# RSA SecurID Software Token 3.0
## *for Windows® Workstations*
## Administrator's Guide

**Contact Information**

See our Web sites for regional Customer Support telephone and fax numbers.


RSA Security Inc.
**www.rsasecurity.com**

RSA Security Ireland Limited
**www.rsasecurity.ie**


## Trademarks



## License agreement



## Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when exporting this product.

## Distribution

Limit distribution of this document to trusted personnel.



First printing: June 2002

# Contents

# Overview

The RSA SecurID Software Token 3.0 for Windows Workstations application is used to access a network or standalone resource protected by an RSA ACE/Server. RSA SecurID Software Token 3.0 provides a software-based security token that resides on a user's computer hard drive or smart card. With the token, authorized users can gain access to protected company resources.

To access a protected computer, the user must "authenticate" to the RSA ACE/Server. Authentication is the process by which you prove your identity to the system. To authenticate, the user needs the software token and two authentication factors:

- A secret, memorized personal identification number (PIN)
- The current 8-digit random number (called the tokencode) generated by the RSA SecurID Software Token application. The tokencode changes every 60 seconds.

The Software Token application uses these two factors to calculate a PASSCODE (a combination of the PIN and the tokencode) that it sends to the RSA ACE/Server. When the Server verifies that the PASSCODE is valid, the user is granted access to the protected resource. During these transactions, the user's PIN is never exposed. The combination of PIN and tokencode provides secure user authentication and access control.

## Product Components

The following components are included with RSA SecurID Software Token 3.0.

| | |
|---|---|
| **SecurID.exe** | Software Token application program. Provides a GUI through which users can obtain a PASSCODE to copy and paste into the login application. |
| **securid.chm** | Online help file for users. |
| **user.pdf** | *User's Guide*. |
| **iesdclnt.ocx** (OCX control for IE)<br>**npsdclnt.dll** (DLL for Netscape) | RSA ACE/Agent Browser Plug-In. Allows users to gain access to a protected Web site by entering a user ID and PIN into a form or dialog box. |
| **stauto32.dll** | RSA SecurID Software Token API (**.dll**). Required for all Software Token applications. The API also enables third-party vendors to develop an interface to Software Token. Any program that can use Windows DLLs can start the Software Token application and retrieve PASSCODEs directly. **Stauto32.dll** is automatically installed with RSA SecurID Software Token 3.0 software. |

| | |
|---|---|
| **stauto32.pdf** | *Developer's Guide*. |
| **LoginAutomation.exe** | Login Automation program. Allows users to dial in to a remote server and authenticate by typing a user ID and PIN and selecting a software token. |
| **SecurIDRas.exe** | Default login application |
| **rasall.scp** | Default script file used for Login Automation. |
| **AdminTool.exe** | Administration Tool. |
| **securid-admin.chm** | Online help for Adminstration Tool. |
| **admin.pdf** | *Administrator's Guide* (this document). |

# Administrative Tasks

As the administrator of the RSA SecurID Software Token application, you have the following responsibilities:

- Issue software token records from the RSA ACE/Server.
- Create and distribute installation packages (or install them on users' computers). If you plan to deploy the RSA ACE/Agent Browser Plug-In or Login Automation, include them with the installation package.
- Notify users of PIN length parameters and restrictions.
- For users who will authenticate with a smart card, install a supported card reader and driver on users' computers or have users install them. See **readme.txt** and **getting_started.pdf**.
- For users who will have RSA SecurID Software Token and RSA Keon Desktop installed on the same computer, the Desktop should be installed first.
- Troubleshoot user problems.
- Revoke software tokens, if necessary, from the RSA ACE/Server.

## Clock Settings

Correct clock settings are crucial to the proper functioning of the RSA SecurID Software Token application. Instruct users to make sure these settings are correct on their computers before they install the Software Token application. Remind them to check the clock settings occasionally and to adjust them if necessary.

# Installing the Application

Before you begin creating user installation packages, you should install the RSA SecurID Software Token application on your own computer. This allows you to familiarize yourself with the program.

## Types of Installations

The Windows Installer lets you select from three types of installations:

**Typical**. This selection installs the Software Token application, the Login Automation program, and the RSA ACE/Agent Browser Plug-In.

