SECTOR Network
Secure Business App Ecosystem

RSA Ready Implementation Guide for RSA SecurID

Last Modified: December 5, 2014

Partner Information

Product Information	
Partner Name	SECTOR Network
Web Site	**https://sector.openpeak.com**
Product Name	SECTOR Network Secure Business App Ecosystem
Version & Platform	iOS and Android
Product Description	The SECTOR Network is a secure business app ecosystem endorsed by leading service providers worldwide, allowing mobile users to securely access business content. SECTOR Network apps are managed, secured and accessed within SECTOR-based enterprise secure mobile work-spaces. Secure mobile workspaces are virtual containers that separate "work" and "personal" data on employee owned devices enabling corporate data security while maintaining individual employee privacy. Enterprise mobile management solutions participating in the SECTOR Network include: AT&T Toggle®, BlackBerry® Secure Work Space, and Deutsche Telekom SAMBA!

SECTOR® Network
Secure Enterprise Apps

Solution Summary

RSA SecurID customers can use enterprise secure mobile workspaces participating in the SECTOR Network to enable their employees' iOS and Android devices to become RSA SecurID tokens, so employees no longer need to carry a separate hardware token.

Once a business user has installed the RSA SecurID app by downloading it from Google Play or the Apple App Store, they will need to separately import a software token. RSA SecurID customers can securely provide this seed token through enterprise secure mobile workspaces participating in the SECTOR Network.

Functional Description	
Authenticator provides its own GUI to present tokencode	N/A
Authenticator can securely store token seed record	N/A
Authenticator supports copy/paste of tokencode	N/A
Authenticator supports multiple seed records	N/A
Authenticator supports passphrase protection of application	N/A
Authenticator provides RSA Software Token Automation (user enters only PIN to authenticate)	N/A
Partner product provisions Authenticator (creates account, assigns token, delivers seed to device)	Yes
Authenticator supports CT-KIP provisioning protocol	No

Partner Product Configuration

Before You Begin

This document contains instructions for provisioning an RSA SecurID software token seed record to the user through a secure email message for enterprises using SECTOR Network-based workspaces such as AT&T Toggle, BlackBerry Secure Work Space and Deutsche Telekom SAMBA!

Procedure Overview

You should have working knowledge of the SECTOR-based secure mobile workspace, RSA Authentication Manager and RSA software tokens as well as access to the appropriate administrative documentation. Ensure that the SECTOR-based workspace solution and RSA Authentication Manager are running properly prior to configuring the integration. This document is not intended to suggest optimal installations or configurations.

The RSA SecurID app contains an embedded authenticator that can generate and display a 6-digit or 8-digit tokencode at 30 or 60-second intervals. In order to initialize a user's authenticator, **you must provision an RSA SecurID software token seed record to the user through a secure email message**, and the user must import the seed record into the application.

This process consists of the following sequence of events:

- An administrator configures an RSA Application Policy in the RSA Security Console. The policy includes the email address of an RSA Authentication Manager administrator who is responsible for assigning and delivering software token seed records.
- An administrator configures an RSA Application Policy in the IT Admin Portal of the SECTOR-based enterprise secure mobile workspace solution. This policy sets permissions to allow the authorized token seed record within the secure workspace to communicate with the RSA SecurID app.
- The RSA administrator assigns a software token to the user, binds it to the user's device ID and emails its seed record to the user in an *SDTID* file or a Compressed Token Format (CTF) URL.
- The user installs the RSA SecurID app on his/her mobile device, and then opens the email in the SECTOR-based enterprise workspace (i.e. AT&T Toggle, BlackBerry Secure Work Space or Deutsche Telekom SAMBA!) to import the seed record and instantiate the RSA SecurID authenticator.

