Explorer

When iD2 Personal is installed, if the CSP component is selected for installation, CSP will be available to Internet Explorer. No additional configuration is required.

Viewing Available Certificates

Select **Internet Options** from the **Tools** menu, and click the **Content** tab to display the *Certificates* option.


Internet Options
General
Security
Content
Connection
Programs
Advanced
Content Advisor
Ratings help you control the Internet content that can be viewed on this computer.
Enable...
Settings...
Certificates
Use certificates to positively identify yourself, certificate authorities and publishers.
Personal...
Authorities...
Publishers...
Personal information
Microsoft Profile Assistant stores your name, address, and other personal information.
Edit Profile...
Reset Sharing...
Microsoft Wallet provides a secure place to store private information for Internet shopping.
Addresses...
Payments...
OK
Cancel
Apply

Click the **Personal** button to view the available certificates.

Details of the selected certificate may be displayed by clicking the **View Certificate** button.

SSL Client Authentication

When connecting to a secure site you will be prompted for the certificate to use, with the Client Authentication dialog box.

You may view the certificate details. When you have selected a certificate you will be prompted for the PIN code.

Enter the PIN code and you may access the secure site, using the certificate on the smart card to identify yourself.

Of course, the connection can only be established if your certificate is accepted by the server.

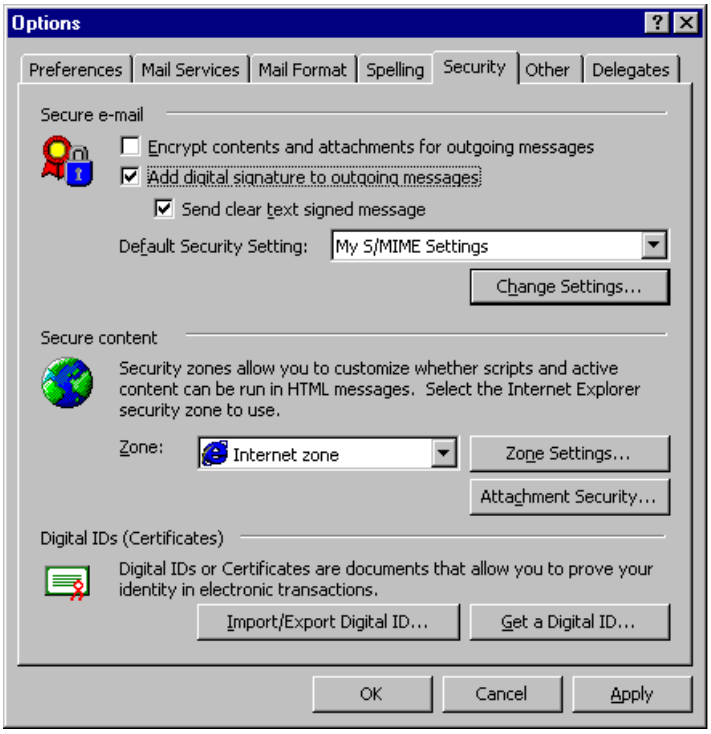
Microsoft Outlook 98

In Outlook 98 you can use the CSP in two different ways, either to sign and/or encrypt **all** outgoing mail, or on an individual basis (i.e., to specify for each mail whether to sign and/or encrypt it or not).

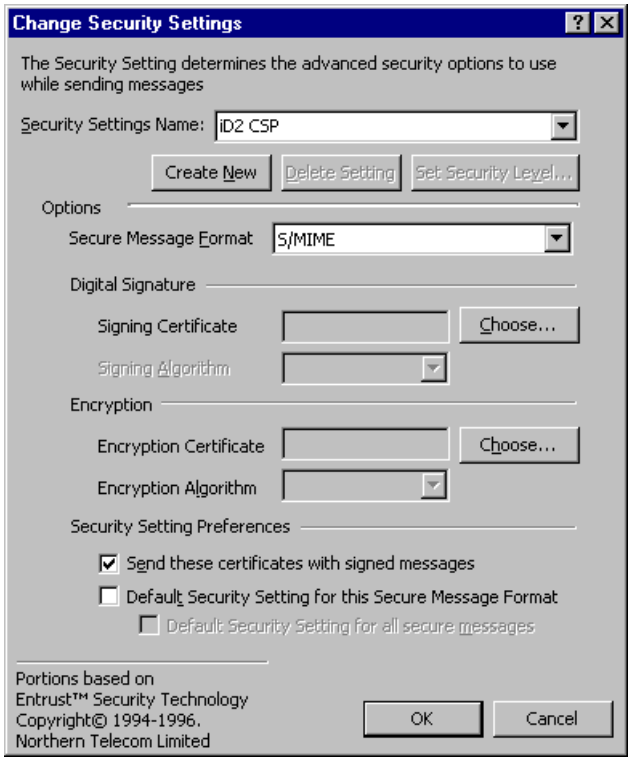
Configuration in Outlook 98

After installation of iD2 Personal, you need to configure Microsoft Outlook 98 to use iD2 Personal as the CSP. This is described in this section.

Be sure to have your smart card inserted in the card reader, then, in Outlook 98, select **Options** from the Tools menu. The following dialog box will be displayed.



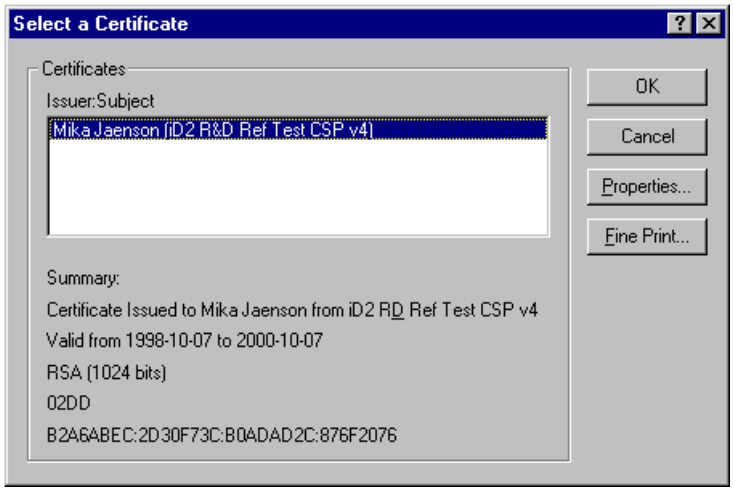
You need to define a new Security Setting. Use the **Change Settings** button to open the Change Security Settings dialog box.



