# SafeNet Authentication Service

# Token Guide

## KT-4 Token

## Document Information

| | |
|---|---|
| **Document Part Number** | 007-012410-002, 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.<br>4690 Millennium Drive<br>Belcamp, Maryland  21017, USA |
| **Email** | TechPubs@safenet-inc.com |

# Contents

# Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)** - A cloud authentication service of SafeNet Inc.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)** - The software used to build a SafeNet authentication service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)** - A term used to describe the implementation of SAS-SPE on customer premises.
- KT-4 Keychain tokens

# Overview

The KT-4 Keychain token generates a new, pseudo-random passcode each time the token is activated. The token is activated by pressing the button located to the right and below the LCD display.

A KT-4 PIN consists of a string of 3 to 8 characters that is used to guard against unauthorized use. If PIN protection is enabled, the user must provide a PIN with the one-time passcode to authenticate.


# Token Control

Depending upon the options enabled in the token, the user may be permitted to enter a PIN, change his PIN, or resynchronize the token. These actions require the use of the button to accept options presented to the user through the LCD display. The token will provide prompts and allow the user to input the digits 0 through 9, the letter **E**, and the symbol ┤.

Where input is required, the token will cycle through the input options. When the correct digit, letter, or symbol is displayed, the user pushes the button to accept the input. For example, to input the PIN 123, the user will press the button 3 times, once after each of the numbers 1, 2, and 3 is displayed, respectively, followed by **E**.

Pressing the button when the letter **E** is displayed indicates to the token that the user will provide no additional input. Pressing the button when the ┤ symbol is displayed erases the input immediately to the left of the symbol. This is used to correct input error.

# Operating Modes & Options

The KT-4 supports a wide range of operating modes that can be modified using the SafeNet Authentication Service Manager and a 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 *SafeNet Authentication Service Administrator Guide* for a complete list of modes and options.

## QUICKLog

Password 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 SafeNet KT, RB and MP series 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, **QUICKLog** mode is supported by all systems that require a logon password.

## 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

- **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.

## Manual Shut-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). This setting is recommended when using the KT-4 token.

## Auto 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.

## PIN Policy Group

PIN styles are separated into two general groups: **Stored on Server** or **Token Activated by PIN**. The KT-4 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). When operating in this mode, the PIN can consist of alphanumeric characters.

- **No PIN:** Means that 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** 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-changeable 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 two (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.

# Using the KT-4 with 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

Press the 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 (e.g., ABCD12345678).

## Changing PIN

If enabled, this feature permits the PIN to be changed according to the established security policy (applies to PIN Style **Stored on server, User-changeable PIN** and **Stored on server, Server-changeable PIN**).

The SafeNet Authentication Service 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 SafeNet Authentication Service. In both cases, the PIN will meet the minimum PIN policy requirements (complexity, length, non-trivial, etc.) as configured on the Server. A SafeNet Authentication Service 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 KT-4 with 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. The KT-4 supports numeric PINs only in this mode. Note that the PIN is not prepended to the passcode and is never sent across the network.

## Generating a Passcode

Press button to enable token. The token will display the prompt: **PIN?** #, where # corresponds to:

- The digits 0 through 9 that are used for the PIN. Press the button when the correct digit of the PIN is displayed.
- **E**, which is used to indicate that all digits of the PIN have been entered. This applies only where the PIN length is 7 or less. Press the button when **E** is displayed and all digits of the PIN have been entered.
- ┤, which is used to erase an incorrectly entered digit. Press the button to erase the digit to the left of the ┤ symbol.

For example, if the PIN is **123**:

| Token Displays | Action |
|---|---|
| PIN ? | Press Button |
| *2 | Press Button |
| **3 | Press Button |
| ***E | Press Button |

The token will display the one-time passcode.

