RSA SecurID Software Token Security Best Practices Guide

Version 3

The Security Division of EMC

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: **www.rsa.com**.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**.

License Agreement

The guide and any part thereof is proprietary and confidential to EMC and is provided only for internal use by licensee. Licensee may make copies only in accordance with such use and with the inclusion of the copyright notice below. The guide and any copies thereof may not be provided or otherwise made available to any other person.

No title to or ownership of the guide or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of the guide may be subject to civil and/or criminal liability.

The guide is subject to update without notice and should not be construed as a commitment by EMC.

Note on Encryption Technologies

The referenced 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 the referenced product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Disclaimer

EMC does not make any commitment with respect to the software outside of the applicable license agreement.

EMC believes the information in this publication is accurate as of its publication date. EMC disclaims any obligation to update after the date hereof. The information is subject to update without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED TO SUGGEST BEST PRACTICES, IS PROVIDED "AS IS," AND SHALL NOT BE CONSIDERED PRODUCT DOCUMENTATION OR SPECIFICATIONS UNDER THE TERMS OF ANY LICENSE OR SIMILAR AGREEMENT. EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

All references to "EMC" shall mean EMC and its direct and indirect wholly-owned subsidiaries, including RSA Security LLC.

Copyright © 2011 EMC Corporation. All Rights Reserved.

April 2011

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.

Introduction

This guide is intended to help identify configuration options and best practices designed to ensure secure operation of RSA SecurID® Software Token products, and offer maintenance recommendations, however, it is up to you to ensure the products are properly monitored and maintained when put on your network. Use this guide in conjunction with your software token documentation, and with your applicable RSA Authentication Manager product documentation and RSA Authentication Manager Security Best Practices Guide.

RSA periodically assesses and improves all product documentation. Please check RSA SecurCare® Online for the latest documentation.

Protecting Software Token Distribution Files

RSA strongly recommends that all RSA SecurID Software Token products distributed as files or as Compressed Token Format (CTF) strings be protected with strong passwords that conform to best practices for password selection.

RSA also strongly recommends that all software token distribution files or strings utilize device binding designed to limit the installation of tokens to only those machines matching the binding information. Refer to your software token documentation for more details on implementing token binding for your platform.

By default, in Authentication Manager 6.x and 7.x, the software token seed is securely randomized when the token is issued so that the previous seed is no longer valid. The default settings should always be used. (In Authentication Manager 6.1, “Retain Token Info” should be disabled; in Authentication Manager 7.1, “Regenerate Token” should be enabled).

PINless Tokens

If you use PINless RSA SecurID tokens (also known as Tokencode Only), you should immediately ensure that a second authentication factor, such as a Windows password, is required to authenticate to protected systems.

Important: If the system does not have a second factor and one cannot be implemented, RSA strongly recommends switching your RSA SecurID tokens to require a PIN immediately. If you cannot switch all tokens to require a PIN, RSA strongly recommends auditing agents on systems that do not require a second authentication factor for PINless token users.

- Implement help desk procedures that ensure that administrators:
    - allow a user to authenticate with a PINless token only when the user requires access to systems that enforce an additional authentication factor.
    - allow a user to authenticate with a PINless token only when there is a second authentication factor required on every system the user may access.
    - flag groups that contain users with PINless tokens to ensure that these groups are enabled only on agents that protect systems that require a second authentication factor.
- If you use PINless tokens, RSA strongly recommends that the audit trails of the following administrative activities be carefully monitored:
    - agent creation
    - group creation and assignment
    - group membership changes
    - token assignment
    - PINless token enablement

Protecting Desktop and Laptop Devices

The Windows or MacOS operating systems provide the foundation of the security environment for the RSA SecurID Software Token product for desktops. RSA strongly recommends that users keep their operating system updated with the latest security patches to help maintain the overall security of the platform.

In addition, RSA strongly recommends that software token users 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

When available, RSA recommends that you enable the device PIN or device password available on your mobile or tablet platforms. Once enabled, you are required to enter the PIN or password to access to the applications installed on the device. Enterprises should establish policies requiring the use of a device PIN for access when deploying RSA SecurID Software Token products to mobile platforms. In the case of Blackberry deployments, the Blackberry Enterprise Server (BES) may be utilized to enforce these policies across all managed Blackberry devices. Microsoft Exchange ActivSync also provides similar controls for iPhone, iPad, Android and other devices.

Recommendations for Users

Token Distribution Media

Upon successful completion of the token provisioning operation for the platform, you should instruct end users to remove all e-mails and files containing token distribution file information from the application or file system, from which the token information was originally obtained. This includes e-mails with links containing Compressed Token Format (CTF) data obtained from the Token Converter tool, file attachments containing token distribution files, and e-mails and files containing CT-KIP activation codes and URLs. The RSA SecurID Software Token products make an attempt to remove this information upon successful import, but e-mail systems and other applications are beyond the scope of the software token application.

RSA strongly recommends that end users never share their token files, strings, or activation codes with anyone, and accept token provisioning information only from trusted sources.

PIN Management

RSA strongly recommends the following to protect RSA SecurID PINs:

- Configure Authentication Manager to lockout a user after three failed authentication attempts. Require manual intervention to unlock users who repeatedly fail authentication. For information about configuring the number of failed attempts, see the following Knowledgebase articles:

  For Authentication Manager 7.1: **a54315 - How to change the failed authentication thresholds**.