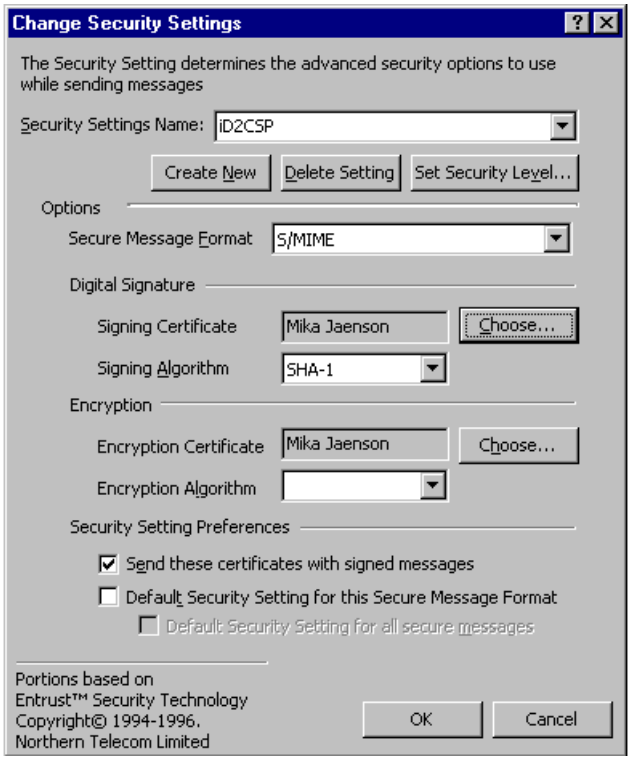
Click the **Create New** button and enter a Security Settings Name of your own choice.

Then click the **Choose…** button next to *Digital Signature*, *Signing Certificate* to select the certificate to use when signing your mail. The Select a Certificate dialog box will appear.

Select the certificate you want to use (normally there will be only one choice).



Click the **OK** button. This will take you back to the Change Security Settings dialog box.



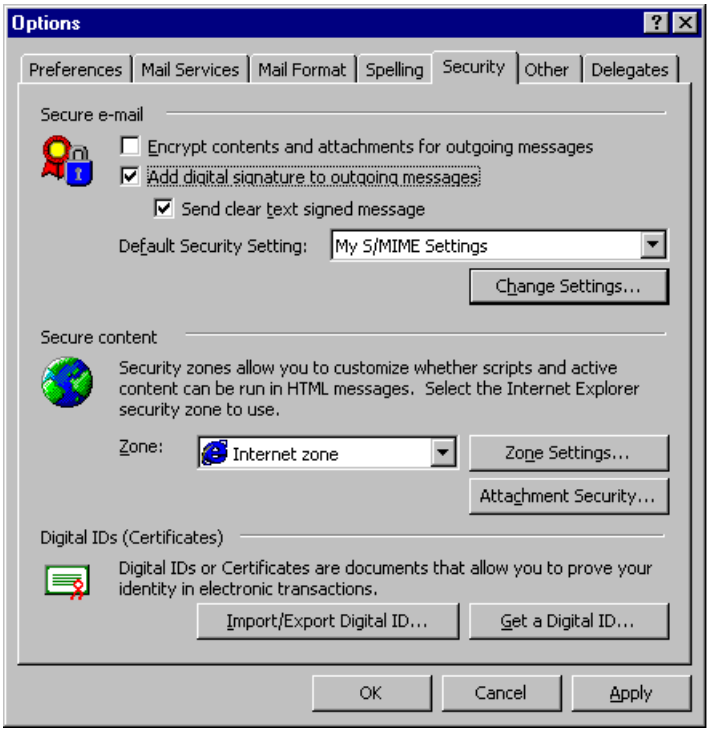
Select a certificate for encryption. Click the **Choose…** button next to *Encryption*, *Encryption Certificate* to select a certificate to use for encryption. Select the certificate and click the **OK** button.

Click **OK** in this and the successive dialog box, and you have finished configuring CSP for Outlook 98.

You are now ready to use iD2 Personal to sign and encrypt your Outlook 98 mail and to use it when connecting to secure sites in Internet Explorer.

Signing and Encrypting All Outgoing Mail

If you want to sign and/or encrypt all outgoing mail, select **Options** from the **Tools** menu and click the **Security** tab.

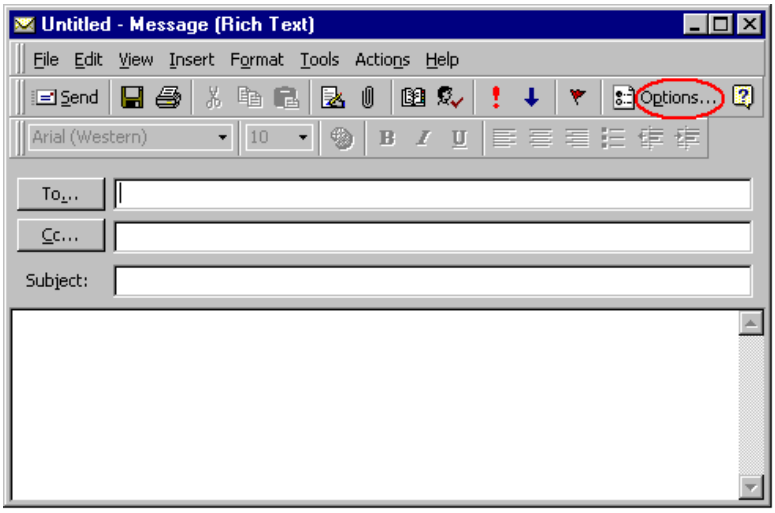


Select *Add digital signature to outgoing messages* and click the **Apply** button. After this, you will be prompted to sign each mail before it is sent. You may also specify *Encrypt contents and attachments for outgoing messages* to encrypt all messages.

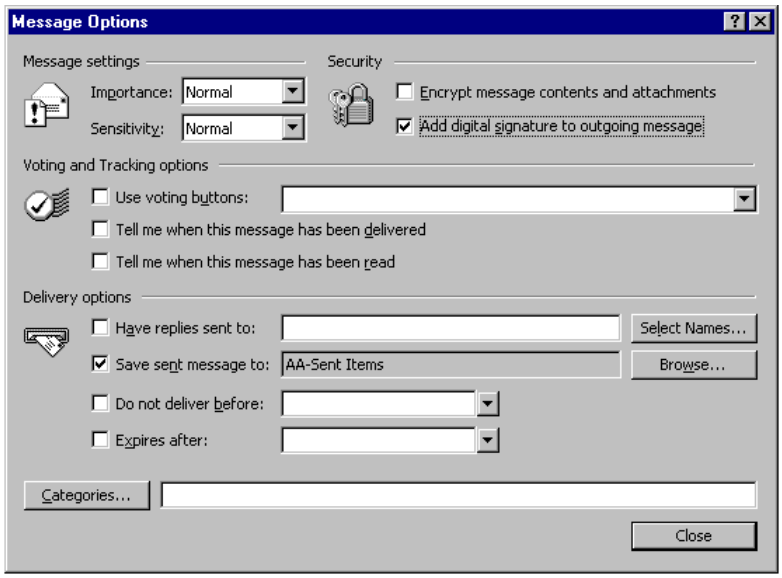
You may still send unsigned and/or unencrypted mail by canceling the selection for *Add digital signature to outgoing message* and/or *Encrypt contents and attachments* in the Options dialog for the individual message.

Signing and Encrypting Individual Mail

If you have not specified any security options and want to sign and/or encrypt an individual mail, use the **Options** button when creating the mail.



Clicking the **Options** button will open the Message Options dialog box.