**Compact**. This selection installs only the Software Token application and associated files.

**Custom**. This selection installs all of the product components, including the Administration Tool. It also allows you to select only the specific components you want to install. Use this selection when creating user installation packages. See "Creating User Installation Packages" on page 10.

## Installation Procedure

**To install RSA SecurID Software Token 3.0:**

1. Open Windows Explorer.
2. Locate and double-click the Software Token 3.0 **setup.exe** file.
3. When prompted, select **Custom** so that all of the components will be installed.
4. Follow the installation prompts to complete the installation.

## Upgrades

You can upgrade to Software Token 3.0 by uninstalling the earlier version and then installing Software Token 3.0. With this method, you will need to distribute new software tokens to users. Since Login Automation settings will be lost, users will need to set up a new connection profile, as described in the *User's Guide*.

The installation program for Software Token 3.0 automatically upgrades from Software Token 2.5 and 2.5.1 and preserves existing software tokens, but smart card communication selections are not carried over. Users will need to redefine their smart card communication selections, as described in the *User's Guide*.

If you need to preserve existing software tokens in versions prior to 2.5, see the following table.

| Software Token Version | To Preserve Existing Software Tokens |
|---|---|
| Software Token 2.0 and 2.0.1<br>SoftID 1.2, 1.3, and 1.5 | Upgrade to Software Token 2.5.1 before installing Software Token 3.0. |
| SoftID 1.4 | Upgrade to SoftID 1.5, install Software Token 2.5.1, and then install Software Token 3.0. |

# Creating and Distributing User Packages

You can create installation packages containing the RSA SecurID Software Token application to be deployed to users. This process requires

- Associating software token records with users and then issuing software tokens as SDTID files.
- Creating and installing user installation packages on user computers.

## Issuing Software Tokens

Issuing a software token entails exporting tokens to a file that you can distribute to users. A software token file will have the extension .**sdtid**. Software tokens are issued using the RSA ACE/Server Database Administration application. See the *RSA ACE/Server Administrator's Guide* and the Database Administration application Help for more information.

## Creating User Installation Packages

This section explains how to create a custom installation package that can be installed remotely on a user's computer. This type of installation allows you to deploy the RSA SecurID Software Token application to large numbers of users without their having to run a setup program. The only action required of users is to reboot the system after the installation is complete.

To create a custom installation package, the administrator runs the installation on a machine in record mode and saves the results to a response file. The administrator then distributes the installation files along with the response file to the end user's system. When the **EndUserSetup** program is executed on the user's system, the product is installed silently with the options you selected when the response file was created. Optionally, you can distribute tokens with the package, and the tokens will be installed automatically with the application.

### Creating a Response File

1. On a machine that does not have the RSA Software Token application installed, create a new, temporary directory, and copy the installation files to it.

   The installation files include all files in the root directory of the CD (or Zip file, if the installation was downloaded from the Web).

   Do not include the **TokenAPI** or **ReaderDrivers** subdirectory unless you want the user to have access to them. Files in these directories are not used by the setup program.

2. Start a command prompt and change to the directory where you copied the installation files.

3. Enter the following command:

   ```
   Setup /r /f1"<path to setup files>\EndUser.iss"
   ```

   where <*path to setup files*> is the fully qualified path to the directory where you copied the files. For example, the command you type may look like this:

   ```
   Setup /r /f1"C:\SoftwareTokenTemp\EndUser.iss"
   ```

   **Note:** You must specify the fully qualified path. Otherwise, the file will not be created in the correct path.

4. The installation program is launched. Make the following selections:
   - On the Welcome screen, click **Next**.
   - On the Choose Destination Location screen, either select the default or browse to a valid location for the target device. Click **Next**. The default location is

     **C:\Program Files\RSA Security\RSA Security Software Token**
   - On the Setup Type screen, click **Custom > Next**.
   - On the Select Features screen, select the options that you want installed on the user's system. All options are selected by default, including the Software Token Administration Tool. Clear the Administration Tool unless you want users to have access to it. Click **Next**.
   - On the Start Copying Files screen, you can review your settings or return to the previous screen to make changes.
   - On the InstallShield Wizard Complete screen, click **No, I will restart my computer later**.

When setup is complete, the file **EndUser.iss** will be in the directory with the installation files. This file contains your responses to the setup program.

