RSA SecurID Token 2.3 for the Java ME Platform Administrator's Guide

RSA®

The Security Division of EMC

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers**:** **www.rsa.com**

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 using, importing or exporting this product.

Distribution

Limit distribution of this document to trusted personnel.

April 2008

Contents

Preface 5
About This Guide 5
RSA SecurID Token for the Java ME Platform Documentation 5
Related Documentation 5
Getting Support and Service 5

Chapter 1: System Requirements and Deployment Tasks 7
About RSA SecurID Token for the Java ME Platform 7
System Requirements 7
Software Token Support 8
Ensuring Accurate Clock Settings 8
Deployment Tasks 8

Chapter 2: Deploying the Application 9
Deployment Overview 9
Installing the RSA SecurID Token Application 9
Migrating Users from the Previous Version 9
Installation Methods 10
Stopping the RSA SecurID Token Application 11
Removing the RSA SecurID Token Application 11

Chapter 3: Deploying Software Tokens 13
Issuing Tokens 13
Software Token Settings in RSA Authentication Manager 7.1 13
Software Token Settings in RSA ACE/Server 5.2 or RSA Authentication Manager 6.0 and 6.1 16
Assigning a Software Token to a Device 16
Assigning a Token Password 17
Distributing Software Tokens 17
Distributing Tokens Using Dynamic Seed Provisioning 18
Distributing Tokens Using the Numeric String 19
Setting Up Token Import Options 19
Preparing Users for Deployment 19
Instructions on Using the Application and the Token 20
Sample E-mails 20

Chapter 4: User Options 23
Importing a Token 23
Importing a Token Using the Web Download Method 23
Importing a Token Using the Numeric Input Method 24
Setting a PIN if the Device Displays a PIN Prompt 24
Setting a PIN if the Device Displays a Tokencode 25
Using the RSA SecurID Token to Access a Protected Resource 26
Changing the Token Password 26

Viewing the Token Serial Number, Device ID, and Application Information 27
Viewing GMT and Local Time.. 28
Stopping the RSA SecurID Token Application 28

Chapter 5: Troubleshooting.. 29

Appendix A: Customizing the Application 31
Including a Token with the Application 31
Specifying the URL for the Web Download Token Import Method 32
Disabling a Token Import Method.. 32
Replacing the RSA SecurID Banner Image... 33
Adding URLs to the Application Menu... 33

Preface

About This Guide

This guide describes how to prepare for and deploy RSA SecurID Token 2.3 for the Java ME Platform in an enterprise environment. It is intended for RSA Authentication Manager administrators and other personnel who are responsible for deploying and administering RSA SecurID Token applications. It assumes that these personnel have experience using RSA Authentication Manager. Do not make this guide available to the general user population.

RSA SecurID Token for the Java ME Platform Documentation

For more information about RSA SecurID Token 2.3 for the Java ME Platform, see the following documentation:

Release Notes. Provides information about what is new and changed in this release, as well as workarounds for known issues. The latest version of the *Release Notes* is available from RSA SecurCare Online: **https://knowledge.rsasecurity.com**.

Help. Contains end-user topics associated with the application screens.

Related Documentation

RSA Secured Partner Solutions directory. RSA has worked with a number of manufacturers to qualify products that work with RSA products. Qualified third-party products include Virtual Private Network (VPN) and remote access servers (RAS), routers, web servers, and many more. To access the directory, including implementation guides and other information, go to **http://www.rsasecured.com**.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsa.com/support**
RSA Secured Partner Solutions Directory	**www.rsasecured.com**

RSA SecurCare Online offers a knowledgebase that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news and software downloads.

Before You Call Customer Support

Make sure you have direct access to the device running the RSA SecurID Token application.

Please have the following information available when you call:

- ❑ Your RSA Customer/License ID
- ❑ RSA SecurID Token for the Java ME Platform software version number
- ❑ Make and model of the device
- ❑ Name and version of the device operating system

1 System Requirements and Deployment Tasks

This chapter introduces RSA SecurID Token 2.3 for the Java ME Platform and describes the system requirements and the tasks you need to complete before deploying the application and issuing software tokens.

About RSA SecurID Token for the Java ME Platform

RSA SecurID Token 2.3 for the Java ME Platform is authentication software that transforms a Java-enabled device into a network authentication device. The software consists of a Java application and an RSA SecurID software token. The software token generates eight-digit pseudorandom numbers, called tokencodes, in regular intervals. A tokencode allows resources protected by RSA SecurID to verify the identity of the user.

For example, users can use software tokens to gain access to Virtual Private Network (VPN) and web applications. The RSA SecurID Token application ensures strong security in a single handheld application and eliminates the need for the user to carry a separate hardware token.

The application supports tokens that require a unique SecurID personal identification number (PIN) as well as tokens that do not require a PIN. You set the requirement when you issue tokens in RSA Authentication Manager.

System Requirements

The RSA SecurID Token application requires the following hardware and software:

- A device that meets the following requirements:
  - Java ME and Mobile Information Device Profile (MIDP) 2.0
  - 134 KB minimum available space on the device for the Java application (Application size can vary if the application is customized.)
  - 1 KB available space on the device for the software token
- Access to a network resource protected RSA ACE/Server 5.2 or RSA Authentication Manager 6.0 and later.
- A user record with an assigned software token in the Authentication Manager database.
- A file transfer or device management utility that is compatible with the device (for example, Nokia PC Suite or Sony Ericsson PC Suite), and a computer that meets the requirements of the utility. (This requirement applies only if the application is being installed on the device using a file transfer or device management utility.)

Software Token Support

The RSA SecurID Token application supports only 128-bit (AES) tokens. This version does not support 64-bit (SID) tokens.

Ensuring Accurate Clock Settings

Local time, the time zone, and the Daylight Savings Time setting must be set correctly so that users can perform RSA SecurID authentication from their devices. Instruct users to verify the time settings on their devices before they install the application and periodically after installation to make sure that their settings are correct. If the clock settings on a user's device drift, they will no longer be synchronized with the clock settings on the Authentication Manager host, and the user will not be able to be authenticated.

Users who cross time zones with their devices need to change only the time zone in order to reflect the correct local time.

Deployment Tasks

Before deploying RSA SecurID Token for the Java ME Platform, you must complete the following tasks:

- Decide on a method for deploying the application to devices. For more information, see Chapter 2, "Deploying the Application."
- Decide whether or not to customize the application before you deploy it. For more information, see Appendix A, "Customizing the Application."
- Issue and distribute software tokens using RSA Authentication Manager. For more information, see Chapter 3, "Deploying Software Tokens."