Select *Add digital signature to outgoing messages* and click the **Close** button. You will then be prompted to sign the mail before it is sent.

If you want to encrypt the mail as well, select *Encrypt message contents and attachments* before clicking the **Close** button.

Sending Signed Mail

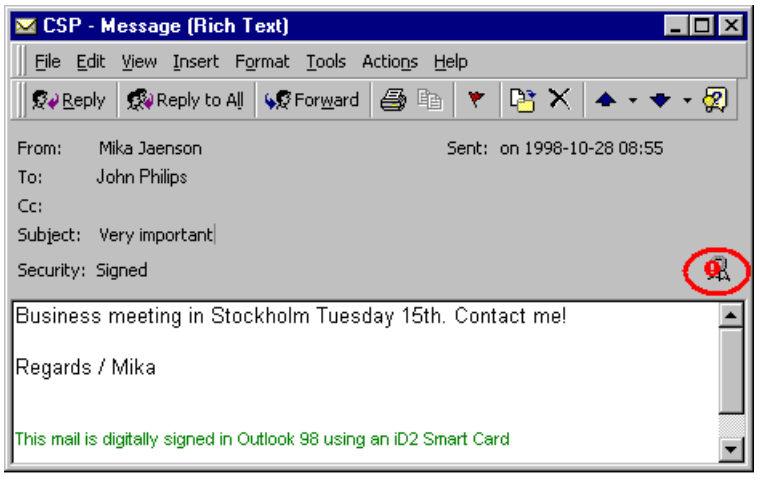
When your mail is ready to be sent, and you have specified that it should be signed, the following dialog box will be displayed.

Enter your PIN code and click the **OK** button to send your signed mail.

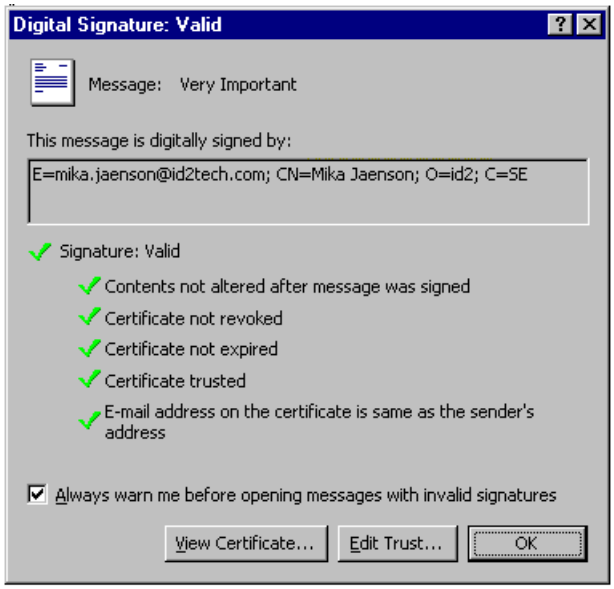
Note: If you click the **Cancel** button, your mail will still be sent, but an invalid signature will be generated on the mail. When arriving at the destination, the user reading the mail will get an **Invalid signature** message.

Receiving Signed Mail

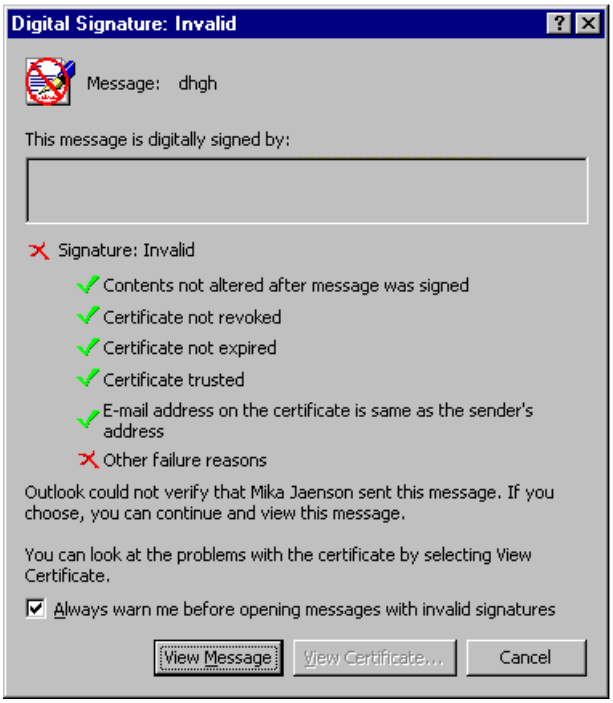
When you receive a signed mail and the signature is valid, the following message is displayed.



By clicking the icon on the far right of the message header you may view the signature details of the signed message.



When you receive a message with an invalid signature the following dialog box appears when opening the message.



You may still view the message content by clicking the **View Message** button.

Sending Encrypted Mail

When you want to encrypt the mail you are going to send, you need access to the certificate of the receiver.

Getting the Certificate

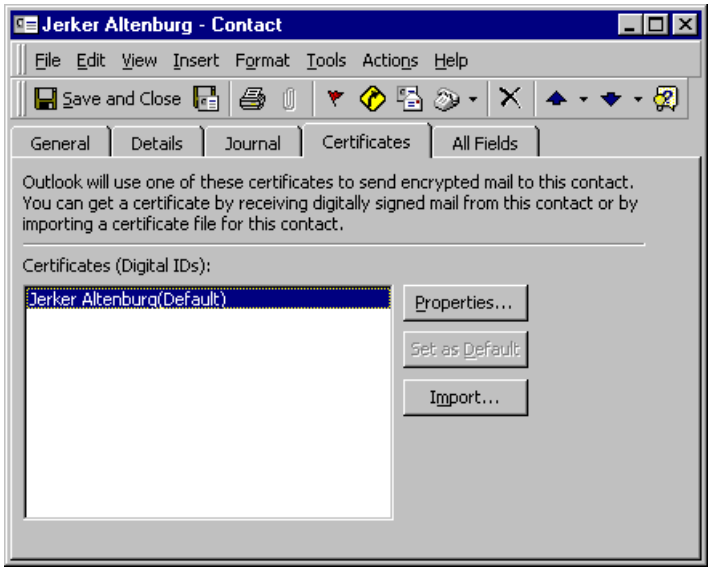
To use the certificate of the receiver you must have it stored in the **Contacts** folder of Outlook 98. An easy way to obtain it is to receive a signed mail from this person. The signed mail includes the certificate and the certificate is easily added to your contacts:

1. Open the signed mail
2. Place the pointer on the sender name in the *From* field
3. Click the right mouse button
4. Select **Add to Contacts**

You may get the certificate in other ways, e.g., find it in a directory, and use the import function of the **Contacts** folder to import the certificate. When you have obtained the certificate you may start using it to encrypt mail.

