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.
## Revision History

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Date</th>
<th>Section</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>March 17, 2011</td>
<td></td>
<td>Version 1</td>
</tr>
<tr>
<td>2</td>
<td>March 21, 2011</td>
<td>Token Data Protection</td>
<td>- New reminder to use a second factor with PINless tokens.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- New recommendation to limit users to one assigned token.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PIN Policy</td>
<td>New recommendation on using 4-character PINs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Replay Attacks</td>
<td>New recommendation on PIN lockout policy to help against replay attacks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Customer Support Information</td>
<td>New list of Customer Support phone numbers</td>
</tr>
<tr>
<td>3</td>
<td>April 8, 2011</td>
<td>PINless Tokens</td>
<td>New section of recommendations for using PINless tokens.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Infrastructure Protection</td>
<td>Added a note about securing test environments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PIN Policy</td>
<td>Modified recommendation on 8-character PINs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Preventing Social Engineering</td>
<td>Added recommendations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Confirming A User’s Identity</td>
<td>New section for Help Desk administrators describing methods of confirming a user’s identity.</td>
</tr>
</tbody>
</table>
Introduction

This guide is intended to help identify configuration options and best practices, and offer monitoring/auditing recommendations for RSA SecurID® Authentication Engine (SAE). However, it is up to you to ensure they are properly monitored and maintained when put on your network. Use this guide in conjunction with SAE product documentation and the RSA SecurID Software Token Best Practices Guide.

For guidance and best practices within a security application, refer to the RSA Authentication Manager Security Best Practices Guide.

Encryption Key Generation

RSA SecurID Authentication Engine for C and Java provide interfaces for obtaining an encryption key that you can use to help protect token data. RSA strongly recommends the following best practices for all RSA SecurID Authentication Engine implementations:

- RSA strongly recommends that you use the APIs available in the SAE toolkit to generate a cryptographically strong encryption key. For information, see your SAE documentation.
- Select passphrases to supply to the key generation functions that conform to industry-standard best practices. For example, select passphrases that are at least 15 characters in length, and which also contain upper and lowercase letters, digits, and punctuation characters, and so on.
- Maintain a backup copy of the keys stored in secure offline locations. The backup copy is required in the event that the key is corrupted or lost.
  
  Have a plan to re-issue your keys should your backup media be corrupted or otherwise unusable.

Backup Media Protection

Information used by RSA SecurID Authentication Engine can be stored in your databases, in Token XML files, and in Token distribution files when RSA SecurID® Software Tokens are used. RSA strongly recommends that you use strong encryption (at least AES-128) to safeguard backup media that may contain this information.
Token Data Protection

Importing new tokens and distributing tokens to users are sensitive operations and if not done properly could expose an organization to security risks. Below is a list of recommendations designed to minimize risk during these sensitive operations.

**Important:** RSA strongly recommends that you do not assign more than one token to a user as this may reduce the likelihood that users will report a lost or stolen token.

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 Token Files

RSA manufacturing or certified partners deliver token files for import into your systems. These files enable the use of strong authentication, and they contain sensitive information about tokens. RSA strongly recommends the following best practices:

- Limit access to these files to individuals responsible for the import of tokens into RSA SecurID Authentication Engine.
- Store backup copies of Token XML files in a secure location, preferably encrypted in a secure location with no network connectivity.
- Files used for the import operation should be permanently deleted from the file system when the import operation is complete.
- Secure any media used to deliver token info to you.

Token Information

RSA recommends a defense-in-depth approach for protecting token data stored in your environment. RSA strongly recommends that your storage systems encrypt the token data with a separate key in addition to the encryption provided by RSA SecurID Authentication Engine. Using two separate keys maximizes the protection of stored token data.