2 Deploying the Application

This chapter describes options for deploying the RSA SecurID Token application.

Deployment Overview

RSA recommends that you install the RSA SecurID Token for the Java ME Platform application and a software token on the device and become familiar with the application. You must install the application first, and if you did not include a token with the application, you must import a software token. When you run the RSA SecurID Token application, the device becomes an RSA SecurID Token authenticator that can import a token and generate a new tokencode every 60 seconds.

Installing the RSA SecurID Token Application

The RSA SecurID Token application includes two files:

- **SecurID.jar.** This is the RSA SecurID Token application.
- **SecurID.jad.** This is a configuration file with MIDlet descriptors that you can modify to customize the application. For more information, see Appendix A, "Customizing the Application."

Note: If the application is customized, the modified JAD file must be included when the application is deployed.

Migrating Users from the Previous Version

RSA SecurID Token 2.3 for the Java ME Platform does not support an application upgrade from the previous version, RSA SecurID Token 2.2 for the Java ME Platform. Additionally, tokens from the 2.2 version cannot be transferred to the current version.

Users running the previous version require special instructions:

- **For users running the previous version with a single token:** Instruct users to remove RSA SecurID Token 2.2 for the Java ME Platform from the device using the appropriate method for removing midlets, and install the current version, RSA SecurID Token 2.3 for the Java ME Platform. As an administrator, you must reissue the token by including the token with the application (See "Including a Token with the Application" on page 31.) or distributing the token to the user so that the user can import the token (See "Distributing Software Tokens" on page 17.).
- **For users running the previous version with multiple tokens:** Instruct users not to install RSA SecurID Token 2.3 for the Java ME Platform. The current version does not support multiple tokens.

Installation Methods

The most common method of installing the RSA SecurID Token application is over the air (OTA). The user downloads the application using the browser on the device and follows the installation prompts.

The web server hosting the download can be the RSA web site or another web server. If the application needs to be customized, an administrator must download it from the RSA web site, customize it, and make it available on a web server. If the application does not require customization, users can download it from the RSA web site.

The application can also be installed using a file transfer or device management utility that is compatible with the device (for example, Nokia PC Suite or Sony Ericsson PC Suite). To install the application using a file transfer or device management utility, download the JAR and JAD files to your computer, connect the device to your computer, and use the utility to install the program. For instructions, see the documentation for the utility.

Note: RSA SecurID Token 2.3 for the Java ME Platform must be installed on a device running Java ME and Mobile Information Device Profile (MIDP) 2.0. Also, the application must be installed on the device. Do not install it on a memory card.

To install the RSA SecurID Token application:

1. Do one of the following:
   - Download the application using the browser on the device. Use the URL provided by an administrator, or go to the RSA web site: **http://rsa.com/jme/**.

     When prompted, press **Yes** to download the application, and follow the prompts to install the application on the device. If you are prompted to choose whether you want to install the application on the device or a memory card, select the device.
   - Install the application on the device using a file transfer or device management utility that is compatible with the device, for example, Nokia PC Suite or Sony Ericsson PC Suite.

     The application file is **SecurID.jar**, but if the application is customized in any way, an administrator will also provide **SecurID.jad** and instruct you to install the application using this file. For more information, see the documentation on the utility.
2. Start the RSA SecurID Token application. The License Agreement screen is displayed.
3. Read the text of the license agreement, and press **Accept**. (You must accept the license agreement before you can use the application.)
4. Do one of the following:
   - If a token is not included with the application, the Import New Token screen is displayed. You must import a token before you can use the application. See "Importing a Token" on page 23.
   - If a token is included with the application, continue to the next step.

5. If the application was installed with a password-protected token, enter the password provided by your administrator, and press **OK**.
6. Do one of the following:
    - If the token requires a PIN and the device displays a PIN prompt, you must create a PIN. See "Setting a PIN if the Device Displays a PIN Prompt" on page 24.
    - If the token requires a PIN and the device displays a tokencode, you must create a PIN. See "Setting a PIN if the Device Displays a Tokencode" on page 25.
    - If the token does not require a PIN, a tokencode is displayed immediately and you can begin using the token. See "Using the RSA SecurID Token to Access a Protected Resource" on page 26.

Stopping the RSA SecurID Token Application

To stop the application:

Select **Menu** > **Exit**.

Removing the RSA SecurID Token Application

To remove the RSA SecurID Token application, stop the application and then use the proper method for removing MIDP applications from the device. For more information, see the documentation for the device.

3 Deploying Software Tokens

This chapter describes recommendations and guidelines for issuing software tokens using RSA Authentication Manager. The chapter also describes token deployment options.

Issuing Tokens

You can issue software tokens in RSA ACE/Server 5.2, or RSA Authentication Manager 6.0 and later.

- To issue tokens in RSA Authentication Manager 7.0 and later, use the RSA Security Console. For more information, see the *RSA Authentication Manager Administrator's Guide* and the RSA Security Console Help for your version.
- To issue tokens in RSA ACE/Server 5.2 or RSA Authentication Manager 6.0 and later, use the Database Administration application. For more information, see the *RSA Authentication Manager Administrator's Guide* and the Database Administration application Help for your version.

Also, you can issue software tokens through the RSA SecurID Authentication Engine API. To use the API, see the *RSA SecurID Authentication Engine Developer's Guide*.

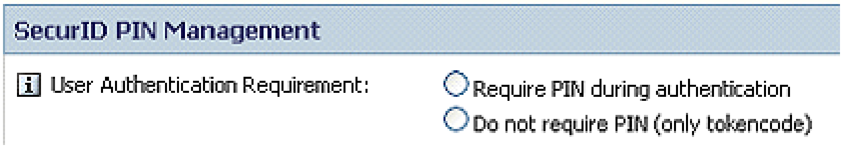
Important: RSA SecurID Token 2.3 for the Java ME Platform supports only 128-bit tokens (AES algorithm). You cannot use 64-bit tokens (SID algorithm).

The following sections describe the basic token attributes you can configure, depending on your version of Authentication Manager. You can also configure optional token attributes in any supported version of Authentication Manager, as described in "Assigning a Software Token to a Device" on page 16.

Software Token Settings in RSA Authentication Manager 7.1

If you deploy RSA SecurID Token with RSA Authentication Manager 7.1, use the RSA Security Console to issue tokens.