  For Authentication Manager 6.1: **a54318 – How to modify number of Incorrect Passcodes before next tokencode mode or disabling token**.

- Instruct all users to guard their PINs and to never tell anyone their PINs. Administrators should never ask for or know the user's PIN.

- Configure Authentication Manager to require users to change their PINs at regular intervals. These intervals should be no more than 60 days. If you use 4-digit numeric PINs, the intervals should be no more than every 30 days. For information about configuring PIN lifetime intervals, see the following Knowledgebase articles:

  - For Authentication Manager 5.2 and 6.1: **a54380 - How do I regenerate the token seed when issuing Software Tokens in Authentication Manager 5.2 and 6.1?**

  - For Authentication Manager 7.1: **a54379 - How do I regenerate the token seed when issuing Software Tokens in Authentication Manager 7.1?**

- For Authentication Manager 7.1, configure policies that restrict the re-use of PINs.

- For Authentication Manager 7.1, configure the use of the dictionary to prevent the use of simple PINs.

- For RSA Authentication Manager 6.1, the software token PIN should be equal in length to the tokencode, and all numeric.

- For Authentication Manager 7.1:

  – when software tokens are issued as PINPad-style tokens (the Displayed Value is set to Passcode in the Software Token Settings), 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 Displayed Value is set to Tokencode in the Software Token Settings), the software token PIN should be alphanumeric and eight digits in length.

Note: It is important to strike the right balance between security best practices and user convenience. If alpha numeric 8-digit PINs are too complex, find the strongest PIN policy that best suites your user community.

Device Management

RSA strongly recommends that in order to avoid authentication issues with the RSA Authentication Manager or RSA SAE-based applications, end users should install a token identified by a unique serial number on only one device. Installing a token with the same serial number on multiple devices with different time sources may result in authentication failures on the server. Token device binding should be utilized to simplify the end user experience and prevent your end users from installing the same token on multiple devices.

Distribution of applications and software may take many forms on the various platforms. In many cases, the platform is owned by the end user, and may or may not be managed by the Enterprise. RSA strongly recommends that end users be trained to obtain application software for their device from trusted sources only.

Lost devices represent lost tokens and should be reported as soon as possible to the Help Desk administrator. The Help Desk administrator must ensure the token is disabled for use until either the device is found or a replacement device is obtained and provisioned with a replacement token.

Help Desk Guidance

RSA strongly recommends educating end users about the information they should share with Help Desk administrators. End users should never disclose the token serial number in whole or part to anyone other than a Help Desk administrator upon request when a problem is occurring with a token.

End users should be aware of information that Help Desk Administrators should not request, including device PIN or device password, PIN, tokencode, passcode or token distribution password. Any request for this information listed should signal to the end user that a social engineering attack may be in progress.

Supporting Your Users

It is crucial to have well defined policies around help desk procedures for your Authentication Manager. Help Desk administrators must understand the importance of PIN strength and the sensitivity of data like the user's login name and token serial number. Creating an environment where an end user is frequently asked for this kind of sensitive data increases the opportunity for social engineering attacks.

Train end users to provide, and Help Desk administrators to request the least amount of information needed in each situation.

Advice for your Users

RSA strongly recommends that you instruct your users to do the following:

- Never give the token serial number, PIN, tokencode, token, passcode or passwords to anyone.
- To avoid phishing attacks, do not enter tokencodes into links that you clicked in e-mail. Instead, type in the URL of the reputable site to which you want to authenticate.
- Inform your users of what information requests to expect from Help Desk administrators.
- Always log out of applications when you're done with them.
- Always lock your desktop when you step away.
- Regularly close your browser and clear your cache of data.
- Immediately report lost or stolen tokens

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

Preventing Social Engineering Attacks

Fraudsters frequently use social engineering attacks to trick unsuspecting employees or individuals into divulging sensitive data that can be used to gain access to protected systems. RSA strongly recommends that you use the following guidelines to reduce the likelihood of a successful social engineering attack:

- Help Desk administrators should only ask for a user's User ID over the phone when they call the help desk. Help Desk administrators should never ask for token serial numbers, tokencodes, PINs, passwords, and so on.
    - The Help Desk telephone number should well-known to all users.
- Help Desk administrators should perform an action to confirm the user's identity before performing any administrative action on a user's token or PIN. For example, ask the user a question that only they know the answer to verify their identity. For more information, see

Confirming a User's Identity.

- If Help Desk administrators need to initiate contact with a user, they should not request any user information. Instead, users should be instructed to call back the Help Desk at a well-known Help Desk telephone number to ensure that the original request is legitimate.
- To confirm that all PIN changes are requested by authorized users, you should have a policy in place 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 voicemail message. Users that suspect a change was made by an unauthorized person should contact the Help Desk.

Confirming a User's Identity

It is critical that your Help Desk Administrators verify the end user's identity before performing any Help Desk operations on their behalf. Recommended actions include:

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

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

- Send the user an e-mail to a company email address. If possible, use encrypted e-mail.
- Work with the employee's manager to verify the user's identity.
- Verify the identity in person.
- Use multiple open-ended questions from employee records (for example: Name one person in your group; What is your badge number?). Avoid yes/no questions.

Customer Support Information

For information, contact RSA Customer Support:

U.S.: 1-800-782-4362, Option #5 for RSA, Option #1 for SecurCare note

Canada: 1-800-543-4782, Option #5 for RSA, Option #1 for SecurCare note

International: +1-508-497-7901, Option #5 for RSA, Option #1 for SecurCare note