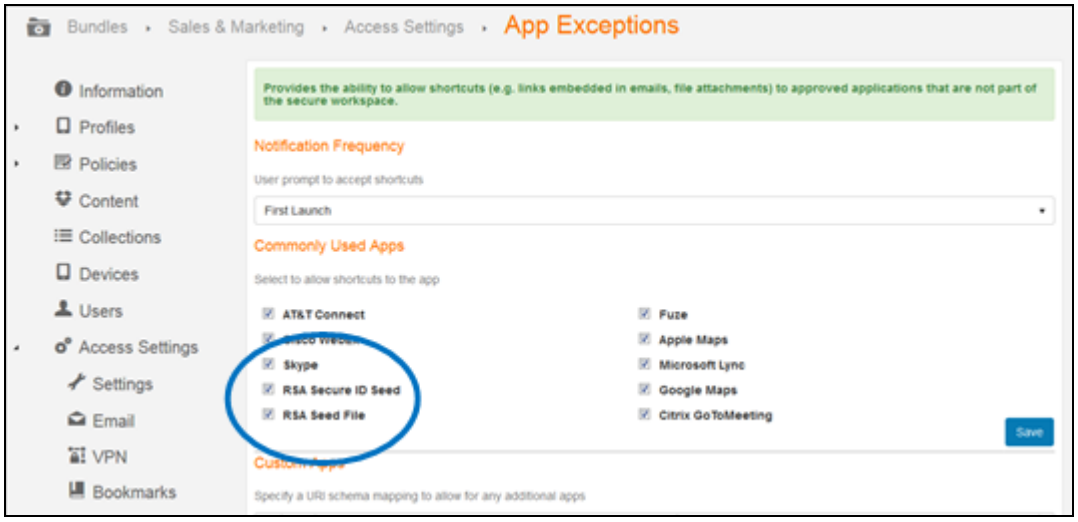
Product Configuration

This section provides directions for configuring an RSA Application Policy in the IT Admin Portal of the SECTOR-based secure mobile workspace solution. It is intended for IT administrators.

Configuring an RSA Application Policy in the IT Admin Portal

The application policy authorizes direct access to approved applications that are not part of the secure mobile workspace. These 'shortcuts' are handled as app exceptions. Selecting the RSA Secure ID Seed and RSA Seed File as an app exception, will permit the authorized token seed record within the secure workspace to communicate with the RSA SecurID app located outside of the secure workspace.

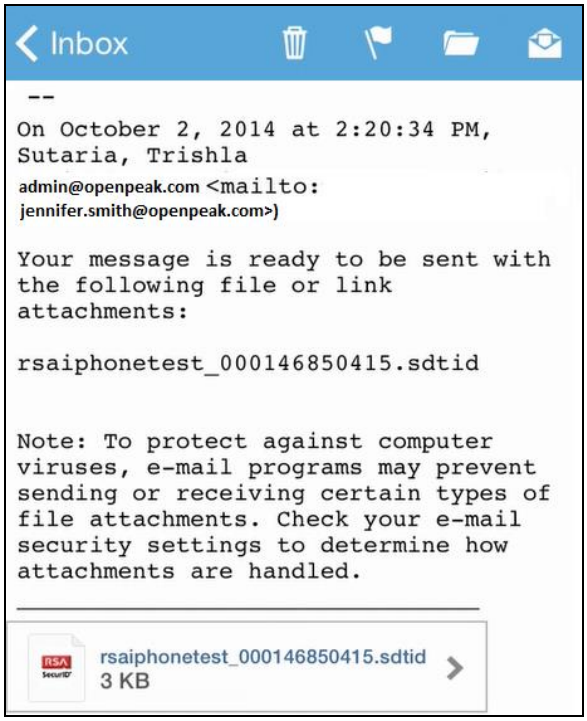
1. Log in to the IT Admin Portal of your SECTOR-based secure mobile workspace solution and navigate **Bundles > Access Settings > App Exceptions**.
2. Select the **Notification Frequency** from the drop-down list – First Launch, Every Launch, or Every 30 Days.
3. Under Commonly Used Apps, mark the checkbox for both RSA Secure ID Seed and RSA Seed File to allow authorized access.
4. Click **Save**.