When provisioning a software token, you must specify whether the user must enter a PIN during authentication. You select this option in the **User Authentication Requirement** section of the Edit screen:



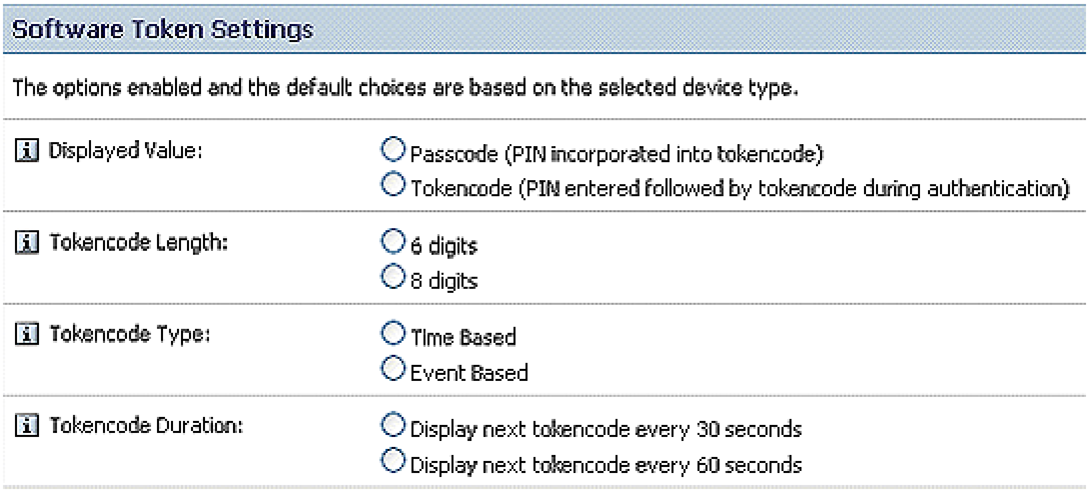
SecurID PIN Management

User Authentication Requirement: ○ Require PIN during authentication ○ Do not require PIN (only tokencode)

If you select **Require PIN during authentication**, a user must enter a PIN and a tokencode to be authenticated to a resource protected by RSA SecurID. If you select **Do not require PIN (only tokencode)**, the user enters only a tokencode. Select this option if you plan to distribute tokens that do not require a PIN.

When preparing to distribute a token file, you can select options in the Distribute Software Token screen that further control the behavior of the token. You select these options in the **Software Token Settings** section, as shown in the following figure.

Note: Some options in this screen are not supported. See the following sections for detailed information on supported options.



Software Token Settings

The options enabled and the default choices are based on the selected device type.

Displayed Value:
○ Passcode (PIN incorporated into tokencode)
○ Tokencode (PIN entered followed by tokencode during authentication)

Tokencode Length:
○ 6 digits
○ 8 digits

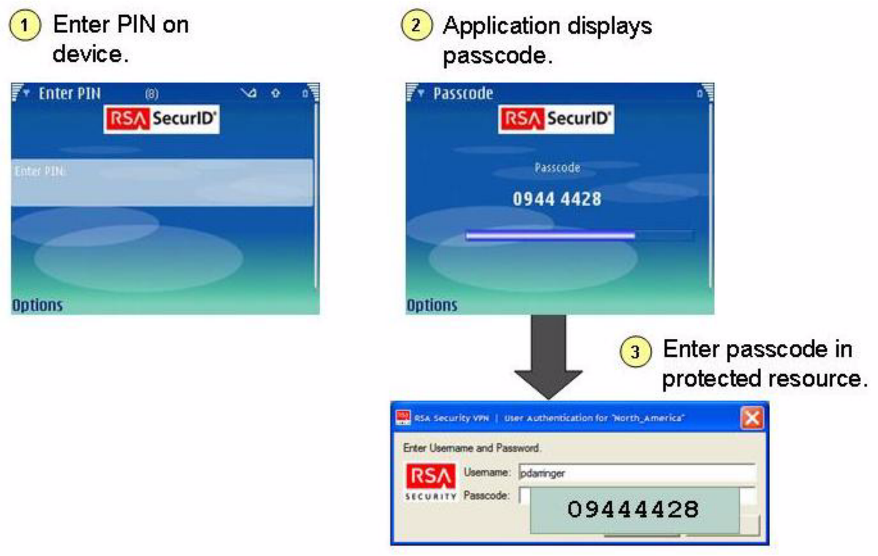
Tokencode Type:
○ Time Based
○ Event Based

Tokencode Duration:
○ Display next tokencode every 30 seconds
○ Display next tokencode every 60 seconds

Displayed Value

The Displayed Value options allow you to specify the value that will be displayed in the RSA SecurID Token application if you issue a token that requires a PIN. The options are Passcode (PIN incorporated into tokencode) or Tokencode (PIN entered followed by tokencode during authentication). If you issue tokens that do not require a PIN, Displayed Value options are not present.

If you select **Passcode**, the user's authentication experience is like that of a user with a hardware token that contains a numeric keypad for entering a PIN. The following figure describes the user experience.



1 Enter PIN on device.

2 Application displays passcode.

3 Enter passcode in protected resource.

0944 4428

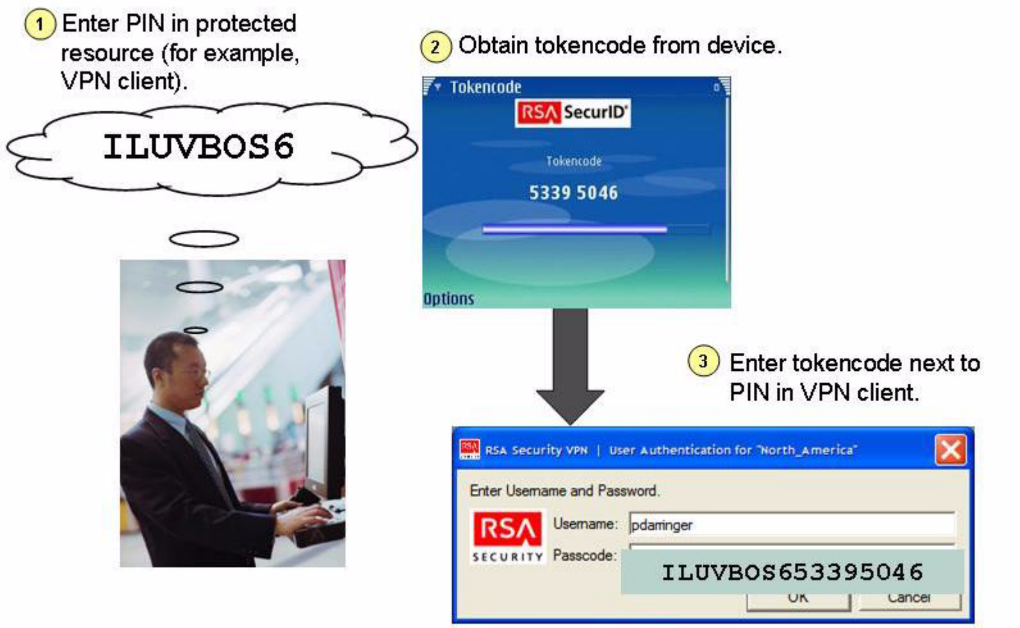
RSA Security VPN | User Authentication for "North_America"

Enter Username and Password.