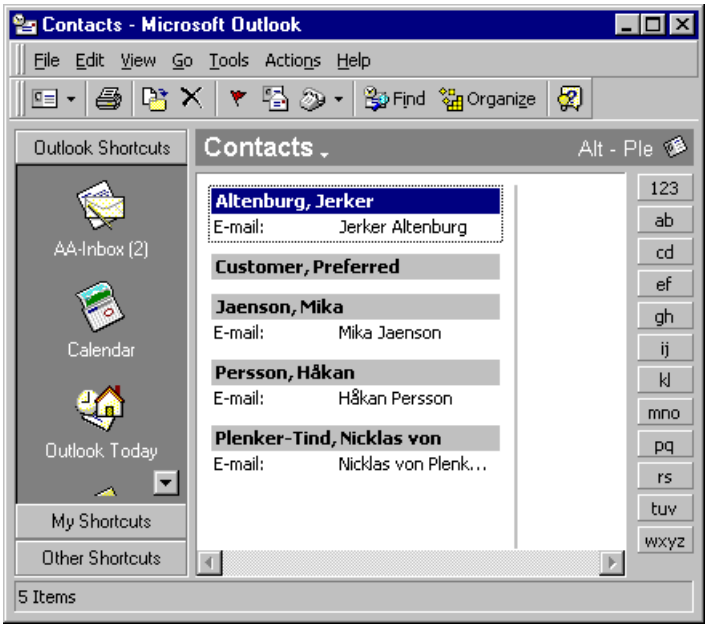
Using the Certificate

As previously stated, you need to have the certificate of the receiver in your **Contacts** folder. You may check the certificate by double-clicking the contact and selecting the **Certificates** tab:



Sending the Mail

To send an encrypted mail you must open your **Contacts** folder.



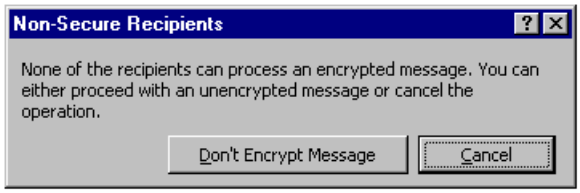
Use the following procedure:

1. Place the pointer on the selected contact
2. Click the right mouse button
3. Select **New Message to Contact**
4. Click the message **Options** and select *Encrypt message contents and attachments*.

The mail will now be encrypted when sent.

No Certificate Present

If Outlook 98 cannot find a certificate for the receiver, you will get an error message indicating that the mail could not be encrypted.



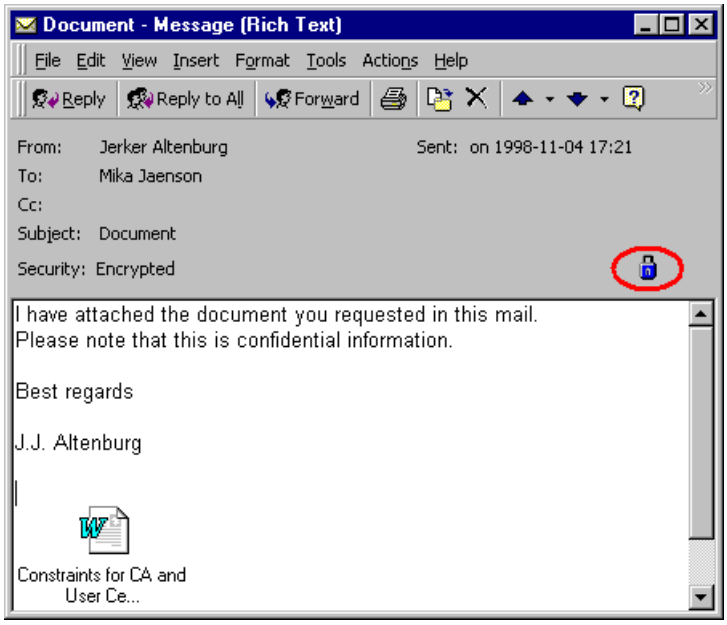
You may now choose to send the message unencrypted or cancel the operation.

Receiving Encrypted Mail

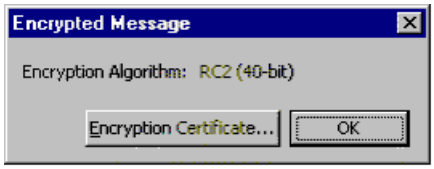
When you want to read an encrypted mail, you must enter the PIN-code for your smart card.

Note: The message has been encrypted with your public key and your private key must be accessed to decrypt it.

When the mail is opened you may inspect details of the encryption by clicking on the encryption icon to the far right in the message header.



Clicking the icon will present you with a dialog box similar to the following:



If you wish, you may view the certificate (your own…) used for encryption of the mail.

Sending Signed and Encrypted Mail

You may choose to both sign and encrypt the mail you are sending. Simply specify both options in the message **Options** dialog.

Note: You have to start in your **Contacts** folder, as specified in the section "Sending Encrypted Mail" on page 54.

You need to enter your PIN code to sign the mail, and you must also have access to the certificate of the receiver.

Microsoft Outlook Express

Using iD2 Personal CSP in Microsoft Outlook Express is very similar to the procedure in Outlook 98 and consequently, is not described here.

Configuration in Outlook Express

You may use iD2 Personal in Microsoft Outlook Express instead of Microsoft Outlook 98. The concept of CSP, and security settings, is the same in both products. The configuration procedure in Outlook Express differs from the one in Outlook 98, but it is quite straightforward and does not need to be described in detail in this document.

Microsoft Windows 2000

Logon to Windows 2000 is supported by iD2 Personal CSP but there are a number of restrictions concerning the use of smart cards for this purpose. Refer to the Microsoft documentation for details concerning this topic.

Cryptographic Module

Introduction to Cryptographic Module

iD2 Personal is a PKCS #11 v2.01 compliant product. It may be added to Netscape Communicator as a Cryptographic Module, the standard procedure for integrating third-party software with Netscape software.

Netscape can use the functions provided by iD2 Personal, among which are support for certificates and keys stored on smart cards and accessed via different smart card readers.

You may use iD2 Personal to access secure web sites in Netscape Communicator, and to send and receive encrypted and/or signed mail in Netscape Messenger.

Note: If you are using a PIN-pad device, the standard dialog boxes requesting a PIN code may look different or not appear. Instead, you will get a signal from the PIN-pad.

Netscape Communicator

You may use iD2 Personal in SSL negotiations in your Netscape Communicator browser. When a secure site (https://……) requests client authentication, you may use the certificate on your smart card to connect to the server. This section describes this procedure.

