SafeNet Authentication Service

Welcome Guide

RB-1 Tokens

Document Information

Document Part Number	007-012425-002, Rev. B
Release Date	February 2015

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Overview

The RB-1 Key PIN Pad token generates a new, pseudo-random passcode each time the token is activated.

An RB-1 PIN is a numeric string of 3 to 8 characters that is used to guard against the unauthorized use of the token. If PIN protection is enabled, the user must provide a PIN to activate the token.

Key Pad Summary

Key	Function
0-9	Used to enter PIN.
PASSWORD	Turns the token on/off in **Password** mode.
DIGSIG	Turns the token on in **Digital Signature** mode.
MENU	Provides access to the LCD contrast control and token resynchronization mode. The PIN may be required to access the menu items.
ENT	Used to confirm or complete any keypad inputs.
CLR	Used to clear a keypad input error (e.g., PIN, challenge).
CHGPIN	Used to change the PIN used to activate the token.

Operating Modes and Options

The RB-1 supports a wide range of operating modes that can be modified using the SAS ID Manager and a serial or USB token initializer, according to organizational and security policy requirements.

The PIN length, complexity, and maximum number of incorrect consecutive PIN attempts must be configured during token initialization. If the PIN attempts threshold is exceeded, the token will not generate a passcode and will, depending on the configuration, either require re-initialization or a PIN reset before it can be used again. A brief list of the more common operating modes follows. Refer to the *SAS ID Administrator Guide* for a complete list of modes and options.

Mode

Quick Log mode is the recommended mode for all SafeNet token types because it greatly simplifies the user logon experience and strengthens security by eliminating the requirement to have the user key a challenge into a token to get an OTP. In addition, **Quick Log** mode is supported by all systems that require a logon password.

- **Quick Log:** Password is displayed immediately by the token (or after Display Name, if this option is enabled on the **Display** tab).
- **Challenge-response:** Requires the user to key a numeric challenge into the token before a response is generated.

Complexity

- **Hexadecimal:** Token generates passcodes comprised of digits and letters from 0–9 and A-F.
- **Decimal:** Token generates passcodes comprised of digits from 0-9.
- **Base32:** Token generates passcodes comprised of digits and letters from 0-9 and AZ.
- **Base64:** Token generates passcodes comprised of digits and letters from 0-9 and Aa-Zz, as well as other printable characters available via Shift + 0-9.

Length

- Determines the passcode length. Options are 5, 6, 7, or 8 characters. The default value is **8**.

Display Mask

- **Telephone Mode:** Replaces the fourth character of a passcode with a dash (-). This is generally used in combination with Response length: 8 characters and Display
- **Type:** Decimal, to resemble the North American telephone number format.
- **None:** Passcode is displayed as set by Response length and Display type.

Passwords per Power Cycle

The **Single password (passcode) per power cycle** option is recommended. For applications requiring dual authentication or where multiple consecutive logons are required, select **Multiple** mode. Note that the **Automatic shut-off** option will power the token off automatically after the specified time interval elapses.

- **Single** - Only one passcode is provided after the token is activated. The token must be powered off and re-activated to generate another passcode.
- **Multiple** -The token will generate passcodes as required until it is powered off.

Manual Shut-Off

The **No** setting is recommended when using the RB-1 token.

- **Yes** – The user can force the token off at any time.
- **No** – The user cannot force the token off. The token will automatically turn off (based on **Automatic shut-off** configuration).

Auto Shut-off

This setting determines the length of time a passcode is displayed on the token, after which the token display is cleared and the token is turned off. Available options are 30, 60, and 90 seconds. This setting is also used to prevent the token from being reactivated before expiration of the shut-off period.

PIN Policy Group

PIN styles are separated into two general groups—**Stored on Server** or **Token Activated by PIN**. The RB-1 also supports a **No PIN** option, although this is not recommended. The **Stored on Server** option requires the user to prepend the PIN to the passcode displayed on the token. The combination of the PIN and passcode form the password that is used to authenticate the user (the passcode cannot be used to authenticate unless the PIN is prepended). The PIN is not input into the token (in other words, it is not required to activate the token and generate a passcode). When operating in this mode, the PIN can consist of alphanumeric characters.