Username: pdarringer

Passcode: 09444428

If you select **Tokencode**, the user's authentication experience is like that of a user with a hardware token that displays a tokencode (for example, a SID600 or SID700 token). The following figure describes the user experience.



1 Enter PIN in protected resource (for example, VPN client).

ILUVBOS6

2 Obtain tokencode from device.

3 Enter tokencode next to PIN in VPN client.

5339 5046

RSA Security VPN | User Authentication for "North_America"

Enter Username and Password.

Username: pdarringer

Passcode: ILUVBOS653395046

Tokencode Length

The RSA SecurID Token application requires 8 digits for the tokencode length. The 6 digit option is not supported.

For more information, see the *RSA Authentication Manager 7.1 Administrator's Guide* and the RSA Security Console Help.

Tokencode Type

The RSA SecurID Token application requires time-based tokens. With time-based tokens, the tokencode changes in regular intervals. The event-based option is not supported.

For more information, see the *RSA Authentication Manager 7.1 Administrator's Guide* and the RSA Security Console Help.

Tokencode Duration

The RSA SecurID Token application requires a tokencode that changes every 60 seconds. The 30-second option is not supported.

For more information, see the *RSA Authentication Manager 7.1 Administrator's Guide* and the RSA Security Console Help.

Software Token Device Type

The RSA SecurID Token application requires the tokencode type **J2ME 2.3**.

For more information, see the *RSA Authentication Manager 7.1 Administrator's Guide* and the RSA Security Console Help.

Software Token Settings in RSA ACE/Server 5.2 or RSA Authentication Manager 6.0 and 6.1

With versions 5.2, 6.0, and 6.1, the user authentication requirement is either Passcode or Tokencode only.

- Select **Passcode** if you plan to issue tokens that require entering a PIN. The user must enter the PIN in the RSA SecurID Token application.
- Select **Tokencode only** if you plan to issue tokens that do not require a PIN.

For more information, see the *Administrator's Guide* and the Database Administration application Help.

Assigning a Software Token to a Device

To ensure that a software token is used only on its intended device, you can assign the token to the device using the Device ID number.

Note: The Device ID number is the same as the International Mobile Equipment Identity (IMEI) number.

During this procedure, you will ask the user to locate the Device ID number and send it to you. Ask the user to send you the Device ID number even if you have it in your records. If the user can view the Device ID number, this means that the device makes the Device ID number available to the application so that the application can confirm that the token is assigned to the correct device.

If the user cannot view the Device ID number using the application, the value is displayed as "Not available." In this case, the device cannot support a token that has been assigned to the device using the Device ID number.

To assign a token to a Device ID number:

1. Instruct the user to obtain the Device ID number, as described in "Viewing the Token Serial Number, Device ID, and Application Information" on page 27. Have the user send you the Device ID number in an e-mail.
2. Use one of the following methods to edit the token record:
   - **RSA Authentication Manager 7.0 and later.** In the RSA Security Console, select the token you want to edit, and open the **Edit** page. In the **Software Token Device Type** section, enter the Device ID number next to the **DeviceSerialNumber** attribute.
   - **RSA ACE/Server 5.2 or RSA Authentication Manager 6.0 or 6.1.** In the Database Administration application, select the token that you want to edit, and open the Edit Token Extension Data page. Enter the Device ID number as the value of the predefined DeviceSerialNumber attribute.
3. Save and distribute the token to the user.

Assigning a Token Password

If you save the token as a SDTID file, you can set a file password. The password prevents an unauthorized person from using the token.

The user must enter the token password when importing the token and when using the token to gain access to protected resources. Be sure to communicate the password to the user before delivering the token.

Distributing Software Tokens

The RSA SecurID Token application supports two methods of distributing software tokens to users:

- **Dynamic Seed Provisioning (Remote Token-Key Generation).** Use the Cryptographic Token-Key Initialization Protocol (CT-KIP). This option is available in RSA Authentication Manager 7.1.

  If you are using the RSA SecurID Authentication Engine, you can implement dynamic seed provisioning with the RSA SecurID Key Generation Toolkit 1.2. For more information, see "Distributing Tokens Using Dynamic Seed Provisioning" on page 18.

- **Numeric string.** Save the software token to a SDTID file, convert the token to a numeric string (81-digit number) using the RSA SecurID Software Token Converter 2.3, and send the numeric string to the user through secure e-mail or another electronic medium.

  The RSA SecurID Software Token Converter is a command line utility that converts a SDTID file into a numeric string. Download the utility from **http://rsa.com/node.aspx?id=2521**. For more information on using the token converter, see the *Readme* in the download package.

Distributing Tokens Using Dynamic Seed Provisioning

RSA Authentication Manager 7.1 supports software token distribution through dynamic seed provisioning (remote token-key generation). Dynamic seed provisioning uses the Cryptographic Token-Key Initialization Protocol (CT-KIP).

With dynamic seed provisioning, Authentication Manager and the device that hosts the software token simultaneously and securely generate the same seed value on a device and in Authentication Manager. This greatly reduces the security risks associated with sending token files through e-mail or placing them on electronic media.

To configure this distribution method, complete the following actions in the RSA Security Console:

- Assign tokens to users.
- Select **J2ME 2.3** as the software token device type.
- Select **Generate CT-KIP Credentials for Web Download** as the token distribution method.

When you are ready to distribute the token, you must communicate the CT-KIP Web Download URL and the token activation code to the user. To download the token, the user enters this information in the Web Download screen in the RSA SecurID Token application.

Note: To simplify the download process, you can configure the Web Download URL so that the user does not need to enter it. For more information, see "Specifying the URL for the Web Download Token Import Method" on page 32.

For more information, see the *RSA Authentication Manager 7.1 Administrator's Guide* and the RSA Security Console Help.