## Adding a Software Token Distribution File (Optional)

If you want to include a software token distribution file as part of the user installation package, you can do so by copying the file to the same directory as the installation files. When the setup program executes, it automatically imports the software tokens in the file. Since the installation package is run silently, the token distribution file that you add to the package should not be password protected when it is created by the RSA ACE/Server. See the *RSA ACE/Server Administrator's Guide* and the Database Administration application Help for instructions on issuing tokens.

## Reducing the Size of the User Installation Package

If you are sending the user package over the network, it is a good idea to reduce the size of the file created by the InstallShield program. The following table lists the files that you can choose to delete.

| File Name | Description |
|---|---|
| **InstMsiA.exe** | Windows Installer for Windows 98. Required only if Windows Installer is not already installed on the system. |
| **InstMsiW.exe** | Windows Installer for Windows NT and 2000. Required only if Windows Installer is not already installed on the system. |
| **RSA SecurID Software Token.pdf** | Version 2.0 Program Definition File, for use with SMS. Not needed for silent installations. |
| **SecurID_Windows_Workstations_splash.bmp** | Splash screen displayed by setup program. Not needed for silent installations. |
| **ACEAgentBrowserPlugins.cab** | Base support for RSA ACE/Agent Browser Plug-In. |
| **AdminTool.cab** | Software Token Administration Tool. |
| **DefaultHelpFiles.cab** | Help files for Software Token application. |
| **DefaultProgram.cab** | Software Token Application. |
| **ExplorerPlugin.cab** | RSA ACE/Agent Browser Plug-In for Internet Explorer. |
| **LoginAutomation.cab** | Login Automation application. |
| **NetscapePlugin.cab** | RSA ACE/Agent Browser Plug-In for Netscape. |

## Running the Installation on the User's System

After creating the user installation package, deploy it to users as follows.

1. Copy the contents of the directory where you created the response file (including the token file, if any) to a temporary directory on the user's system.
2. Execute the silent installation program, **EndUserSetup.exe.**
3. After installation is complete, delete the files in the temporary directory.
4. Notify users that you have installed the Software Token application and instruct them to reboot before starting the application.

## Alternative Distribution Methods

As an alternative to creating a user installation package that you install silently on user computers, you can have users install the RSA SecurID Software Token application themselves. Users require administrative privileges in order to install the installation package.

- Put the setup files on a network drive. Delete the **cab** files that contain the components you do not want users to have (such as the Administration Tool). See "Reducing the Size of the User Installation Package" on page 12.
- Notify users of the location of the setup files and instruct them to install the application.
- Send token files to users through e-mail and instruct users to install their tokens manually after they have installed the Software Token application.

Users require write permission to the directory into which the Software Token application is installed before they can install or transfer software tokens. As a security measure, you may decide not to grant write permission and instead install and transfer the tokens yourself.

# Administration Tool

The RSA SecurID Software Token application includes an Administration Tool, shown in the illustration, for performing the following tasks:

- Transferring software tokens to a smart card or to a token database
- Deleting tokens from a smart card or from the token database
- Selecting the method by which the application will communicate with the user's smart card

