RSA SecurID® Software Token Security Best Practices Guide for RSA Authentication Manager 8.x

Revision Number 9

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

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

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIM IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Dates: April 2011, December 2012, June 2014, March 2015, June 2017, July 2017, October 2020

Revision History

Revision Number	Date	Section	Revision
1	March 17, 2011		Version 1
2	March 21, 2011	Protecting Mobile Devices	Added information about Microsoft Exchange ActivSync.
		PIN Management	• Provided more detailed software token PIN recommendations for RSA Authentication Manager 6.1 and 7.1. • Revised recommendations for configuring PIN policies
		Device Management	Changed “Token binding” to “Token device binding.”
		Help Desk Guidance	Removed the reference to “device password.”
		Customer Support Information	New list of Customer Support phone numbers
3	April 8, 2011	Protecting Software Token Distribution Files	Added information about using default settings when issuing software tokens.
		PINless Tokens	New section of recommendations for using PINless tokens.
		PIN Management	• New links to Knowledgebase articles that provide procedures related to the recommendations. • Reprioritized the list of recommendations.
		Preventing Social Engineering Attacks	New recommendations about Help Desk administrators interacting with users.
		Confirming A User’s Identity	New section for Help Desk administrators describing methods of confirming a user’s identity.
4	Dec. 1, 2012	All	Edited document to improve precision and clarity
		Protecting Mobile Devices	Added information about third-party device management solutions for iOS and Android devices.
		PIN Management	Clarified that by default, RSA Authentication Manager 7.1 locks the user account after three incorrect authentication attempts, whereas RSA Authentication Manager 6.1 disables the token.
		Token Management	Made information on Handling Lost Tokens into a separate subsection.
5	June 2014	All	• Updated to include information for RSA Authentication Manager 8.x. • Added information about protecting custom CTF URLs • Replaced Customer Support contact

			information with RSA Customer Support URL
6	March 2015	Software Token Seeds	Added information that RSA Authentication Manager 8.x always securely randomizes the software token seed.
		Protecting Backup Files	Added a new section with rules for securing backup files.
		Device Management	Stated that RSA SecurID Software Token products are not supported on rooted or jailbroken mobile devices.
		Handling Lost Tokens	Expanded the description for what to do when a user loses a token.
		Removing or Suspending User Accounts	Added recommendations for what to do about users who have left the organization permanently or for an extended period of time.
7	June 2017	Software Token Distribution, Device Management	Updated description of device binding.
8	July 2017	All	• Added information about binding IDs. • Added cross-references to other product documentation. • Added section on token provisioning options. • Removed information for RSA Authentication Manager 6.1 and 7.1.
9	October 2020	Software Token Distribution, Device Management	• Updated the Device Binding references.

Introduction

This guide is intended to identify best practices designed to help ensure secure operation of RSA SecurID® Software Token products. It is your responsibility to ensure that your software token products are used properly and carefully monitored and maintained. Use this guide in conjunction with your software token documentation, and with the following:

- *RSA® Authentication Manager Security Configuration Guide*
- *RSA SecurID® Authentication Engine (SAE) Best Practices Guide*

This guide is intended for customers using RSA Authentication Manager 8.0 and later. RSA strongly recommends customers using versions prior to RSA Authentication Manager 8.0 upgrade to the latest version of RSA Authentication Manager at the earliest possible opportunity.

RSA periodically assesses and improves its Best Practices Guides. Please check RSA Link for the latest documentation.

Token Data Protection

Software Token Seeds

RSA Authentication Manager products are engineered to securely randomize the software token seed when a token is issued so that the previous seed is no longer valid.

RSA SecurID Authentication Engine (SAE) is designed to randomly generate a new seed for each software token when you import a manufacturing token record XML file containing software tokens into the API. For more information, see the SAE documentation.

Software Token Provisioning Options

There are a few options for distributing software tokens:

- Dynamic seed provisioning: A four-pass protocol that uses the Cryptographic Token Key Initialization Protocol (CT-KIP) to eliminate the need for a token distribution file.
- File-based provisioning (SDTID files): Software token files (SDTID files) that can be distributed as an email file attachment.
- Compressed Token Format (CTF strings): Alphanumeric or numeric format for delivering software tokens to mobile devices.

RSA recommends using the RSA Authentication Manager dynamic seed provisioning feature because the CT-KIP process helps prevent the potential interception of the token's seed. Only use SDTID or CTF if your company policy dictates that the Token apps cannot connect to the Internet or that a CT-KIP server cannot be set up.

Dynamic Seed Provisioning

Dynamic seed provisioning eliminates the need for a token distribution file (SDTID file). The RSA SecurID app running on a device (the client) and Authentication Manager (the CT-KIP server) use a four-pass CT-KIP protocol to exchange information that is used to dynamically generate a unique shared seed. Information critical to seed generation is encrypted during transmission using a public-private key pair. The generated token seed value is never transmitted across the network.