If you are using the RSA SecurID Authentication Engine, you can implement dynamic seed provisioning with the RSA SecurID Key Generation Toolkit 1.2. The Toolkit, a Java API, allows the token and a CT-KIP server to dynamically and securely agree on a random seed value. The RSA SecurID Key Generation Toolkit integrates directly with RSA SecurID Authentication Engine 2.3.

For more information on the RSA SecurID Key Generation Toolkit, go to **http://www.rsa.com/node.aspx?id=3161**.

For more information on RSA SecurID Authentication Engine, go to **http://www.rsa.com/node.aspx?id=3096**.

Distributing Tokens Using the Numeric String

After you convert the SDTID file into a numeric string, you can send the numeric string to the user through secure e-mail or another electronic medium.

Setting Up Token Import Options

The RSA SecurID Token application provides two methods for importing software tokens: Web Download and Numeric Input. By default, the device displays both methods on the Import New Token screen. Both options require administrator setup, as described in the following sections.

If you want to allow only one token import method, you can customize the **SecurID.jad** file. For more information, see "Disabling a Token Import Method" on page 32.

Web Download

The Web Download token import method is based on dynamic seed provisioning. For more information, see "Distributing Tokens Using Dynamic Seed Provisioning" on page 18.

Because it can be difficult for a user to enter the URL on a device keypad, RSA strongly recommends that you customize the **SecurID.jad** file to include the Web Download URL. The user then has to enter only the token activation code to complete the download. For more information, see "Specifying the URL for the Web Download Token Import Method" on page 32.

Numeric Input

If you have sent a numeric string to the user, the user selects **Numeric Input** on the Import New Token screen. The input screen contains 17 fields. The user enters the first 5 numbers into field **1 of 17**, the next 5 numbers into field **2 of 17**, and so on. When there is only 1 number left, the user enters it in the last field.

Preparing Users for Deployment

To ensure the successful deployment of the RSA SecurID Token application, you need to instruct the user on installing the application, importing a software token, and using the token to access a protected resource.

Instructions on Using the Application and the Token

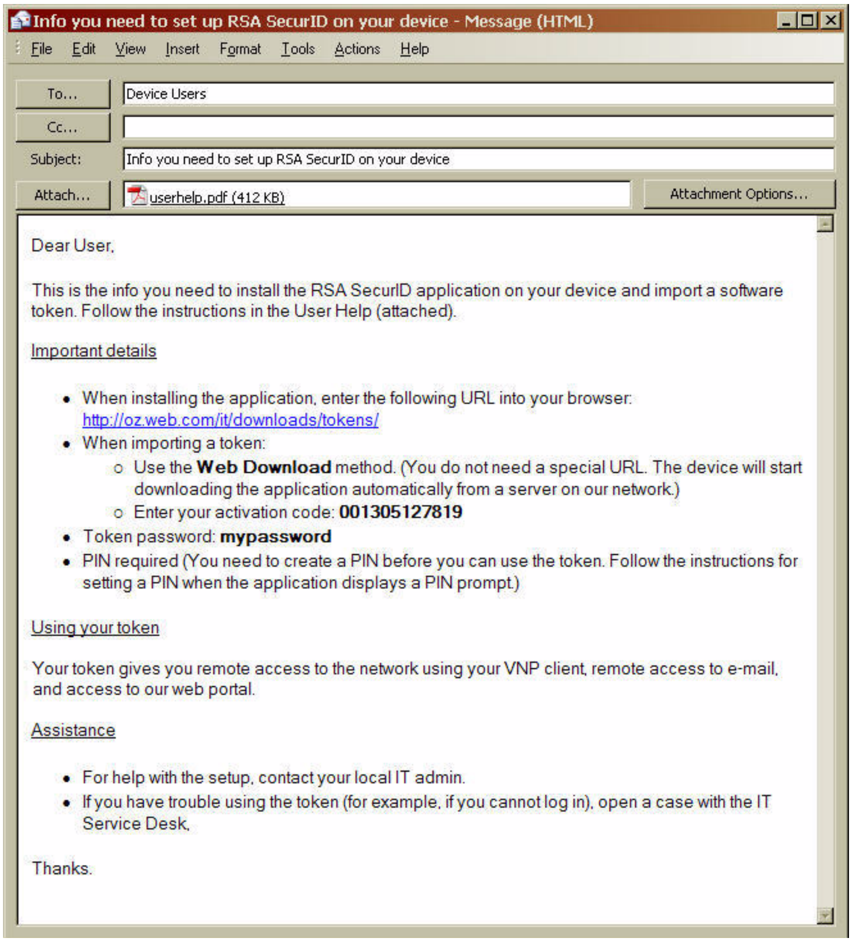
RSA recommends that you send an e-mail to the user and attach the User Help (**userhelp.pdf**).

Additionally, users need the following information:

- Token import method:
  - For Web Download, provide the URL (if the Web Download URL is not configured) and the token activation code.
  - For Numeric Input, provide the numeric string.
- Token password, if applicable.
- Instructions and the URL for setting the PIN, if applicable.
- List of applications and URLs that require RSA SecurID Token authentication.

Sample E-mails

The following e-mail is an example based on the Web Download token import method.



To...: Device Users

Cc...:

Subject: Info you need to set up RSA SecurID on your device

Attach...: userhelp.pdf (412 KB)

Dear User,

This is the info you need to install the RSA SecurID application on your device and import a software token. Follow the instructions in the User Help (attached).

Important details

- When installing the application, enter the following URL into your browser: http://oz.web.com/it/downloads/tokens/
- When importing a token:
  - Use the **Web Download** method. (You do not need a special URL. The device will start downloading the application automatically from a server on our network.)
  - Enter your activation code: **001305127819**
- Token password: **mypassword**
- PIN required (You need to create a PIN before you can use the token. Follow the instructions for setting a PIN when the application displays a PIN prompt.)

