Authenticating with an RSA SecurID Token

Note to Administrator: Customize these instructions before handing them out to your end-users. If you are deploying the RSA SecurID Authenticator SID800, for end-user instructions see the *RSA Security Center Help* and the *RSA Authenticator Utility 1.0 User's Quick Reference,* both of which are provided with the RSA Authenticator Utility 1.0.

You have been assigned an RSA SecurID token to use when logging in.

To gain access to the protected system, you must enter a valid RSA SecurID passcode, which is made up of two factors:

- Your secret, memorized Personal Identification Number, or PIN.
- The tokencode currently displayed on the front of your RSA SecurID token. The tokencode changes at a specified time interval, typically every 60 seconds.

Before You Begin

Your administrator will tell you

- Whether you are to receive a system-generated PIN or create your own
- The required length of your PIN
- Whether your PIN is to be alpha-numeric or just numeric

Completing New PIN Mode

You are in New PIN mode because your token is not yet associated with a PIN, which is required for two-factor authentication.

To complete New PIN mode:

1. When you are prompted for your passcode, type the tokencode currently displayed on your RSA SecurID token.
2. Do one of the following:
   - Receive a system-generated PIN:

     When prompted, indicate that you want to receive a system-generated PIN. Memorize the PIN. Do not write it down.

- Create your own PIN:
  - Indicate that you want to create your own PIN.
  - When prompted, enter a PIN.
  - If prompted again, confirm the PIN.

3. Wait for the next tokencode, and then follow the instructions in "Authenticating with a Standard Card, Key Fob, or Disconnected SID800 Token" or "Authenticating with a PINPad."

Authenticating with a Standard Card, Key Fob, or Disconnected SID800 Token

To authenticate with a Standard Card, Key Fob, or disconnected SID800 Token:

When prompted for the passcode, type your PIN followed by the tokencode currently displayed on your token. For example, if your PIN is 1234, and the current tokencode is 800261, enter **1234800261**.

Note: You cannot reuse RSA SecurID tokencodes. To log in again, wait for a new tokencode to appear.

Authenticating with a PINPad

To authenticate with an RSA SecurID PINPad:

1. Enter your PIN into the PINPad, and press the diamond (♦) near the bottom of the PINPad. A new passcode appears on the token.
2. When prompted, type your passcode.
3. As soon as your passcode has been accepted, press the **P** on your PINPad to clear the PIN from your card's memory.

The Next Tokencode Prompt

On occasion, even after you type your passcode or tokencode correctly, the system prompts you to enter the next tokencode in order to confirm your possession of the token.

To authenticate in Next Tokencode mode with a Standard Card, Key Fob, or disconnected SID800 Token:

Wait until the tokencode changes, and then type the new one. Enter only the tokencode. Do not enter your PIN.

If you are not granted access after correctly entering the next tokencode, call your system administrator.

To authenticate in Next Tokencode mode with a PINPad:

1. Press the **P** on the PINPad to clear the PIN from your card's memory.
2. Wait until the tokencode changes, and then type the new one. Enter only the tokencode. Do not enter your PIN.

Security Precautions

If an unauthorized person learns your PIN or obtains your RSA SecurID token, this person can assume your identity. Any action this intruder takes is attributed to you in the system's security log.

For your own protection and for that of the system, always take the following precautions:

- Never reveal your PIN to anyone.
- If you think someone has learned your PIN or your token is missing, notify the security administrator right away.
- Follow your system's standard logoff procedures. Failure to log off properly can create an unprotected route into the system.