For increased security, use dynamic seed provisioning if you provision software tokens with RSA Authentication Manager because the CT-KIP process is engineered to prevent the potential interception of the token's seed.

The RSA SecurID app must send a one-time provisioning activation code when it initially contacts the CT-KIP server. The CT-KIP server evaluates the activation code to verify that the token is approved for dynamic seed provisioning. You deliver a dynamically provisioned token with a QR code or by sending an email containing a custom CT-KIP URL hyperlink to the email client on a supported platform (for example, iOS or Android).

For more information, see "Dynamic Seed Provisioning" in the *RSA SecurID Software Token for iOS Administrator's Guide* and the *RSA SecurID Software Token for Android Administrator's Guide*, "Use Dynamic Seed Provisioning to Deliver Software Tokens" in the *RSA SecurID Software Token for Windows Administrator's Guide*, and "Dynamic Seed Provisioning for Software Token Delivery" in the *RSA Authentication Manager Security Configuration Guide*.

File-based Provisioning (SDTID Files)

RSA Authentication Manager and RSA SecurID Authentication Engine (SAE) for Java are designed to generate software token files (SDTID files). RSA strongly recommends protecting SDTID files with a token file password as part of the provisioning process.

To deliver a token, you send an email with an SDTID file attachment to the email client on the device. If you password-protect the file, RSA recommends sending the password separately, using a secure channel and best practices for communicating sensitive data.

For more information, see "File-based Provisioning (SDTID Files)" in the *RSA SecurID Software Token for iOS Administrator's Guide* and the *RSA SecurID Software Token for Android Administrator's Guide*.

Compressed Token Format (CTF Strings)

Compressed token format (CTF) is an alphanumeric or numeric format for delivering software tokens to mobile devices. RSA strongly recommends protecting CTF strings with a strong password. RSA Authentication Manager 8.x can natively generate custom CTF URLs. Using the Security Console, you configure a software token, select the CTF distribution option, and select the option to password protect the token.

For more information, see "Compressed Token Format (CTF Strings)" in the *RSA SecurID Software Token for iOS Administrator's Guide* and the *RSA SecurID Software Token for Android Administrator's Guide*."

Software Token Distribution

Take the following steps to protect software tokens during distribution:

- Assign strong passwords to all software tokens distributed as SDTID files. Use passwords that conform to best practices. Send the password to the user separately from the token SDTID file, using a secure channel.
- Assign strong passwords to custom CTF URLs. RSA Authentication Manager can natively generate custom CTF URLs. Using the Security Console, you configure a software token, select the CTF distribution option, and select the option to password protect the token.
- Use the Security Console in RSA Authentication Manager to bind all software tokens to binding IDs.

Binding is engineered to allow installation only on a device or class of devices with a matching device ID. You can bind to either the class GUID or the binding ID.

Instruct users to treat the binding ID as sensitive information and to use a secure channel to deliver it to the administrator. After the user sends the administrator the binding ID, the administrator should use a separate, secure channel to communicate the information needed by the Token app to complete the provisioning process, for example, the CT-KIP URL.

The binding ID helps ensure that the provisioned token goes to a specific device or set of devices and should be part of a comprehensive strategy of maintaining security during the provisioning process. During your provisioning workflow, confirm that each item needed for provisioning is included in separate, secure communications and not combined into a single communication.

RSA best practices recommend that the CTF be password-protected and that the CTF NOT be communicated together with the binding ID.

RSA best practices also recommend the token be distributed in a disabled state with a temporary PIN assigned.

Important: If an adversary obtains the CTF URL, binding ID, password, and PIN, it is conceivable that an adversary could emulate this binding ID on a separate, rooted or “jail-broken” device, and the binding ID control could be circumvented.

For more information, see “Device Binding” in the software token administrator’s guide for your device operating system.

- After a user successfully provisions a token, instruct the user to delete all e-mails and files containing token information from their devices. This includes e-mails containing custom CTF URL links, file attachments containing token distribution files (SDTID files), and e-mails or files containing custom CT-KIP URLs and activation codes. RSA SecurID software token products make an attempt to remove this information upon successful import, but systems and other applications are beyond the scope of the software token application.

  In addition, instruct users to never share their token files, custom CTF or CT-KIP URLs, or activation codes, and caution them to accept token provisioning information only from trusted sources.

Tokencode Tokens (No PIN Required)

As a security best practice, you should require PINs as part of RSA SecurID authentication. If you choose to use PINless RSA SecurID tokens (Tokencode tokens), make sure the system enforces a second authentication factor, such as a Windows password.