- **No PIN** - The user will not use a PIN. The token-generated password will be sufficient for authentication.
- **Fixed PIN** - The PIN created for the token at the time of initialization is permanent and cannot be modified by the user or operator. **Fixed PIN** can only be changed by re-initializing the token after selecting a new PIN value through this tab. This PIN must be entered into the token before a passcode is displayed.
- **User-selected PIN** - The user may change the PIN at any time. The initial PIN set during initialization must be changed by the user on first use of the token. This PIN must be entered into the token before a passcode is displayed. The PIN value selected by the user must be within the limits set under the **Min PIN Length**, **Characters allowed**, **Try Attempts**, and **Allow Trivial PINs** options.
- **Server-side Fixed** - This PIN must be prepended to the passcode. An Operator can change the PIN. This mode emulates **SecurID PIN** mode.
- **Server-side User Select** - Periodic PIN change is forced by the server according to the **PIN Change Period** option. The user will determine the new PIN value within the limits set under the **Min PIN Length**, **Characters allowed**, **Try Attempts**, and **Allow Trivial PINs** options. This PIN must be prepended to the passcode. This mode emulates the **SecurID PIN** mode.

- **Server-side Server Select** - Periodic PIN change is forced by the server according to the **PIN Change Period** option. The server will determine the new PIN value within the limits set under the **Min PIN Length**, **Characters allowed**, **Try Attempts**, and **Allow Trivial PINs** options. This PIN must be prepended to the passcode. This mode emulates the **SecurID PIN** mode. Initial PIN modifications for a **Stored on Server** PIN only become active when **Reset Server-side PIN** is selected.
- **Token Activated by PIN** – This option requires the user to key the PIN into the token before a passcode is generated. In this mode, only the passcode displayed by the token is sent to the authentication server; the PIN is not transmitted across the network. When operating in this mode, the PIN can only consist of numeric characters.

Initial PIN

The initial PIN value required for the token. The value is permanent if **Fixed PIN** is selected as the PIN style. This value must be changed on first use of the token for **User-selected PIN**. Use the **Randomize** button to change the initial value to a random number within the limits set under the **Random PIN Length**, **Min PIN Length**, and **Characters allowed** options.

Random PIN Length

The minimum PIN length generated when clicking the **Randomize** button. The valid range is 3–8 characters.

Minimum PIN Length

The minimum PIN length required to authenticate. The valid range is 1-8 characters.

Allow Trivial PINs

- **No** - Prevents the use of sequences or consecutive digits/characters longer than 2. For example, **124** or **ABD** are permitted; **123** or **ABC** are not permitted.
- **Yes** - No sequence checking. For example, **123** is permitted.

Max PIN Attempts

- Number of consecutive incorrect PIN attempts permitted. The valid range is **1–7** and **Unlimited** attempts. The **Unlimited** option is available in cases where the PIN is entered into the token.

If this value is exceeded for **Stored on Server** PINs, authentication will not be permitted until the operator has reset the PIN value. If this value is exceeded for **Token Activated by PIN** options, the token will be locked and will not generate passcodes until it is physically reinitialized.

Token Usage Options

Using the RB-1, PIN Stored on Server

In this mode (assuming **Quick Log** mode is being used), the token requires no input data to generate a new, one-time passcode, but the user must prepend his PIN to the passcode displayed by the token in order to generate an acceptable password.

Generating a Passcode

1. Press the **PASSWORD** button to activate the token. A one-time passcode is automatically generated.
2. Enter the PIN (for example, **ABCD**) and passcode (for example, **12345678**) at the password prompt (ABCD12345678).

Changing a PIN

If enabled, this feature permits the PIN to be changed according to the established security policy. The SAS ID Server will enforce a PIN change at regular intervals. Depending on the options selected, the user will be prompted to enter a new PIN or will be provided with a new PIN generated by the SAS ID Server. In both cases, the PIN will meet the minimum PIN policy requirements (complexity, length, non-trivial, etc.) as configured on the server. A SAS ID Server Operator may also force a PIN change for individual users, as required.

When a PIN change is required, the user will be prompted through the process. Once complete, the user must re-authenticate to gain access to protected resources.

Using RB-1 Token Activated by PIN Mode

In this mode, the user must key a PIN into the token before a passcode is generated. The displayed passcode is then used during logon. Note that the PIN is not prepended to the passcode and is never sent across the network. The numeric keypad is used to enter the PIN.

First Use

On first use, the user must key a PIN provided by the System Administrator into the token, whereupon the token will immediately require the PIN to be changed to a new value known only to the user, within the PIN parameters selected during initialization. Thereafter, the token will generate a passcode after the PIN has been correctly entered.