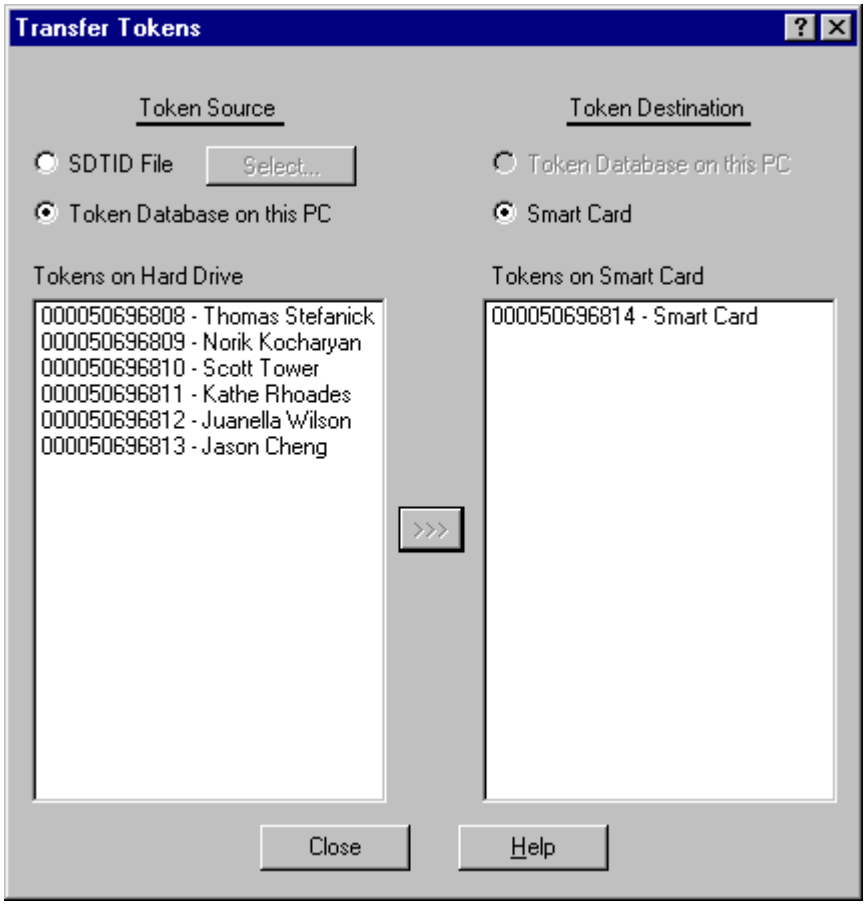
**Note:** Close the Software Token program before attempting to run the Administration Tool. You cannot run both programs at the same time.


## Using the Transfer Tokens Utility

The Transfer Tokens utility lets an administrator transfer software tokens to a user's smart card or to a database on the administrator's computer. For example, you can point to an SDTID file that contains multiple tokens and quickly populate smart cards with the tokens.

1. (For transferring tokens to a smart card) Insert the user's smart card into the card reader on the administrator's computer.
2. Start the Administration Tool.
3. If the smart card is passphrase protected, enter the passphrase.

4. On the RSA SecurID Software Token Administration menu, click **Transfer Tokens**.




5. Under Token Source, click the source of the token to be transferred. If the source is an SDTID file, click **Select** to browse for the file, and click the file to open it. If the tokens are password protected, enter the password.

6. Select the token or tokens that you want to transfer. You can use Windows key controls to select multiple tokens.

7. Under Token Destination, click the destination to which the token should be transferred.

8. Click >>>. You are prompted with the confirmation message, **Are you sure that you want to permanently transfer the selected tokens?**. Click **Yes** to complete the transfer.

9. Click **Close**.

# Using the Delete Tokens Utility

The Delete Tokens utility lets an administrator delete tokens from the user's smart card. You need to obtain the user's smart card in order to do this. You can also delete tokens from the token database on the user's computer. In that case, you run the Administration Tool while at the user's computer.

**Note:** Only an administrator can delete tokens.

Typically, tokens should be deleted in the following situations:

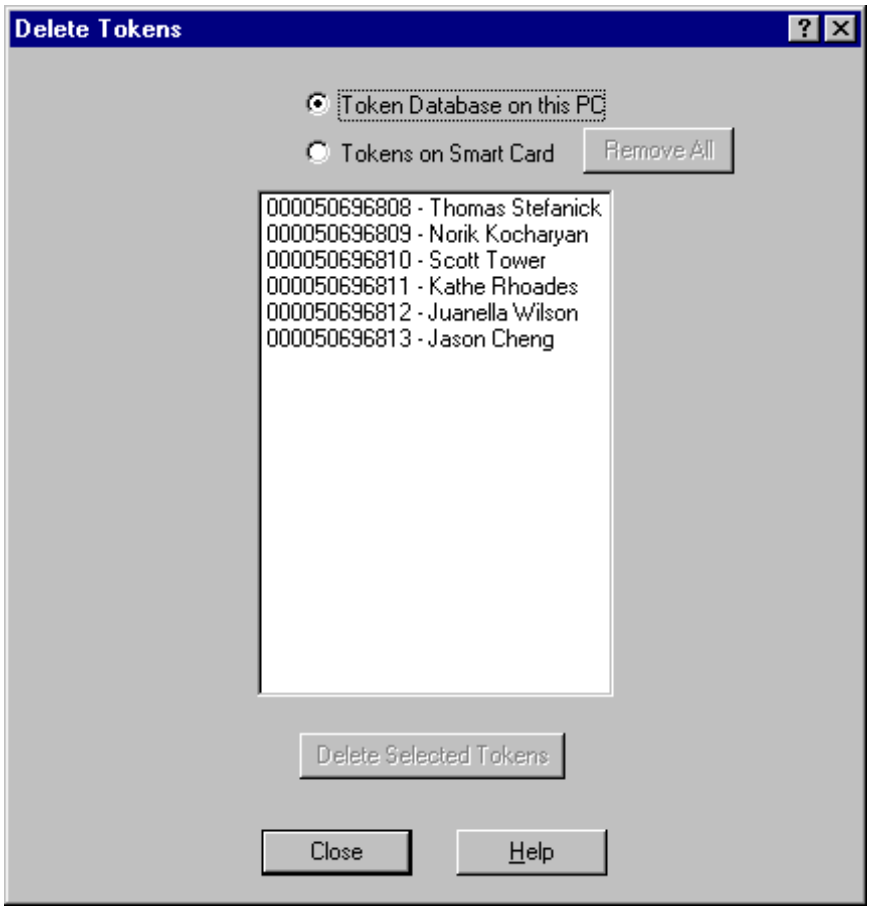
- When an unauthorized user has gained access to a token.
- When the user of a passphrase-protected token has forgotten the token passphrase.
- When a user no longer needs a token (for example, the user's responsibilities change or the user leaves the company).
- When a token expires.