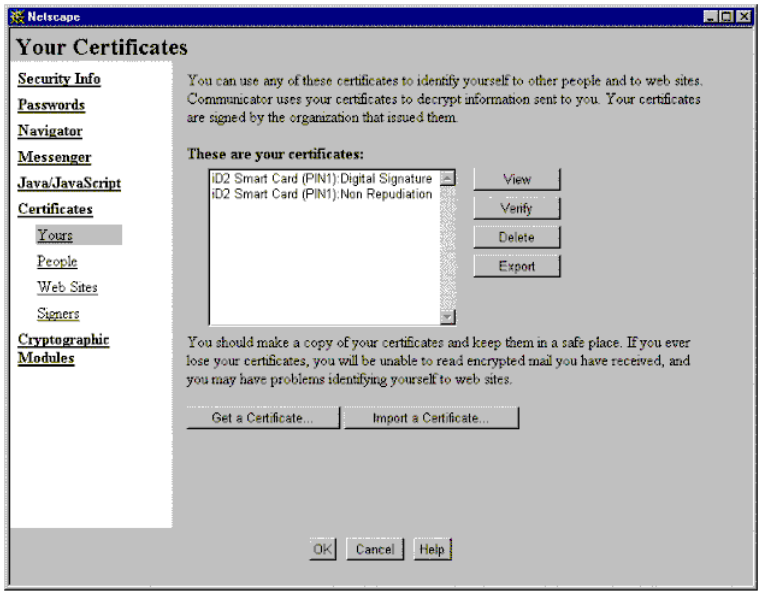
Warning: You cannot use this procedure in conjunction with Authenticator. If Authenticator has been installed, you must delete the browser Secure Proxy settings that point to Authenticator. If an external Proxy server is used, replace the Secure Proxy settings with those of the external server.

Configuration in Netscape Communicator

If a Netscape browser was selected during installation of iD2 Personal, configuration of the Netscape Communicator has already been performed. No further configuration is necessary.

Viewing Available Certificates

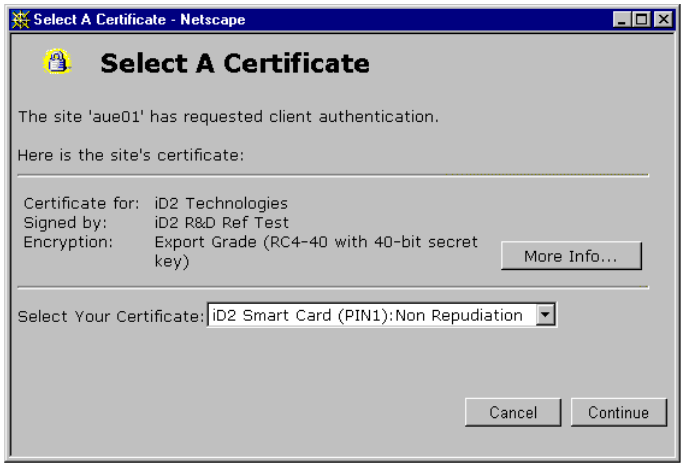
Select **Security**, and click on the **Certificates** > **Yours** option to display your available certificates.



Note: All your certificates are displayed, although only certificates of the *Non-Repudiation* type may be used when connecting to secure sites.

SSL Client Authentication

When you try to connect to a secure site (https://….) the following dialog box will be displayed.



Choose one of the available certificates.

Select a certificate of the appropriate type. The available certificates in the list box may vary between different versions of Netscape.

Note: Be sure to select a certificate of the *Non-Repudiation* type if you have Netscape version 4.05, otherwise the signing procedure will fail.

Click on **Continue**. You will then be prompted for your PIN code, and the connection will be established.

Netscape Messenger

In Netscape Messenger you can use the Cryptographic Module to send and receive signed mail and encrypted mail.

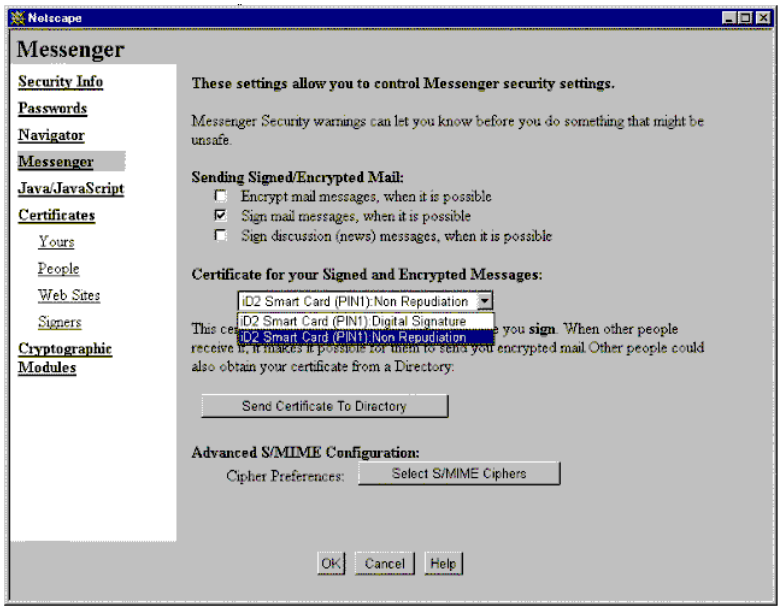
Configuration

If a Netscape browser was selected during installation of iD2 Personal, configuration of Netscape Messenger has already been performed. No further configuration is necessary.

Sending Signed Mail

Before you can send a signed mail, you must select an appropriate certificate. Select **Security** and click on the **Messenger** option in the dialog box.

Note: Ensure your smart card is inserted in your smart card reader.

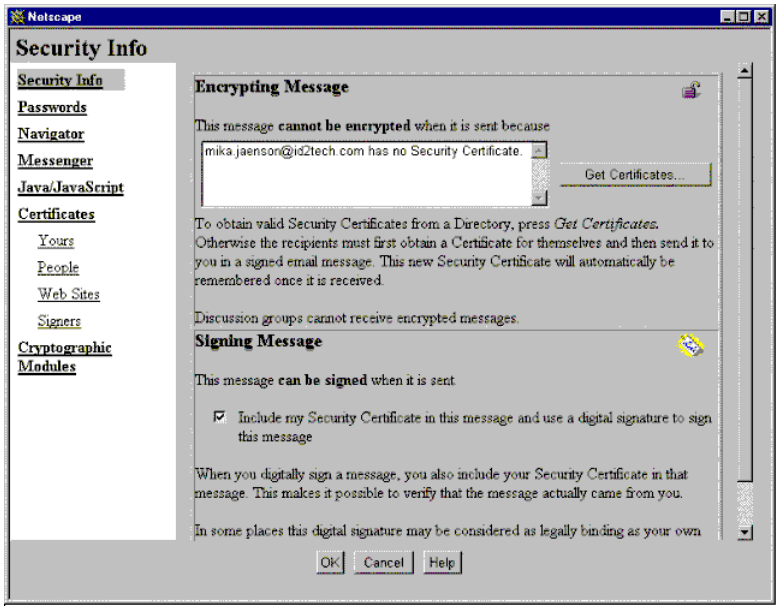


The available certificates in the list box may vary between different versions of Netscape.

Note: Be sure to select a certificate of the *Non-Repudiation* type if you have Netscape version 4.05, otherwise the signing procedure will fail.

You should now compose your message.

Select the **Security Info** option.



Specify that the mail is to be signed by selecting *Include my Security Certificate in this message and use a digital signature to sign this message*. Click **OK**.