Important: If the system does not have a second factor and one cannot be implemented, reconfigure your RSA SecurID tokens to require a PIN. If you cannot reconfigure all tokens, and you are using RSA Authentication Manager, regularly audit your agents on systems that do not require a second authentication factor for Tokencode token users.

- Implement Help Desk procedures to ensure that administrators:
  - Allow a user to authenticate with a Tokencode token only when the user requires access to systems that enforce an additional authentication factor.
  - Allow a user to authenticate with a Tokencode token only when there is a second authentication factor required on every system the user may access.
- Flag groups that contain users with Tokencode token to ensure that these groups are enabled only on agents that protect systems requiring a second authentication factor. If you use Tokencode tokens, log and review the audit trails for the following activities to ensure that these operations are performed by properly authenticated and authorized entities:
  - Agent creation
  - Group creation and assignment
  - Group membership changes
  - Token assignment
  - Tokencode token enablement

For more information, see "Tokencode Tokens (No PIN Required)" in the RSA Authentication Manager Security Configuration Guide.

Protecting Desktop and Laptop Devices

The Microsoft Windows or Mac OS X operating systems provide the foundation of the security environment for the RSA SecurID Software Token product for Windows and Mac desktops. To help maintain the security of the platform, make sure that users keep their operating system updated with the latest security patches.

In addition, require desktop and laptop software token users to set a device password to protect all tokens stored on the local hard drive. Setting a device password helps ensure that only the user for whom the tokens are intended can access the tokens.

Protecting Mobile Devices

Instruct users to enable the device PIN or device password available on their mobile platforms. Once these security features are enabled, users are required to enter their PIN or password to access the applications installed on the device. Enterprises should establish policies requiring the use of a device PIN or device password for access when deploying RSA SecurID software token products to mobile platforms. For Blackberry 10 deployments, your IT department should use the Blackberry Enterprise

Server (BES) 10 or later to enforce these policies across all managed Blackberry devices. A variety of third-party solutions are available for managing iOS and Android devices.

For more information, see “Supported Token Types” in the *RSA SecurID Software Token for iOS Administrator’s Guide* and the *RSA SecurID Software Token for Android Administrator’s Guide*.

Protecting Backup Files

Mobile device backup files can contain sensitive application data. Instruct your users to encrypt any backup files, and store the backup files in a secure location.

During the restore process, a user might need to provide a password so the backup can be decrypted. Instruct users to record the password into safe locations, as dictated by your organization’s policies, so that it will be available when the mobile device needs to be restored.

For more information, see “Perform Encrypted Backups Using iTunes” in the *RSA SecurID Software Token for iOS Administrator’s Guide*.

Token Management

PIN Management

Take the following actions to help protect RSA SecurID PINs:

- Instruct all users to guard their PINs and to never tell anyone their PINs. Administrators and Help Desk personnel should never know or ask for the user’s PIN.
- If possible, do not use 4-digit PINs. If you must use a short PIN (a 4-character PIN), require alphanumeric characters (a-z, A-Z, 0-9) when the token type supports them.
- Configure Authentication Manager to require users to change their PINs at regular intervals. These intervals should not exceed 60 days. If you use 4-digit numeric PINs, the intervals should not exceed every 30 days. For information about requiring periodic PIN changes for users, see the Security Console Help topic “Edit a Token Policy.”
- Configure policies that restrict the re-use of PINs.
- Configure the use of the dictionary to prevent the use of simple PINs.
- When software tokens are issued as PINPad-style tokens, the software token PIN should be equal in length to the tokencode, and all numeric.
- When software tokens are issued as fob-style tokens, the software token PIN should be alphanumeric and eight digits in length. To require alphanumeric PINs, an administrator must configure the token policy in the Security Console.

Note: It is important to achieve the right balance between security best practices and user convenience. If alphanumeric 8-digit PINs are too complex, enforce the strongest PIN policy that meets your company policy.

For more information, see “PIN Management” in the *RSA Authentication Manager Security Configuration Guide*.

Device Management

To avoid authentication issues with RSA Authentication Manager or with applications that integrate RSA SecurID Authentication Engine (SAE), do not allow users to install a software token identified by a unique serial number on more than one device. Installing a token with the same serial number on multiple devices with different time sources may result in authentication failures on the authentication server. Use token device binding to allow a user to install a token on one device.

Distribution of applications and software may take many forms on the various platforms. In many cases, the platform is a mobile device owned by the user, and the device may or may not be managed by the enterprise. Caution users to obtain application software for their device from trusted sources only.

RSA does not support installing RSA SecurID Software Token products on a rooted Android mobile device or a jailbroken iOS mobile device. Do not allow such a device in your deployment.

For more information, see “Device Binding” in the software token administrator’s guide for your device operating system.

Handling Lost Tokens

Instruct users to report lost mobile devices or laptops that contain a software token as soon as possible to the Help Desk administrator. The Help Desk administrator should confirm the user’s identity and ensure that the token is disabled for use until either the device is found or a replacement device is obtained and provisioned with a replacement token.