1. Press the **PASSWORD** button. The token will display the **PIN?** prompt.
2. Use the numeric keypad to enter the PIN. If an incorrect digit is accidentally entered, press **CLR** to erase all digits and restart the process. Press **ENT** once all PIN digits have been entered.
3. The token will display the **New PIN?** prompt. Enter a new PIN value using the numeric keypad. Press **ENT** to complete input.
4. The token will display the **Verify** prompt. Re-enter the new PIN value and press **ENT** to complete input.
5. The token will display the **Card OK** confirmation. Press **PASSWORD** to turn the token off.

Generating a Passcode

1. Press the **PASSWORD** button. The token will display the **PIN?** prompt.
2. Use the numeric keypad to enter the **PIN**. If an incorrect digit is accidentally entered, press **CLR** to erase all digits and restart the process. Press **ENT** once all PIN digits have been entered.
3. **In Quick Log mode:** The token displays the one-time passcode.
4. **In Challenge-response mode:** Enter the 8 digits of the challenge using the numeric keypad. Press **ENT** to complete the input. The token displays the one-time passcode.

The token display will clear and the token will automatically shut-off at the preset **Automatic shut-off** interval of 30, 60, or 90 seconds. The token can be manually turned off by pressing **PASSWORD**, if enabled.

User-changeable PIN

If configured, the RB-1 permits the user to change the PIN required to activate the token. When the user keys in the initial PIN (sometimes referred to as the deployment PIN), they will be prompted to immediately change the PIN to a new value, within the parameters of the security policy established during initialization. Thereafter, the user can change their PIN as often as desired:

1. Press **CHGPIN** and enter the current PIN at the **PIN?** prompt.
2. At the **NEWPIN?** prompt, enter the digits of the new PIN and press **ENT**.
3. At the **VERIFY** prompt, re-enter the new PIN and press **ENT** to confirm.
4. The token displays a **CARD OK** message to indicate that the new PIN has been accepted.

Generating Digital Signatures

RB-1 tokens are able to generate digital signatures.

1. Press **DIGSIG** and enter your PIN, if required. Press **ENT** to complete the PIN entry process.
2. At the **Ready** prompt, enter the input data (for example, the 8-digit form hash/challenge) generated by the document to be signed. Press **ENT** to complete input. The digital signature is displayed for entry into the application/document.
3. Press **ENT** and repeat step 2 if multiple signatures are required.
4. Press **PASSWORD** to end digital signature mode.

Token Resynchronization

Token resynchronization may be required if the user has generated a large number of passcodes without logging on (authenticating). Token resynchronization requires the user to enter a “challenge” into the token. The challenge must be provided by the Help Desk or via a web-based resynchronization page. In the unlikely event that the token requires resynchronization with the authentication server:

1. Press **MENU** and enter your PIN, if required. The **Contrast** prompt will be displayed.
2. Press **MENU** again to display the **ReSync** option.
3. Press **ENT** to selection this option. Enter the resynchronization challenge using the numeric keypad. Press **ENT** to complete the input.

LCD Contrast Adjustment

The LCD display contrast can be adjusted to lighten or darken the displayed passcode and prompts. To adjust the contrast:

1. Press **MENU** and enter your PIN, if required. The **Contrast** prompt will be displayed.
2. Press **ENT**. The token will display the current LCD contrast level (for example, -xx07xx-).
3. Press **MENU** repeatedly to lighten the display (-xx00xx- is the lightest value). Press **DIGSIG** repeatedly to darken the display (-xx15xx- is the darkest value).
4. Press **PASSWORD** to accept the contrast selection.

Token Initialization

The RB-1 can be reprogrammed as often as required to enable new options, encryption modes, and keys. SAS ID Manager and a USB token initializer are required.

To initialize a token:

1. Place the RB-1 token in the initializer with the LCD display facing the front of the initializer. The LCD end of the token should be toward the bottom of the initializer.
2. Follow the SAS ID Manager directions for token initialization.
3. Click **Next** to initialize. The token will display the **CARD OK** message on successful initialization. .

Battery Replacement

SafeNet tokens operate for approximately 5-6 years before battery replacement is required. Depending on the model, the token display will indicate a low battery condition about two months before failing (by displaying **BATTERY!**) or will grow noticeably dim.

Each RB-1 token holds two coin-cell batteries. Replacement of one battery at a time permits the token to continue functioning. As long as only one battery at a time is removed and replaced, the token will not need to be returned to the Administrator for reprogramming.

To replace the token batteries:

1. Remove the battery compartment cover.
2. Remove one battery and replace it with a new battery (CR2016).
3. Remove the other battery and replace it.
4. Put the battery compartment cover back in place.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	