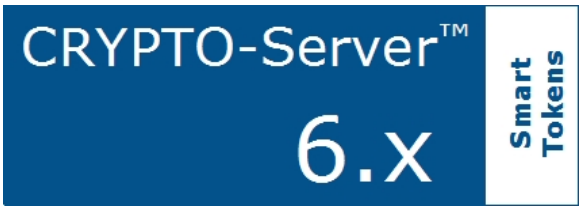

RB-1 PIN Pad Token

QUICK Reference

Table of Contents

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 token on/off in Password mode.
DIGSIG	Turns 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 & Options

The RB-1 supports a wide range of operating modes that can be modified using the CRYPTO-Console GUI 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 reinitialization or a PIN reset before it can be used again. A brief list of the more common operating modes follows. Refer to the CRYPTO-Server Administrator Guide for a complete list of modes and options.

`Display Type`:

- `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 A-Z.
- `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.

`Telephone mode`:

- `Yes`: 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.
- `No`: passcode is displayed as set by Response length and Display type.

`Response Length`:

- Determines the passcode length. Options are 5, 6, 7, or 8 characters.

`Automatic shut-off`:

- Determines the length of time a passcode is displayed on the token, after which the token display is cleared and the token turned off. Options are 30, 60, and 90 seconds. Also used to prevent the token from being reactivated before expiration of the shut-off period.

`Display Name:`

- The value entered (typically the UserID) is displayed by the token before the passcode is displayed. Maximum length is 8 characters.

`PIN Style:`

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.

Stored on Server 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 (i.e. it is not required to activate the token and generate a passcode).

- `Stored on server, Fixed PIN`: this PIN must be prepended to the passcode. An Operator can change the PIN. This mode emulates SecurID PIN mode.

- `Stored on server, User-changeable PIN`: 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`, `Try Attempts`, and `Allow Trivial PINs` options. This PIN must be prepended to the passcode. This mode emulates the SecurID PIN mode. If a token in this mode becomes locked by exceeding the `Try Attempts` value and is re-enabled, the user must authenticate at least once before the token `Try Attempts` is reset to its default value.

- `Stored on server, Server-changeable PIN`: 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`, `Try Attempts`, and `Allow Trivial PINs` options. This PIN must be prepended to the passcode. This mode emulates the SecurID PIN mode. This mode is currently not supported when performing MSCHAPv2 authentication requests. If a token in this mode becomes locked by exceeding the `Try Attempts` value and is re-enabled, the user must authenticate at least once before the token `Try Attempts` is reset to its default value.

Initial PIN modifications for a `Stored on Server PIN` only become active when `Reset Server-side PIN` is selected.

Token Activated by PIN 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.

- `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-changeable 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`, `Try Attempts`, and `Allow Trivial PINs` options.

`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-changeable PIN`. Use the `Randomize` button to change the initial value to a random number within the limits set under the `Random PIN Length` and `Min PIN Length` options.

Use this feature as a "Deployment PIN" with CRYPTO-Deploy to ensure that only valid users are registering their token. Note that the minimum initial PIN length can be longer than the minimum PIN length required by the user.

`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.

`Try Attempts`:

- The number of consecutive incorrect PIN attempts permitted. The valid range is 1–7 attempts.

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 re-initialized.

`Allow Trivial PINs`:

- `No`: prevents the use of sequences or consecutive digits/characters longer than 2. For example, 124 is permitted; 123 is not permitted.

- Yes: no sequence checking. For example, 123 is permitted.

PIN Change Period:

- The period in days between forced PIN changes. The value 0 means unlimited. This option is valid only with Stored on Server PINs.

Mode:

- QUICKLog: passcode is displayed immediately by 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.

QUICKLog™ is the recommended mode for all token types. Challenge-response is not supported in all networking environments and requires more user involvement. Challenge-response mode should be used with RB-1 tokens only if required.

Algorithm:

- Mk 1 Algorithm: supports older token types using DES only.
- Mk 2 Algorithm: supported on most token types and supports DES, 3DES, AES (128/192/256). This mode is automatically selected if supported by the token. RB-1 tokens with serial numbers beginning with 2021xxxxx support this algorithm. The encryption algorithm used in all other series is permanently factory preset.

Challenge in QUICKLog mode:

- No: a challenge is not displayed to the user. This is the recommended setting.
- Yes: a challenge is displayed if supported by network equipment. User will not need to key challenge into token unless token is out of synchronization.

Passwords per power cycle:

- 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.

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.

User can turn token off:

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

The Yes setting is recommended when using the RB-1 token.

Start date:

- The first date, in yyyymmdd format, that the token may be used to authenticate.

Expiry date:

- The last date, in yyyymmdd format, that the token may be used to authenticate.

When an operator changes the Expiry date, the change immediately becomes active on the server and valid for the affected token. This is often used for periodic access typical of contractors. It permits the token to be issued once, while ensuring that the user can only authenticate with an active token during the set periods.

Operational Flags:

- Force PIN change on next use: If checked, the user must change his PIN on the next authentication attempt and the box is cleared on PIN change.

Property Flags:

- Delete token at expiry: On expiry, this token is automatically removed from inventory, if checked.
- Don't change key at initialization: the encryption key used for this token is reused during re-initialization, if checked. It is recommended that this box remain clear to ensure that keys are changed with every initialization.

Usage Flags:

- Authentication enabled: token can be used to authenticate, if checked.
- Signature enabled: If this usage flag is checked, the token may be used to generate digital signatures.

Using the RB-1, PIN Stored on Server

In this mode (assuming QUICKLog™ 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.

The `Stored on server, Server-changeable PIN` mode is currently not supported when performing MSCHAPv2 authentication requests.

Generating a Passcode

Press the `PASSWORD` button to activate the token. A one-time passcode is automatically generated.

Enter the PIN (e.g. `ABCD`) and passcode (e.g. `12345678`) at the password prompt (`ABCD12345678`).

Changing PIN

If enabled, this feature permits the PIN to be changed according to the established security policy.

The CRYPTO-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 CRYPTO-Server. In both cases, the PIN will meet the minimum PIN policy requirements (complexity, length, non-trivial, etc.) as configured on the Server. A CRYPTO-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 the RB-1, Token Activated by PIN

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 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 the ENT once all of the 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 of the PIN digits have been entered.
    a. In QUICKLog™ mode: The token displays the one-time passcode.
    b. 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), he 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 (i.e. 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.

Press ENT and repeat step 2 if multiple signatures are required.

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` to select this option. The token will display the current LCD contrast level (e.g. `-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. CRYPTO-Console, and a serial or USB token initializer are required. To initialize a token:

1. To prepare an RB-1 token for initialization, 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 CRYPTO-Console GUI directions for token initializations. Click `Next` to initialize. The token will display the `CARD OK` message on successful initialization.

Battery Replacement

CRYPTOCard 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.

3. Remove the battery compartment cover.

4. Remove one battery and replace it with a new battery (CR2016).

5. Remove the other battery and replace it.