Distributing Software Tokens

RSA strongly recommends that you take the following steps to help protect your software tokens:

- When generating the token files for distribution, protect the files with a password, which encrypts the file.
- Use passwords that conform to best practices. For example, require a minimum of 15 alphanumeric characters, upper and lower case, at least one special character, and no dictionary words.
- Bind software tokens to device IDs when issuing software tokens. This limits the installation of tokens to only those machines that match the binding information. See your software token documentation.

Infrastructure Protection

Applications utilizing SAE are critical in establishing trust and authorization. RSA strongly recommends that you use firewalls to minimize the network access to these systems, and following network security best practices with respect to deployment of their applications. RSA strongly recommends the use of strong authentication for access to these systems.

Note: RSA strongly recommends that your test environments not be exact copies of your full production environment. If they are, you should take the same precautions to protect the test environment as you do your production environment.
Remote Access to Server Environments

Remote access to server system components should be tightly controlled, using the following approaches:

- Disable remote access methods for the operating system, such as telnet, ftp and so on, that communicate over unsecured channels.
- Disable any other remote access method for the operating system, for example, SSH, unless absolutely required for maintenance. Disable immediately when maintenance is complete.

System Security

RSA strongly recommends using the capabilities of the underlying operating system to limit access to data and services on the critical systems of your security infrastructure. For example, use access controls, firewalls, and strong authentication.

Review all user account access for these systems to ensure that default accounts have been disabled, employ the use of best practices with respect to passwords and password lifecycles, and limit the user accounts to authorized personnel. Establish policies for regular review of access logs, and integrate systems with event monitoring and intrusion detection systems, where available, to ensure the fastest response to security-related events.

Patch Management

All security patches for RSA products originate at RSA and are available for download as an update as long as you have a current maintenance agreement in place with RSA. Updates are available on RSA SecurCare Online at https://knowledge.rsasecurity.com. RSA strongly recommends that you immediately register your product and sign up for RSA SecurCare Online Notes & Security Advisories, which RSA distributes via e-mail to bring attention to important security information for the affected RSA products. RSA strongly recommends that all customers determine the applicability of this information to their individual situations and take appropriate action.

If you want to receive or change which RSA product family Notes & Security Advisories you currently receive, log on to RSA SecurCare Online at https://knowledge.rsasecurity.com/scolems/help.aspx?_v=view5.

RSA strongly recommends that customers follow best practices for patch management and regularly review available patches for all software on systems that host applications that use SAE, including anti-virus and malware software, and operating system software.
Physical Security Controls

Physical security controls help enable the protection of resources against unauthorized physical access and physical tampering. Customer applications utilizing SAE are critical network components so it is very important that physical access be restricted to authorized personnel only. Limit or eliminate the availability of any remote access capabilities that may be used for management purposes.

While following your organization’s security policy, RSA strongly recommends that you implement the following physical security controls:

- Allow only authorized users to physically access applications using SAE.
  - Access to systems hosting applications using SAE should be physically secured, for example, in cabinets with tamper-evident physical locks, and audited on-site access.
  - Secure the server room such that it is only accessible by authorized personnel and audit that access.
  - Minimize the number of people who have physical access to devices hosting applications using SAE.
- Use room locks that allow traceability and can be audited
- Employ strong access control and intrusion detection mechanisms where the product cabling, switches, servers, and storage hardware reside.
- Place tamper evident stickers on each server chassis and other hardware.

System Hardening and Deployment Considerations

To help ensure the highest level of security and reduce the risk of intrusion or malicious system or data access, RSA strongly recommends that you follow industry best practices for hardening the network infrastructure, including, without limitation:

- You should run anti-virus and anti-malware tools with the most current definition files.
- You should not directly connect servers that host applications that use SAE to the Internet or place them in a De-Militarized Zone (DMZ).
- You should not co-host applications that use SAE on the same operating system instance with other software.
- On UNIX systems, you should run applications that use SAE under their own service account and restrict access to its files to that service account. You will not be able to change this service account after installation.