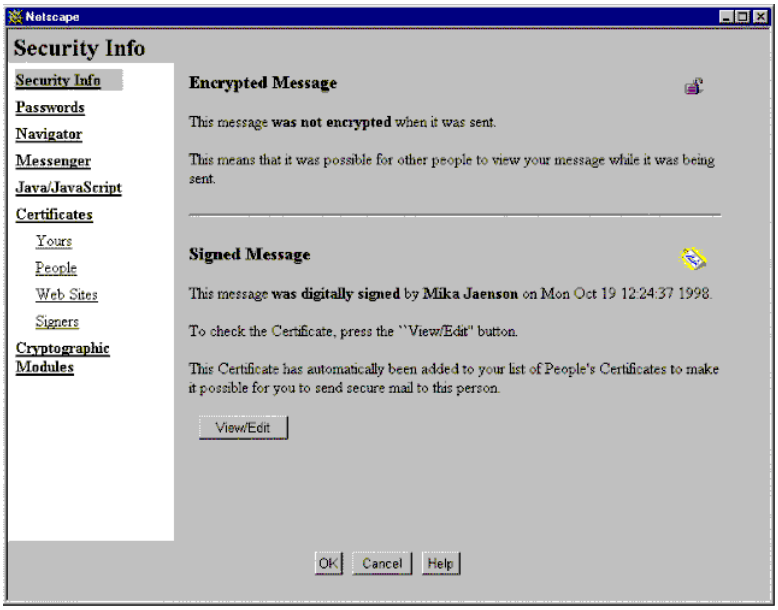
When you have finished editing your mail and click the **Send** button, the Password Entry dialog box will appear.

Enter the PIN code and click **OK**. Your signed mail is now on its way!

Receiving Signed Mail

When you receive a signed mail in Netscape Messenger, there will be a **Signed** button on the message.

Clicking the **Signed** button provides you with information about the sender of the message.



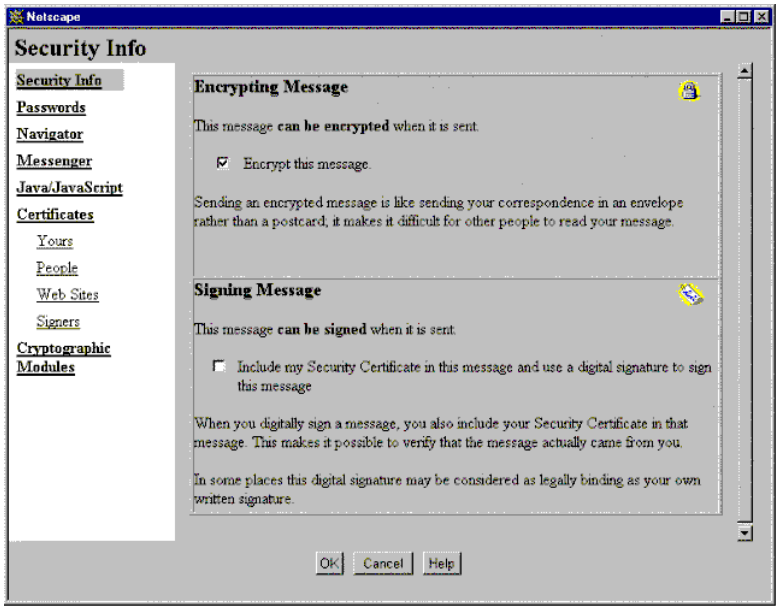
You may view the certificate of the sender using the **View/Edit** button.

The certificate will be automatically added to *People's Certificates*, and you may use it to send encrypted mail.

Note: Messenger does **not** set any trust on the CA certificate, you must add the trust yourself. Consequently, the signature will be displayed as invalid until you specify trust for the CA certificate.

Sending Encrypted Mail

Compose a new message as usual. If you have the e-mail certificate for the destination e-mail address, you may encrypt the message. If you click the **Security Info** option the following dialog box appears.



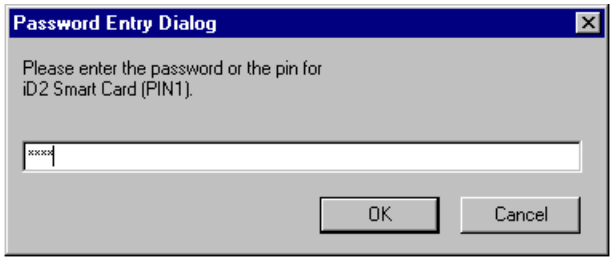
If you have the certificate of the receiver, you will be able to select *Encrypt this message*. Select this option and your mail will be encrypted before it is sent. Only you and the receiver can read the message.

You may have received the certificate of the receiver in a signed mail from that person.

If a certificate for the receiver cannot be found, the message **This message cannot be encrypted when it is sent because <recipient> has no Security Certificate** will appear.

Receiving Encrypted Mail

When you open an encrypted mail, you must have the correct token (i.e., smart card) present to be able to read the mail. You will be prompted for the PIN before the mail can be decrypted and displayed to you (the mail is encrypted with your public key and your private key is needed to decrypt it).



Clicking the **Encrypted** button on the message will display details of the encryption.

Sending Signed and Encrypted Mail

You may specify both encryption and signing when sending a mail, simply by selecting both options in the Security Info dialog box (see page 54).

When sending the mail it will be both encrypted and signed. You need to enter your PIN code to sign the mail and a prerequisite is that you have the certificate of the receiver.

WebSigner

Introducing WebSigner

Your signature is proof that you originated your business order or bank transaction. In Electronic Commerce, this has not been possible until now. WebSigner is a web browser plugin module that is used to create digital signatures in an Internet/Intranet environment. WebSigner can be used together with popular web browsers, including Netscape Navigator and Microsoft Internet Explorer. Calls to WebSigner are embedded in normal HTML pages on a standard web server. The resulting advanced security applications can be easily deployed in modern communication environments.

Digital Signatures

A digital signature is a “fingerprint” of a document or any amount of general data that locks the document to a certain private asymmetric key (e.g., an RSA key). Any changes in the document or false signatures (incorrect RSA keys) will immediately be detected when the signature is verified. The user normally holds the private key used in the calculation. In this case, digital signatures can be considered as a replacement for normal handwritten signatures. If a digital signature is to be unique to a certain person it is important that the key used is private and under the total control of that person.

Use of Digital Signatures

A digital signature can be used in all kinds of electronic environments where handwritten signatures are not possible, e.g., a signature on an order in Electronic Commerce or a signature on a transfer of funds between two banks. The simple authentication procedure, used by many systems to permit this type of action, not only provides inadequate security but also lacks the important proof that the signature is authentic. Only systems with digital signatures can generate total authentication of actions by individuals.

Smart Card Security

WebSigner uses Cryptographic Library to calculate the actual digital signature. This assures complete confidence in the origin of the signature

as Cryptographic Library normally uses smart cards to store and execute the RSA algorithm. Keys stored on private smart cards can always be considered private.

Signature Standards

A digital signature must adhere to a standard. Even though proprietary formats are possible, standardized signatures are an important factor in open systems. The standard describes how a document is coded, the algorithms that can be used, and how the algorithms are flagged in the signature. WebSigner implements the major signature standard PKCS #7 (S/MIME), a standard that is also used in secure e-mail systems. This standard allows messages signed by WebSigner to be sent to, and verified by, security-enabled mail clients.