## User-changeable PIN

If configured, the KT-4 permits the user to change the PIN required to activate the token. The user can change the PIN when the **Chg PIN** prompt is displayed. When the user keys in the initial PIN (sometimes referred to as the deployment PIN), he will be prompted with **Chg PIN** 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 and hold the button (approximately 3-4 seconds) on the token until the **Init** prompt appears. Then release the button.
2. The token will cycle through a series of prompts: **Init**, **Lcd**, **Chg PIN**, and **rESYNC**. The prompts and sequence will vary depending on the options enabled for the token. Press the button while the **Chg PIN** prompt is displayed.
3. Press the button as each digit of the current PIN is displayed. To accept the entered PIN, press the button when **E** is displayed.
4. At the **NuPIN?** prompt, use the button to select the new PIN, one digit at a time as the correct digits are displayed. To accept the entered PIN, press the button when **E** is displayed.
5. At the **AgAin?** Prompt, use the button to re-input the new PIN by repeating step 4.
6. The token displays a **PASS** message to indicate that the new PIN has been accepted. For example, if the old PIN is **123** and the new PIN is **7835**:

| Token Displays | Action |
|---|---|
| PIN ? | Press Button |
| -2 | Press Button |
| --3 | Press Button |
| ---E | Press Button |
| NuPIN? 7 | Press Button |
| 78 | Press Button |

| | |
|---|---|
| 783 | Press Button |
| 7835 | Press Button |
| 7835E | Press Button |
| AgAin? 7 | Press Button |
| 78 | Press Button |
| 783 | Press Button |
| 7835 | Press Button |
| 7835E | Press Button |

# Token Resynchronization

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.

After the token has been resynchronized, a passcode is being displayed.

In the unlikely event that the token requires resynchronization with the authentication server:

1. Press and hold the button (approximately 3-4 seconds) on the token until the Init prompt appears. Then release the button.
2. The token will cycle through a series of prompts: **Init**, **Lcd**, **Chg PIN**, and **rESYNC**. The prompts and sequence will vary depending on the options enabled for the token. Press the button while the **rESYNC** prompt is displayed.

   The digits 0 through 9 will be displayed sequentially to the right of the **rESYNC** prompt. For every digit of the resynchronization challenge, press the button to accept the displayed digit.

   Note: After the last digit of the “challenge” is entered, double-press the button.

   For example, if the resynchronization challenge is **16278371**:

| **Token Displays** | **Action** |
|---|---|
| rESYNC 1 | Press button |
| 16 | Press button |
| 162 | Press button |
| 1627 | Press button |
| 16278 | Press button |
| 162783 | Press button |

| | |
|---|---|
| 1627837 | Press button |
| 16278371 | Press button |
| 16278371 | Press button |

# LCD Display Test

The KT-4 provides a test routine that checks all individual segments and icons of the LCD for proper operation. To enable the test:

1. Press and hold the button (approximately 3-4 seconds) on the token until the **Init** prompt appears. Then release the button.
2. The token will cycle through a series of prompts: **Init**, **Lcd**, **Chg PIN**, and **rESYNC**. The prompts and sequence will vary depending on the options enabled for the token. Press the button while the **Lcd** prompt is displayed.
3. The token will cycle through a series of displays that provide a visual indication of any malfunctioning segments or icons. The token will shut off automatically on completion of the test, depending on the time set for **Automatic shut-off time**.

# Token Initialization

The KT-4 can be reprogrammed as often as required to enable new options, encryption modes, and keys. SafeNet Authentication Service Manager and a USB token initializer are required.

**To initialize a token:**

1. To prepare a KT token for initialization, start with the KT-4 token off, press and hold the KT-4 token button until the display shows **Init** (approximately 3-4 seconds).
2. Release and quickly press the button again. The display will show the prompt **rdY 4 Ir**. The KT-4 token will remain in the **rdY 4 Ir** state for approximately 1 minute. The token cannot be initialized while in any other state.
3. Insert the token into the initializer with the LCD display facing into the initializer.
4. Follow the instructions on the SafeNet Authentication Service Manager. The token will display the **TOKEN OK** message on successful initialization. The token will shut off automatically 10-15 seconds after initialization.

# 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.<br>4690 Millennium Drive<br>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<br>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. | |