## Deleting Tokens from the Hard Drive

Tokens located in the token database on the user's hard drive can be deleted selectively.

**To delete tokens from the hard drive:**

1. Start the Administration Tool from the user's computer.
2. On the RSA SecurID Software Token Administration menu, click **Delete Tokens**.



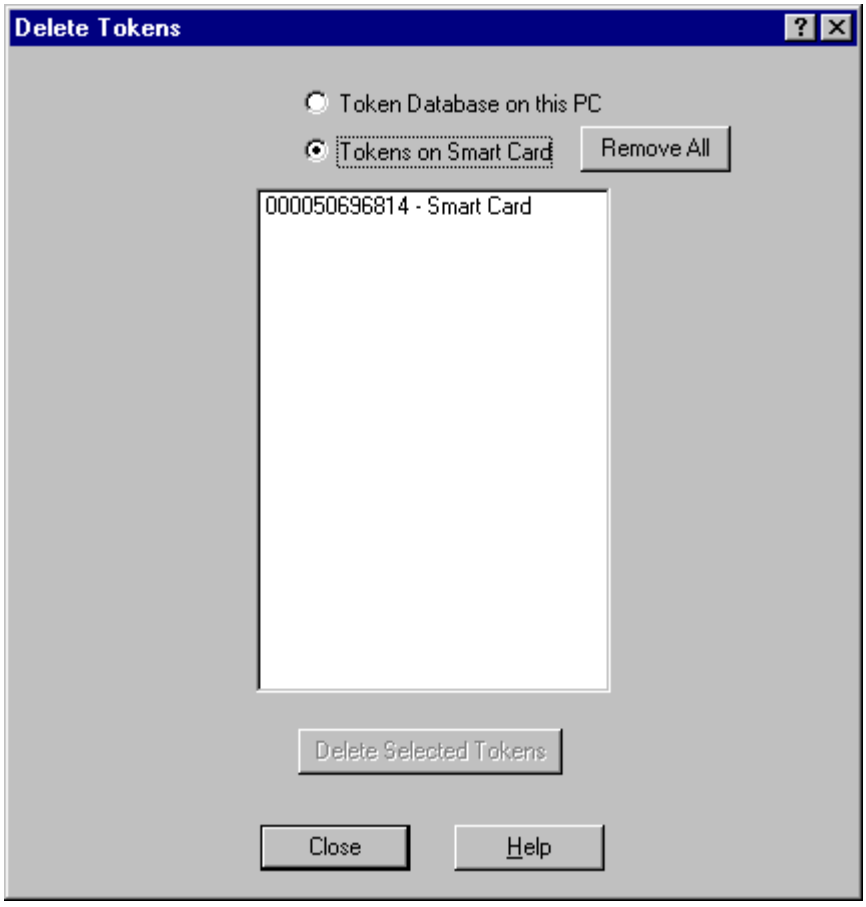

3. On the Delete Tokens screen, select **Token Database on this PC**.
4. Select the specific tokens that you want to delete or select all of the tokens, and click **Delete Selected Tokens**.