Using a Firewall

It is important to restrict network traffic between systems hosting SAE based applications and external systems. RSA strongly recommends that customers utilize firewalls to minimize the network access to applications using SAE, and follow network security best practices.
PIN Policy

RSA SecurID Authentication Engine does not provide a specific policy for PIN assignment or usage. RSA strongly recommends the following:

- Use PINs to provide strong two-factor authentication to systems and resources.
- Instruct users to guard PINs and to never tell anyone their PINs. Administrators should never know or ask for the user’s PIN.
- Your corporate PIN policy should require the use of 6-character to 8-character PINs. RSA recommends that your PIN policy requires alphanumeric characters (a-z, A-Z, 0-9) when the token type supports them.
- Do not use 4-character numeric PINs. If you must use a short PIN (e.g. a 4-character PIN), require alphanumeric characters (a-z, A-Z, 0-9) when the token type supports them.
- For software tokens, the PIN should be equal in length to the tokencode, and all numeric.
- Change PINs at regular intervals. These intervals should be no more than 60 days. If you use 4-character numeric PINs, change them no more than every 30 days.

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

Token Administration

Limit access to token administration operations to authorized personnel that are responsible for the administration of tokens in the application. Use strong authentication for all interfaces that provide access to administration capabilities. You are responsible for implementing these interfaces, as well as for providing log and audit functionality.

Time Management

Systems hosting SAE-based applications provide validation capabilities for One-Time Password (OTP) and signature values, and must be synchronized to the correct time. Moving the clock on the server forward or backward may affect the ability of the server to validate OTP or signature values. RSA strongly recommends that you use NTP to ensures continuous time integration and prevent significant time drifts for the server.
Assigning Tokens to Users

RSA strongly recommends the following best practices for assigning tokens:

- **Hardware Tokens**—Distribute hardware tokens in a disabled state until you can verify that the intended user has received the token.

- **Software Tokens**—Before issuing a software token, generate a fresh, unique and unpredictable random number to be used as the seed. This prevents different users in your organization from obtaining the same token seed.

  The SAE API provides methods for performing this operation. See your SAE documentation for information.

Unassigning Software Tokens

When you unassign a software token:

- Disable the token.

- Generate a fresh, unique and unpredictable random number to be used as the seed. This prevents different users in your organization from obtaining the same token seed.

  The SAE API provides methods for performing this operation. See your SAE documentation for information.

Handling Lost Tokens

When a user reports a lost token, RSA strongly recommends that you take the following steps:

- Help Desk administrators should perform an action to confirm the user’s identity. For example, ask the user one or more questions to which only he or she knows the answer.

- Ask the user when they lost the token.

- Disable the token.

- Make note of the date and audit your logs for authentication attempts with the lost token until the token is recovered. Follow your organization’s security policy to address any suspicious authentication attempts.
Token Operation

RSA strongly recommends enabling the following security features.

Next Tokencode Mode

RSA recommends that RSA SecurID Authentication Engine applications support the implementation of Next Tokencode mode and handle the status and exception messages required from the API. Information should be logged to your event database. You should regularly review the logs to collect information on instances where Next Tokencode mode is activated.

Replay Attacks

RSA strongly recommends that:

- RSA SecurID Authentication Engine applications handle the status and exception messages that are provided when replay attacks are detected. Information should be logged to your event database. You should regularly review the logs to collect information on instances where replay attacks occur. Integration with event monitoring and alert systems will speed the response to these attacks.

- You can limit brute force and replay attacks by adopting and implementing appropriate corporate policies to limit the number of login attempts.

- You have PIN lockout policies, and set them to lock out users after three unsuccessful attempts.

Supporting Your Users

It is important to have well defined policies around help desk procedures for your SAE deployment. 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

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.

- Tell your users what information requests to expect from Help Desk administrators.

- Always log out of applications when you are 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. 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 admins should never ask for token serial numbers, tokencodes, PINs, passwords, and so on.

• The Help Desk telephone number should be 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.

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