In addition, ask the user for information on when the device was lost. Make note of the date and audit your logs for authentication attempts with the lost token. Follow your organization’s security policy to address any suspicious authentication attempts.

For more information, see “Lost Tokens” in the *RSA Authentication Manager Security Configuration Guide*.

Removing or Suspending User Accounts

If a user leaves your organization, delete any corresponding user accounts as soon as possible. Use your RSA Authentication Manager product to delete users who are stored in the internal database as their identity source. You can delete users who use an LDAP directory as their identity source only by using the native LDAP directory interface.

If an RSA Authentication Manager user is on an extended absence, you can disable the user account and enable the account when the user returns to work. When you disable a user account, you suspend the user’s permission to authenticate, which prohibits access to protected resources. For more information, see “Disable a User Account” in the *RSA Authentication Manager Help*.

Help Desk Guidance

Educate users about the information they should share with Help Desk administrators. Instruct users never to disclose the token serial number to anyone other than a Help Desk administrator and to provide the serial number only when a user is having a problem with a token.

Make sure that users are aware of information that Help Desk administrators should not request, including a device PIN or device password, PIN, tokencode, passcode, or token distribution password. Inform the user that any request for this information should signal that a social engineering attack may be in progress.

For more information, see “Procedures and Training” in the *RSA Authentication Manager Security Configuration Guide*.

Supporting Users

Establish secure Help Desk procedures for your RSA SecurID deployments. Make sure that during your provisioning workflow, Help Desk administrators understand to include each item that is needed for provisioning in separate, secure communications and not combined into a single communication. Make sure that Help Desk administrators understand the importance of PIN strength and the sensitivity of data such as the user’s logon name and token serial number. Instruct Help Desk administrators to request sensitive data only when absolutely necessary to decrease the opportunity for social engineering attacks. Train Help Desk administrators to request, and users to provide, the minimum amount of information needed in each situation. Inform users of what information requests to expect from Help Desk administrators.

Advice for Users

Instruct users to do the following:

- Never give the token serial number, PIN, tokencode, token, passcode, or passwords to another user.
- To help prevent phishing attacks, do not enter tokencodes into links that you clicked in e-mail. Instead, type in the URL of the authorized website to which you want to authenticate.
- Before navigating your browser to a website that requires you to provide a tokencode, close the browser completely and restart it from a clean state.
- Regularly close your browser and clear your cache of data.
- Always log out of applications when you have finished working with them.
- Always lock your desktop when you leave your workspace.
- Immediately report lost or stolen tokens.

Note: Consider regular training to communicate this guidance to users.

For more information, see “Advice for Users” in the *RSA Authentication Manager Security Configuration Guide*.

Preventing Social Engineering Attacks

Fraudsters frequently use social engineering attacks to trick unsuspecting users into divulging sensitive data that can be used to gain access to protected systems. Instruct Help Desk administrators to use the following guidelines to reduce the likelihood of a successful social engineering attack:

- Only ask for a user’s User ID over the phone when the user calls the Help Desk. Never ask for tokencodes, PINs, passwords, and so on.
- Provide the Help Desk telephone number to all users.
- Confirm a user’s identity before performing any administrative action on a user’s token or PIN. For example, ask the user a question only they know the answer to as a means of verifying their identity.

- When you need to initiate contact with a user, do not request any user information. Instead, instruct the user to call back the Help Desk at the authorized Help Desk telephone number to verify the original request.
- To confirm that all PIN changes are requested by authorized users, establish a policy to notify users when their PINs have been changed. For example, send an e-mail notification to the user's corporate e-mail address, or leave a voice message. Users who suspect a change was made by an unauthorized person should contact the Help Desk.

For more information, see "Preventing Social Engineering Attacks" in the *RSA Authentication Manager Security Configuration Guide*.

Confirming a User's Identity

Help Desk administrators must verify a user's identity before performing any Help Desk operations on the user's behalf. Specific actions include the following:

- Call the user back on a phone owned by the organization and on a number that is already stored in the system.

  Important: Avoid using mobile phones for identity confirmation, even if they are owned by the enterprise, as mobile phone numbers are often stored in locations vulnerable to tampering or social engineering.

- Send the user an e-mail to a company address. If possible, use encrypted e-mail.
- Work with the employee's manager to verify the user's identity.
- Verify the user's identity in person.
- Ask multiple open-ended questions from employee records (for example: "Name one person in your group"; "What is your badge number?"). Do not ask questions that can be answered yes or no.

For more information, see "Confirming a User's Identity" in the *RSA Authentication Manager Security Configuration Guide*.

Customer Support Information

You can access community and support information on RSA Link at https://community.rsa.com. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.