## Deleting Tokens from a Smart Card

Passphrase-protected tokens on a smart card all share the same passphrase. You can delete tokens selectively if you know the passphrase. Otherwise you must delete all of the tokens. You need to obtain the user's smart card to perform this procedure at the administrator's computer.

**To delete tokens from the smart card:**

1. Insert the smart card into the card reader on the administrator's computer.
2. Start the Administration Tool.
   If the smart card is passphrase protected, you are prompted for the smart card passphrase.
3. If you know the passphrase, enter it; otherwise, click **Cancel**.
   If you enter the passphrase, you can delete tokens selectively. If you click **Cancel**, your only option is to remove all tokens.
4. On the RSA SecurID Software Token Administration menu, click **Delete Tokens**.




5. On the Delete Tokens screen, select **Tokens on Smart Card**.
6. Click to select the tokens you want to delete, either specific tokens or all tokens. You can use Windows key controls to select multiple tokens.

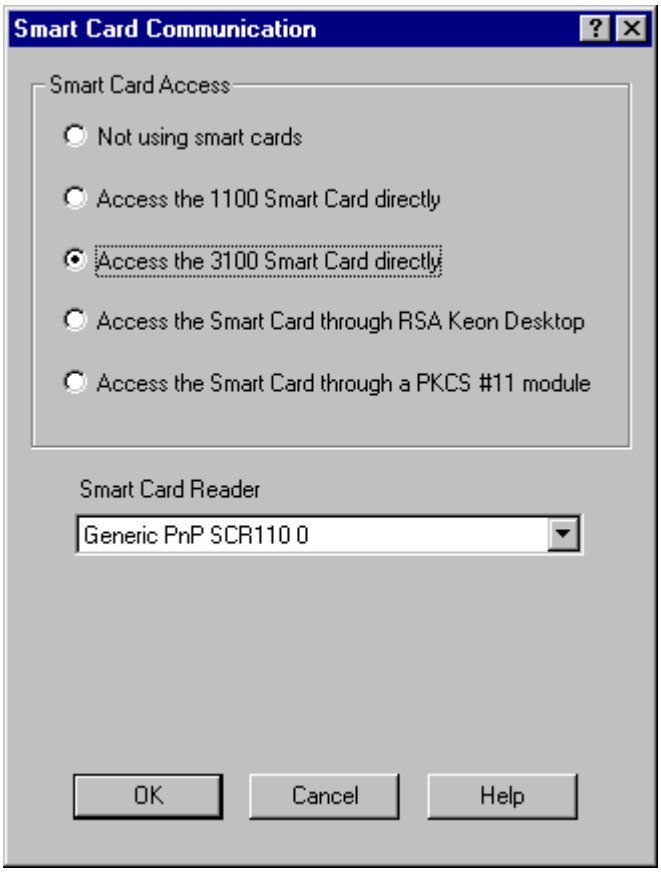
**Note:** If you clicked **Cancel**, you will not see any tokens displayed in the list, even though the smart card contains tokens. In that case, click **Remove All**.

7. Click **Delete Selected Tokens** to remove only selected tokens, or click **Remove All** to remove all tokens.
8. Click **Close**.

## Using the Smart Card Access Options

The Administration Tool lets an administrator set up smart card access for the administrator's computer. This is done from the Smart Card Communication screen, shown in the illustration.

Users can set up smart card access through the Software Token program. Occasionally, however, an administrator might need to set up smart card access for a particular user while at the user's computer. In that case, log in to the user's computer as administrator and run the Administration Tool. For more information on the smart card access options, see the *User's Guide*.




**To set up smart card communication for the administrator:**

1. Start the Administration Tool.
2. Click **Smart Card Access Options**.

3. In the Smart Card Communication dialog box, click the method by which the software will access your smart card.
4. In the Smart Card Reader box, accept the default selection if it is the reader you will use, or use the drop-down menu to make a selection. Click **OK**.

**Note:** If you will access the smart card through the RSA Keon Desktop, the Smart Card Reader selection does not appear. Be sure you are logged in to the Desktop before you attempt to use the Software Token application.

### PKCS #11 Module

If you want the application to access another vendor's smart card through a PKCS #11 module, you must install their **.dll** file on your computer.