Using your token

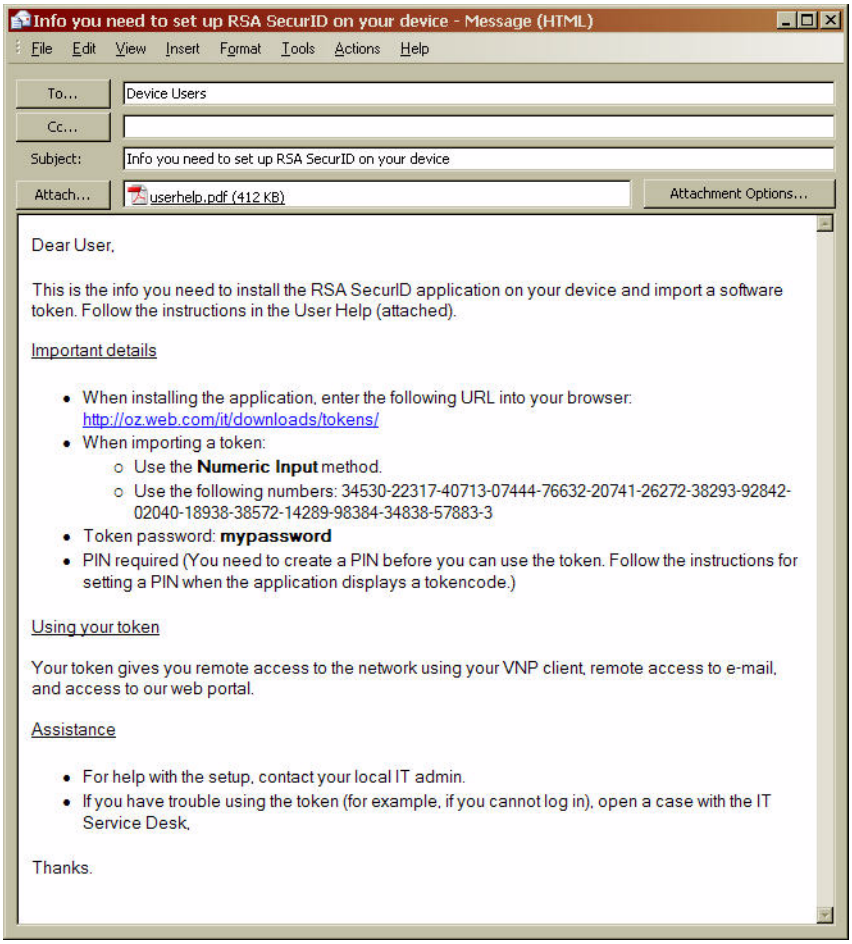
Your token gives you remote access to the network using your VNP client, remote access to e-mail, and access to our web portal.

Assistance

- For help with the setup, contact your local IT admin.
- If you have trouble using the token (for example, if you cannot log in), open a case with the IT Service Desk.

Thanks.

The following e-mail is an example based on the Numeric Input token import method.


Info you need to set up RSA SecurID on your device - Message (HTML)
File Edit View Insert Format Tools Actions Help
To...
Cc...
Attach...
Attachment Options...

To: Device Users

Subject: Info you need to set up RSA SecurID on your device

Attach: userhelp.pdf (412 KB)

Dear User,

This is the info you need to install the RSA SecurID application on your device and import a software token. Follow the instructions in the User Help (attached).

Important details

- When installing the application, enter the following URL into your browser: http://oz.web.com/it/downloads/tokens/
- When importing a token:
  - Use the **Numeric Input** method.
  - Use the following numbers: 34530-22317-40713-07444-76632-20741-26272-38293-92842-02040-18938-38572-14289-98384-34838-57883-3
- Token password: **mypassword**
- PIN required (You need to create a PIN before you can use the token. Follow the instructions for setting a PIN when the application displays a tokencode.)

Using your token

Your token gives you remote access to the network using your VNP client, remote access to e-mail, and access to our web portal.

Assistance

- For help with the setup, contact your local IT admin.
- If you have trouble using the token (for example, if you cannot log in), open a case with the IT Service Desk.

Thanks.

4 User Options

This chapter provides an overview of how users can import and manage a token using the RSA SecurID Token application. Use this chapter to familiarize yourself with the user interface.

Importing a Token

If the RSA SecurID Token application was not installed with a token, you must install a token before you can use the application.

A device running RSA SecurID Token 2.3 for the Java ME Platform supports only one token. If a token was already imported to the device, a new token overwrites it.

Use the appropriate procedure to import a token:

- To use the Web Download method, see "Importing a Token Using the Web Download Method" on page 23.
- To use the Numeric Input method, see "Importing a Token Using the Numeric Input Method" on page 24.

Importing a Token Using the Web Download Method

Before you begin, make sure that you have the token activation code. An administrator may also provide a URL if the application is not configured to download the token automatically from a specific URL.

To import a token using the Web Download method:

1. On the Import New Token screen, select **Web Download**. (If the Import New Token screen is not displayed on the device, select **Menu** > **Import New Token**, and select **Web Download**.)
2. Enter the Activation Code, and if the URL field is displayed, enter the URL provided by an administrator.
3. If prompted to use airtime, select **Yes**, and wait for the download to complete.
4. Do one of the following:
   - If the token requires a PIN and the device displays a PIN prompt, you must create a PIN. See "Setting a PIN if the Device Displays a PIN Prompt" on page 24.
   - If the token requires a PIN and the device displays a tokencode, you must create a PIN. See "Setting a PIN if the Device Displays a Tokencode" on page 25.
   - If the token does not require a PIN, a tokencode is displayed immediately and you can begin using the token. See "Using the RSA SecurID Token to Access a Protected Resource" on page 26.

Importing a Token Using the Numeric Input Method

To import a token using the Numeric Input method, you need to enter the numeric string provided by an administrator. Before you begin, make sure that you have this number available.

To import a token using the Numeric Input method:

1. On the Import New Token screen, select **Numeric Input**. (If the Import New Token screen is not displayed on the device, select **Menu** > **Import New Token**, and select **Numeric Input**.)
2. Enter the numeric string.

   Enter the first 5 numbers into field **1 of 17**, the next 5 numbers into field **2 of 17**, and so on. When there is only 1 number left, enter it in the last field.
3. Press **OK**.
4. If the token is password protected, enter the password provided by an administrator, and press **OK**.
5. Do one of the following:
   - If the token requires a PIN and the device displays a PIN prompt, you must create a PIN. See "Setting a PIN if the Device Displays a PIN Prompt" on page 24.
   - If the token requires a PIN and the device displays a tokencode, you must create a PIN. See "Setting a PIN if the Device Displays a Tokencode" on page 25.
   - If the token does not require a PIN, a tokencode is displayed immediately and you can begin using the token. See "Using the RSA SecurID Token to Access a Protected Resource" on page 26.

Setting a PIN if the Device Displays a PIN Prompt

If you are issued a token that requires a PIN, you must create a PIN the first time you use the token for authentication. The application you use to set your PIN may reside on your computer, or you may be able to access it from the device. In the following procedure, the application resides on the computer.