Signature Alternatives

One of the main functions of WebSigner is to sign data on request from the server. The data may be presented to WebSigner in two alternative ways depending on MIME type:

- *'x-text-to-sign'* is used to present data as plain text, also referred to as the "Standard Profile". Another parameter in <EMBED> tag of the HTML page controls which view WebSigner should use when presenting data. See "Signature Window Normal View" on page 69 and "Signature Window Hidden View" on page 70.
- *'application/x-identrus-signing-plug-in'* is used when the data is contained in a file, also referred to as the "Identrus Profile". The user may open the file to inspect the contents before signing.

Note: The reson for using the term "Identrus Profile" is that this new feature has been developed in accordance with specifications from Identrus.

Signing Plain Text

The Standard Profile is used to sign plain text. In the browser window, WebSigner exists as a button that is used to activate the signature window.

The button is only visible when the HTML page contains the parameter *WSXView*. The appearance of the button may vary depending on the value of parameter *WSXButtonName*. A button with optional text can replace the default button shown here.

The signature window is used whenever the user is requested to sign data.

Two different versions of the signature window exist:

- Signature window normal view
- Signature window hidden view

A parameter, *WSXView*, in the HTML page, decides which view the browser will use when displaying the page.

- In normal view, the data to be signed is visible in a scrollable window.
- In hidden view, the data is not visible, but the user is still able to sign.

Signature Window Normal View

The data to be signed is shown in a scrollable text box.

Note: If you are using a PIN-pad, the dialog box will look slightly different and you must enter the PIN codes at the device.

The server sending the HTML page that invokes WebSigner is supposed to specify an action. This action indicates where the signed data will be sent.

If multiple certificates exist on the token, you must select which certificate to use before signing. The **View** button allows you to see the details of the certificate before making your selection.

Note: A flag named “keyUsage” in the certificate extension may indicate the purpose of a certificate. A certificate to be used for signing should either have the “non-repudiation” bit set and not the “digital signature” nor the “key encipherment” bits set.

Enter the PIN code corresponding to the selected certificate, to prove your identity.

Click **Save as** to save the unsigned plain text into a file.

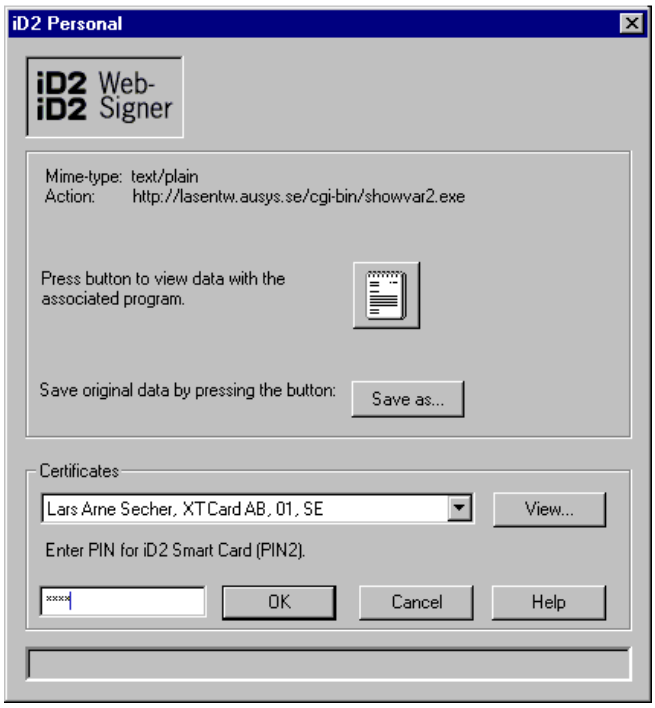
Use **OK** as the submit button when sending the signed data.

Cancel prevents the data from being sent. The **Help** button tells you how to use the controls of the window.

Signature Window Hidden View

The data to be signed is not shown, but you may click the button with the scratch pad icon to see the text in the associated Notepad application.

Note: If you are using a PIN-pad, the dialog box will look slightly different and you must enter the PIN codes at the device.



The server sending the HTML page that invokes WebSigner is supposed to specify an action. This action indicates where the signed data will be sent.

If multiple certificates exist on the token, you must select which certificate to use before signing. The **View** button allows you to see the details of the certificate before making your selection.

Note: A flag named “keyUsage” in the certificate extension may indicate the purpose of a certificate. A certificate to be used for signing should either have the “non-repudiation” bit set and not the “digital signature” nor the “key encipherment” bits set.

Enter the PIN code corresponding to the selected certificate, to prove your identity.

Click **Save as** to save the file you are going to sign.

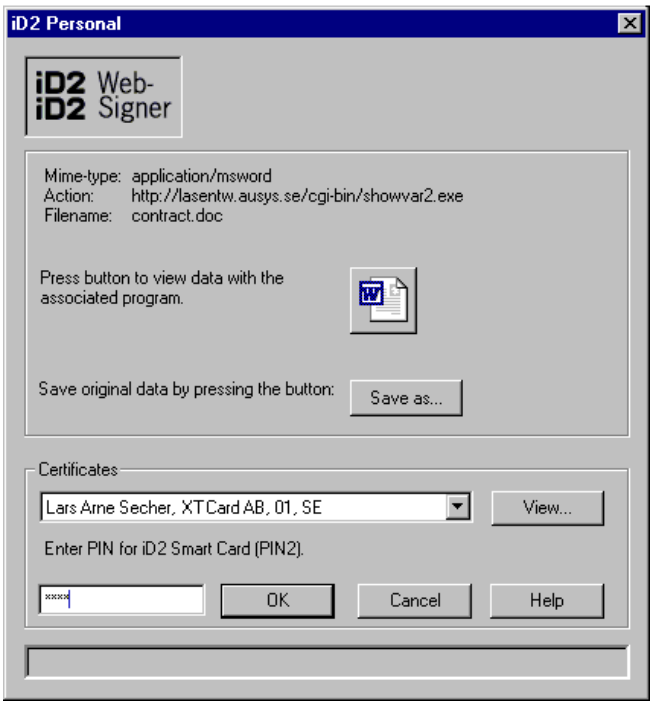
Use **OK** as the submit button when sending the signed data.

Cancel prevents the data from being sent. The **Help** button tells you how to use the controls of the window.

Signing File Contents

The Identrus Profile is used to sign file contents. No user action is required to display the following dialog box.

Note: If you are using a PIN-pad, the dialog box will look slightly different and you must enter the PIN codes at the device.



Click the button with the icon representing the associated application program if you want to inspect the contents of the data to be signed.

Click the **Save as** button if you want to save a copy of the data to be signed.

If multiple certificates exist on the token, you must select which certificate to use before signing. The **View** button allows you to see the details of the certificate before making your selection.

Note: A flag named “keyUsage” in the certificate extension may indicate the purpose of a certificate. A certificate to be used for signing should either have the “non-repudiation” bit set and not the “digital signature” nor the “key encipherment” bits set.