# RSA ACE/Agent Browser Plug-In

The RSA SecurID Software Token product comes with the RSA ACE/Agent Browser Plug-in. The Plug-In can be installed as part of the user installation package.

The Browser Plug-In allows users to use a software token to access protected Web sites. To authenticate, the user tries to access the protected Web site and is prompted for a user ID and PIN. When the PIN is entered, the PASSCODE that is generated is passed to the RSA ACE/Server in the background. Users do not need to interact with the Software Token application. For more information on the Browser Plug-In, see the *User's Guide*.

**Note:** The RSA ACE/Agent Browser Plug-In has been qualified to work with Internet Explorer 5.5 and 6.0 and with Netscape Communicator 4.79. The Browser Plug-In does not work with Internet Explorer 6.0 on Windows NT.

# Login Automation

The RSA SecurID Software Token product comes with a Login Automation program that simplifies the authentication procedure for users. Login Automation can be installed as part of the user installation package.

The Login Automation program allows users to dial in to a remote server and authenticate by typing a user ID and PIN and selecting a software token. They do not need to interact with the RSA SecurID Software Token application.

To use Login Automation

- Each user must create a Windows Dial-Up Networking (DUN) phone book entry. Instructions for setting up a DUN entry are in the Help for the Windows operating system. Or, you can supply users with instructions.
- Each user must create a connection profile for the DUN entry. This is described in the *User's Guide*.
- The administrator uses the default script file, **rasall.scp**, supplied with the Software Token application, edits the default script, or creates a new script file that will be used to send authentication information from the user's computer to a remote RSA ACE/Server host. The script file is used with the default login application, **SecurIDRas.exe**. For information on login automation scripts, see the following section, "Login Automation Scripts."

## Login Automation Scripts

The Login Automation program uses scripts to send authentication information, notably the PASSCODE, from the user's computer to a remote RSA ACE/Server host.

After the login process starts, the Login Automation program performs these steps:

- Saves the original script in a backup file.
- Modifies the original script by adding the current PASSCODE.
- Uses the Windows Remote Access Service API to dial the entry specified in the Login Automation profile. (The script is passed to the API as a parameter.)
- Copies the backup script back into the original script file.

For example, the Login Automation program saves the **rasall.scp** file to **rasall.bak**, executes **rasall.scp**, and copies **rasall.bak** to **rasall.scp**. The changes made during execution are lost.

## Editing Scripts

You can edit the Login Automation program script provided by RSA Security or create your own script. The new script can be included with the Software Token user installation package. See "Creating User Installation Packages" on page 10.

Use Notepad or any text editor to edit a script or create a new script. Save completed scripts to the Software Token directory on the computer running RSA SecurID Software Token. The default path to the scripts is

**C:\Program Files\RSA Security\RSA SecurID Software Token**

Be sure to tell users the location of the customized script.

**CAUTION:** Do not edit a script while a login process is running. Your changes will be overwritten, and errors can occur if an application is trying to run the script you are editing.

### Phone Numbers

If you use a script that dials a phone number, you must edit the dialing section of the script. For example, if the script reads

```
transmit "atdt<yourhostphonenumberhere>"
```

you might edit it as follows:

```
transmit "atdt9,5551212"
```

### Keywords

Make sure the keywords remain in the appropriate places in the script. The keywords are

#$PASSCODE#$

#$PASSCODE_NO_PIN#$

#$NEXT_PASSCODE#$

#$NEW_PIN#$

#$SERIAL_NUM#$

#$USER_NAME#$

## Scripting Reference Information

The name of the scripting language is "Dial-Up Scripting Command Language." The following are pointers to information on the dial-up scripting language, including sample scripts.

- A command reference named **Script.doc** is installed with Dial-Up Networking on the following operating systems:
  - Windows NT: **\WINNT\System32\ras\Script.doc**
  - Windows 98: **\Windows\Script.doc**

**Note: Script.doc** is not included on Windows 2000 or Windows XP systems.

- Sample scripts are installed with Dial-Up Networking on all operating systems. The sample scripts have **.scp** extensions and can be found in:
  - Windows NT: **\WINNT\System32**
  - Windows 98: **\Program Files\Accessiories**
  - Windows 2000: **\WINNT\System32\ras**
  - Windows XP: **\Windows\System32\ras**