To set a PIN if the device displays a PIN prompt:

1. On your computer, open the protected application, for example, your VPN client.
2. Enter your user ID. You are prompted for a passcode.
3. On the device, enter your token password, if prompted.
4. On the Enter PIN screen, enter four zeros, and press **OK**. A passcode is displayed.
5. On your computer, when prompted, enter the passcode from the device in the **Passcode** field.

6. On your computer, when prompted, enter and confirm your new PIN. Your PIN must contain four to eight digits, and it cannot begin with a zero.

   You are prompted for a new passcode.

7. From the RSA SecurID Token application menu on the device, select **Menu** > **Re-enter PIN**, and enter the PIN you created. A new passcode is displayed. Enter it in the **Passcode** field on your computer.

Note: The code changes every 60 seconds. A timer counts down the time remaining before the code changes. If the code changes before you can enter it on your computer, enter the new code to complete your authentication.

Setting a PIN if the Device Displays a Tokencode

If you are issued a token that requires a PIN, you must create a PIN the first time you use the token for authentication. The application you use to set your PIN may reside on your computer, or you may be able to access it from the device. In the following procedure, the application resides on the computer.

To set a PIN if the device displays a tokencode:

1. On your computer, open the protected application, for example, your VPN client.
2. Enter your user ID. You are prompted for a passcode.
3. On the device, enter your token password, if prompted. A tokencode is displayed.
4. On your computer, when prompted, enter the tokencode from the device in the **Passcode** field. You are prompted to create a PIN. Your PIN must contain four to eight digits, and it cannot begin with a zero.
5. On your computer, when prompted, enter and confirm your new PIN. You are prompted for a new passcode.
6. In the RSA SecurID Token application on the device, wait for the tokencode to change.
7. After the tokencode changes, return to the protected application on your computer. In the **Passcode** field, enter your PIN. Enter the tokencode displayed on the device directly to the right of the PIN.

Note: The code changes every 60 seconds. A timer counts down the time remaining before the code changes. If the code changes before you can enter it on your computer, enter the new code to complete your authentication.

Using the RSA SecurID Token to Access a Protected Resource

This procedure describes how to access a protected resource using the RSA SecurID token on the device.

To access a protected resource:

1. On your computer, open the protected application, for example, your VPN client.
2. Enter your user ID. You are prompted for a passcode.
3. On the device, start the RSA SecurID Token application, and enter your token password, if required.
4. If your token requires a PIN, do one of the following:
    - If the RSA SecurID Token application displays a PIN prompt, enter your PIN, and press **OK**. The device displays a passcode. Enter the code in the application on your computer.
    - If the RSA SecurID Token application displays a tokencode instead of a PIN prompt, enter your PIN in the application on your computer, and enter the tokencode to the right of your PIN.
5. If your token does not require a PIN, enter the tokencode displayed on the device in the application on your computer.

Note: The code changes every 60 seconds. A timer counts down the time remaining before the code changes. If the code changes before you can enter it on your computer, enter the new code to complete your authentication.

Changing the Token Password

When a token is password protected, the RSA SecurID Token application prompts you to enter the password before the code is displayed. A password increases the security of your token.

If the token on the device is password protected, you can use the RSA SecurID Token application to create, change, or remove the password. (Removing the token password makes the token less secure and is not recommended.) The password can contain up to 30 characters and is case sensitive.

To change the password:

1. On the Tokencode or Passcode screen, select **Menu** > **Change Password**.
2. Do one of the following:
    - To change the existing password: Enter the current password in the **Current Password** field, and enter the new password in the **New Password** and **Confirm Password** fields.

- To create a password: Enter the new password in the **New Password** and **Confirm Password** fields.
- To remove the password: Enter the current password in the **Current Password** field, and leave the **New Password** and **Confirm Password** fields empty.

Viewing the Token Serial Number, Device ID, and Application Information

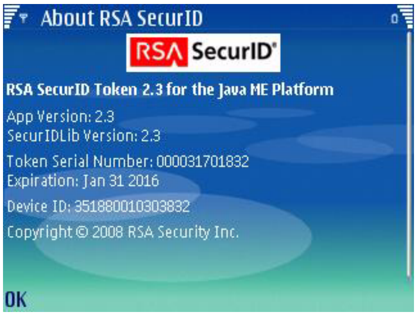
The About RSA SecurID option in the application menu launches a screen that shows the following:

- **Token Serial Number.** You may need the token serial number to activate the token, or an administrator may ask you for the token serial number to verify that you were issued the correct token.
- **Device ID.** An administrator may ask you to provide your Device ID number so that the token can be issued with a special security measure that makes the token usable only on the device.

  In some cases, the application cannot access the Device ID number. In this case, the Device ID is displayed as “Not available”.
- **Name and version of the RSA SecurID Token application and its resource library.** An administrator may ask you to verify the version of the software installed on the device.

To view the Token Serial Number, Device ID, and application information:

Select **Menu** > **About RSA SecurID**. The information is displayed.



RSA SecurID Token 2.3 for the Java ME Platform

App Version: 2.3
SecurIDLib Version: 2.3

Token Serial Number: 000031701832
Expiration: Jan 31 2016

Device ID: 351880010303832

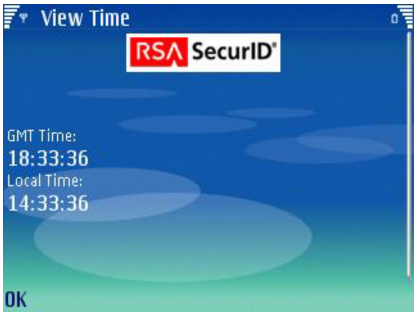
Copyright © 2008 RSA Security Inc.

Viewing GMT and Local Time

The time, date, and time zone settings on the device must be correct in relation to Coordinated Universal Time (also called Greenwich Mean Time, or GMT). Otherwise, your authentication attempts may fail. To assist in troubleshooting, an administrator may ask for the GMT setting displayed in the RSA SecurID Token application.

To view GMT and local time:

On the Tokencode or Passcode screen, select **Menu** > **View Time**. GMT and local time are displayed.



GMT Time:
18:33:36
Local Time:
14:33:36

Stopping the RSA SecurID Token Application

After using the RSA SecurID Token application to access a protected resource, you may stop the application so that you can use the device to perform other functions, such as making a call or using a different application.

To stop the application:

Select **Menu** > **Exit**.

5 Troubleshooting

This chapter describes how to troubleshoot problems a user might encounter in using RSA SecurID Token for the Java ME Platform and steps you can take to correct the problems.