Enter the PIN code corresponding to the selected certificate, to prove your identity.

Use **OK** as the submit button when sending the signed data.

Cancel prevents the data from being sent. The **Help** button tells you how to use the controls of the window.

iD2 CSP Certificate Utility

iD2 CSP Certificate Utility Functions

The purpose of iD2 CSP Certificate Utility is to provide Microsoft products with certificate information from the smart card. Outlook 98, Outlook Express and Internet Explorer read the certificate information from the Windows registry.

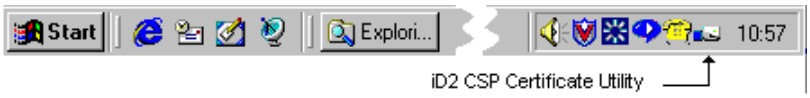
iD2 CSP Certificate Utility makes sure that the certificate information on the card is transferred to the right place in the registry. It also clears the registry when the card is removed.

iD2 CSP Certificate Utility is placed in the startup folder on your computer when installing iD2 Personal and is automatically started whenever your computer is started.

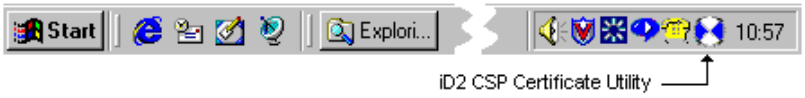
There is normally no need to stop iD2 CSP Certificate Utility, but it can be done by placing the mouse on the iD2 CSP Certificate Utility icon, clicking the right mouse button and specifying **Quit**.

iD2 CSP Certificate Utility can be started by the iD2 CSP Certificate Utility icon in the iD2 Personal program group.

You will notice the utility as a new icon in the system tray on the taskbar.



When iD2 CSP Certificate Utility is active, i.e., accessing the smart card, the icon will change its appearance.



Glossary of Terms

Alleged C4

A secret key algorithm that is compatible with the RSA Data Security's algorithm RC4, a stream cipher designed by Rivest.

API

Application Programming Interface.

CBC

In Cipher Block Chaining mode, each 64-bit plain text block is XORed with the previous cipher text block before being encrypted with the DES key. Thus the encryption of each block depends on previous blocks, and the same 64-bit plain text block can encrypt to different cipher text, depending on its context in the overall message.

Certifying Authority (CA)

A Certifying Authority (CA) can be any trusted central administration that is willing to guarantee the identity of those to whom it issues certificates, and their association with a given key.

Cryptoki

Cryptographic Token Interface.

Cryptoki interface

A cryptographic standard called PKCS #11 version 2.01 that has been specified by RSA Laboratories.

CT-API

An API for CardTerminals that specifies functions used by applications accessing smart cards via smart card devices.

DES

DES is the Data Encryption Standard, i.e., an encryption block cipher defined and endorsed by the U.S. government in 1977. DES is a symmetric cryptographic system. When used for communication, both sender and receiver must know the same secret key that is used both to encrypt and decrypt the message.

DES-EDE3

Triple-DES operations in the sequence *encrypt-decrypt-encrypt* with three different keys.

DSA

Digital Signature Algorithm is a standard for digital signature generation and verification specified in Federal Information Processing Standards Publication 186-1.

EDE

EDE stands for encrypt - decrypt - encrypt where a unique key may be used for each step, i.e., encryption with key 1, decryption with key 2 and encryption with key 3.

Handshake

An initial negotiation between client and server in order to establish the parameters for their transactions.

HTTP

Hypertext Transfer Protocol.

MD2

MD2 is a message-digest algorithm developed by Rivest. MD2 was optimized for 8-bit machines. Description and source code for the algorithm can be found as Internet RFC 1319.

MD5

MD5 is a message-digest algorithm developed by Rivest. MD5 was optimized for 32-bit machines. Description and source code for the algorithm can be found as Internet RFC 1321.

PIN-pad

A smart card reader device with a numeric keypad.

PKCS #11

Cryptographic Token Interface Standard specified by RSA Laboratories.

PKCS #12

A key format specified by RSA Laboratories.

PKCS #15

Cryptographic Token Information Format Standard specified by RSA Laboratories.

PKCS #7

Public-Key Cryptography Standard No 7. Defines a general syntax for messages including cryptographic elements, e.g., digital signatures and digital envelopes.

Private Security Environment

A proprietary virtual smart card file format of iD2 Technologies.

proxy server

A proxy server is a server that acts as an intermediary between a workstation user and the Internet to ensure security, administrative control, and caching service.

RC2

RC2 is a variable key-size block cipher designed by Rivest for RSA Data Security. It is faster than DES and is designed as a replacement for DES.

RC4

RC4 is a stream cipher designed by Rivest for RSA Data Security. It is a variable key-size stream cipher with byte-oriented operations.

root certificate store

A file containing CA certificates of all Certification Authorities that should be trusted. If a trusted CA has signed a certificate then the certificate should be accepted.

RSA

RSA is a public-key cryptographic system for both encryption and authentication; invented by Ron Rivest, Adi Shamir, and Leonard Adleman.

SHA-1

Revised version of Secure Hash Algorithm. The algorithm takes a message of less than 2^{64} bits in length and produces a 160-bit message digest.

S-HTTP

Secure Hypertext Transfer Protocol is an extension to HTTP that provides security services. S-HTTP is designed to provide confidentiality, authenticity, integrity and non-repudiation. It also supports multiple key management mechanisms and cryptographic algorithms, via option negotiation between the parties involved in each transaction.

Web pages that use S-HTTP have a URL starting with https://.

Smart card

A plastic card with a microprocessor that can store information and perform certain calculations and cryptographic functions.

Smart card token

A token based on cryptographic functions available in a smart card.

SOCKS

Socks (or "SOCKS") is a protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet.

SSL

Secure Socket Layer. A protocol designed by Netscape Corporation in order to provide authentication, confidentiality and integrity to socket-based TCP/IP services.

The SSL protocol is application independent, which allows protocols like HTTP to be layered on top of it transparently. The SSL protocol is able to negotiate encryption keys and authenticate the server before data is exchanged by the higher-level application. The SSL protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes.

Different versions of SSL exist. Version 3.0 is the preferred one. Version 2.0 does not fully support the functions required by Authenticator. If your browser only supports version 2.0 of SSL, Authenticator will allow tunneling to take place.

Token

A logical view of a cryptographic device defined in Cryptoki.

Triple-DES

See DES-EDE3.

trusted server store

A file containing server certificates that are to be trusted even if these certificates have been issued by a CA that not exist in the root certificate store

tunneling

A mode of operation during which Authenticator is transparent to all data transferred between the browser and the secure server.

Virtual smart card

A virtual smart card is a system file that replicates the same information that is held in a smart card.

Virtual smart card token

A token based on the same cryptographic functions as those available on smart cards, but simulated by software functions in iD2 Cryptographic Library stored in a file.

X.509

ITU-T Recommendation X.509 specifies the authentication service for X.500 directories and the widely adopted X.509 certificate syntax.

Index

R

S

T

U

W