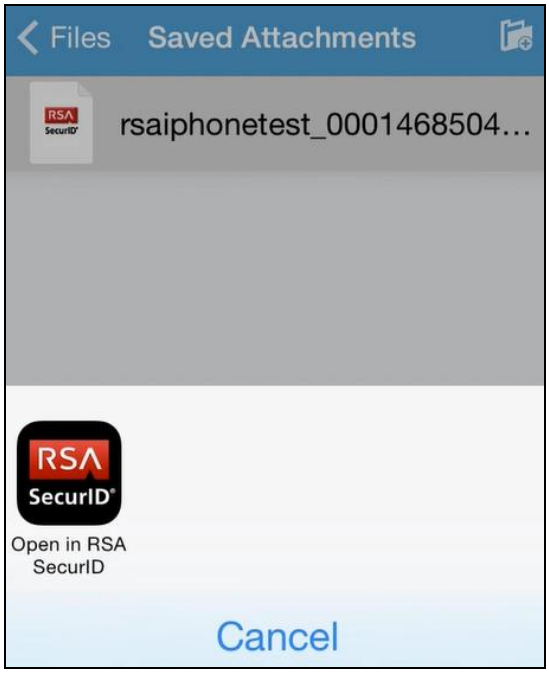
Note: The above screen illustrates a typical IT Admin user interface but may vary slightly across enterprise mobile management solutions participating in the SECTOR Network. Please check with your enterprise mobility management solution provider for additional information.

Importing a RSA SecurID Software Token

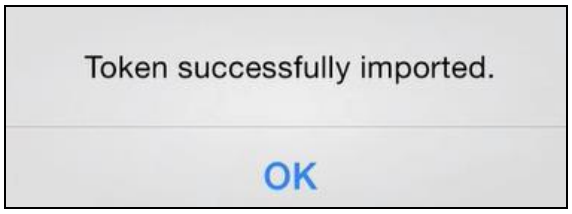
1. On the device you wish to import the token, open your email and save the .sdtid attachment:



2. Browse to your saved attachments and choose the **Open in RSA SecurID** dialog:



3. The RSA SecurID software token application will launch on the mobile device and import the token.
4. The **Token successfully imported** message will display.



5. Your software token is now ready to generate RSA SecurID Passcodes:

Certification Environment

Date Tested: December 5, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Software Token for iOS	2.0	iOS
RSA Software Token for Android	1.6	Android
SECTOR Network Secure Business App Ecosystem	1.0.14778.473 BES12 Client v12.0.1.140 24291_85	AT&T Toggle BlackBerry Secure Work Space Deutsche Telekom SAMBA!

RSA Ready Certification Criteria	
RSA Software Token Import	
Provision password-protected token	✓
Provision copy-protected token	✓
Provision PINPad token	✓
Provision FOB-Style token	✓
Provision PINless token	✓
Provision CTKIP token	N/A
Provision CTF token	✓
Provision File-based token	✓
RSA Software Token SDK or Embedded RSA OTP Algorithm ***	
Strong encryption of token database	✓
Copy protection of token database	✓
Proper display of current tokencode	✓
Interface to enter PIN	✓
Proper display of current PASSCODE	✓
Proper display of lifetime of current code (30/60 seconds)	✓
Successful removal of installed token(s)	✓
Successful re-provisioning of installed token(s)	✓
Proper display of token serial number	✓
Successful addition of token alias/nickname	✓
Successful rename/removal of token alias/nickname	✓
Passphrase protection of application or token	✓
Proper setting of default token	✓
Ability to copy/paste PASSCODE	✓
Successful authentication using partner device	N/A
Partner product displays RSA Ready logo	N/A

RSA Software Token Automation (Software Token API)	
Software Token API-enabled application can extract PASSCODE from Partner product	N/A
Successful authentication using Software Token API-enabled application	N/A
RSA Software Token Provisioning (RSA Authentication Manager Administrative API)	
Partner product provisions Authentication Manager username	N/A
Partner product provisions RSA Software Token assignment	N/A
Partner product provides delivery mechanism for Software Token (.SDTID)	N/A

GLS

✓ = Pass ✗ = Fail N/A = Non-Available Function

*** Using RSA Software Tokens for iOS or Android