Problem	Reason
The RSA SecurID Token for the Java ME Platform application installation fails.	The following conditions can cause installation to fail: • The device is not MIDP 2.0 compliant. • The operating system on the device does not support the application. (Compatible devices include Nokia and Sony Ericsson.) • The download web site is unavailable. • The device cannot download the application because it is not web enabled. • The device does not have enough available memory to install the application.
Application errors occur on the device.	The following conditions can cause application errors on the device: • The application was deployed with a token, but the token is invalid or expired, or the token configuration is invalid. • There is no token on the device, and the user cancels the token import. • There is no token on the device, and the user cannot import a token because the application configuration disables token import methods. • The device cannot run unsigned applications. • The Web Download URL specified in the JAD file is too long. If the URL is more than 200 characters, an error occurs.

Problem	Reason
The user cannot import a token, or the token import fails.	General issues that prevent a token import include: • The token is invalid or expired. (64-bit tokens are not supported.) • The token is not assigned to the device. (This issue occurs only when the token is assigned using the Device ID number.) • The token file containing the numeric input is password-protected, but the user did not enter a valid password. Web download issues that prevent a token import include: • The device is not web enabled. • No token activation code was specified, or the token activation code is invalid. • No URL was specified, or the URL is invalid or too long. The URL must start with http:// or https://, and also be less than 200 characters. • The web site hosting the download is unavailable. • A general packet failure occurred. • The server is untrusted. Numeric input issue that prevents a token import: mistyping or omitting numbers in the numeric string.
The user cannot access a protected resource or is denied access.	The following conditions can prevent a user from accessing a protected resource: • The device time and the system time on the Authentication Manager server are not synchronized. • The user entered an invalid user name or used the wrong token to access the resource. • The token requires a PIN, but the user entered an invalid PIN. (The PIN must be 4 to 8 digits.)

A Customizing the Application

You can customize the RSA SecurID Token application to reconfigure some features and to simplify the deployment of the application and software tokens.

To customize the application, edit the **SecurID.jad** file using a text editor, such as Notepad or WordPad, and deploy the customized version with the application.

The following sections explain different ways that you can customize the JAD file to do the following:

- Include a token with the application
- Specify the URL for the Web Download token import method
- Disable a token import method
- Replace the RSA SecurID banner image
- Add URLs to the application menu

Each section lists the attribute that customizes the application, the syntax for using the attribute, and an example.

Including a Token with the Application

When deploying the RSA SecurID Token application, you can include a token with the application or have the user import a token after the application is installed on the device. To include a token with the application, use the RSA SecurID Software Token Converter 2.3 to convert the token record to a numeric string. In the JAD file, set the value of X-NumericInput to be the numeric string.

Attribute	`X-NumericInput`
Syntax	`X-NumericInput: <numeric string>` Hyphens are not required.
SecurID.jad example	`X-NumericInput: 34530-22317-40713-07444-76632-20741-26272-38293-92842-02040-18938-38572-14289-98384-34838-57883-3`

Specifying the URL for the Web Download Token Import Method

If tokens are distributed using dynamic seed provisioning (CT-KIP), you can specify the Web Download URL so that users enter only the token activation code when importing a token.

Note: The URL must be less than 200 characters. When the URL is longer than 200 characters, an error occurs.

Attribute	`X-CTKIPURL`
Syntax	`X-CTKIPURL: <URL>`
SecurID.jad example	`X-CTKIPURL: https://myctkipserver.com/ctkip/services/CtkipService`

Disabling a Token Import Method

By default, both the Web Download and Numeric Input token import methods are enabled and listed in the Import New Token screen. You can disable either method so that the user cannot select an option that your environment does not support. You can disable both methods only if you distributed a token with the application. (For more information, see "Disabling a Token Import Method" on page 32.)

If you disable one method, the Import New Token screen is not displayed. Instead, the appropriate token installation screen is displayed. If you disable both methods, the Import New Token option is not displayed in the RSA SecurID Token application menu.

Attributes	Web Download method: `X-AllowWebDownload` Numeric Input method: `X-AllowNumericInput`

Syntax	`X-AllowWebDownload: <Yes or No>`
	`X-AllowNumericInput: <Yes or No>`
	Yes (default) enables the token import method, and **No** disables the token import method.

SecurID.jad example	`X-AllowWebDownload: Yes`
	`X-AllowNumericInput: No`

Replacing the RSA SecurID Banner Image

The RSA SecurID Token application displays the RSA SecurID banner on most application screens. You can replace the banner with a PNG image that is no larger than 127 pixels wide by 40 pixels high. (If your custom banner image is larger than these dimensions, test the image on all device models to which the application will be deployed.)

To replace the banner image, encode the PNG image to base64 and add the output to the JAD file using the X-BANNER_PT*n* attribute. This attribute must be enumerated to accommodate each line of code. For example, X-BANNER_PT1 represents the first line of code, X-BANNER_PT2 represents the second line of code, and so on. Include up to 1024 characters on each line.

Attributes	`X-BANNER_PTn` where `n` represents a line of code (up to 1024 characters) in a base64 conversion
Syntax	`X-BANNER_PTn: <line of code>`

SecurID.jad example	`X-BANNER_PT1: iVBORw0KGgoAAAANSUhEUgAAAH8`
	`AAAAoCAIAAABYVLILAAAAAX`
	`X-BANNER_PT2: NSR0IArs4c6QAAAARnQU1BAACxj`
	`wv8YQUAAAAgY0hSTQAAeiYAAICE`

Adding URLs to the Application Menu

The RSA SecurID Token application menu supports up to three custom URLs. For example, a custom URL can link to a page where the user can find special instructions on using the application, or where the user can set up or change a PIN.

Note: Some Java-enabled devices require an application to quit before the browser is launched. Therefore, if the application menu is configured with a custom URL and the user selects this option, the RSA SecurID Token application may close, and if the browser on the device is enabled, it loads the web page.

In the application's default configuration, there are no URLs in the application menu. However, when the application configuration file is modified to include custom URLs, the menu options for each custom URL appear automatically in the application menu.

Attribute	`X-CustomURLn` where `n` represents a URL (1-3) in the application menu `X-CustomURL_LABELn` where `n` represents the label for a URL (1-3) in the application menu

Syntax	`X-CustomURLn: <URL>`
	`X-CustomURL_LABELn: <label>`

SecurID.jad example	`X-CustomURL1: http://www.mycompany.com/`
	`IT/SecurID.html`
	`X-CustomURL_LABEL1: Help`