



Secured by RSA Implementation Guide for SecurID Authenticators

Last Modified: November 2, 2012

Partner Information

Product Information	
Partner Name	Keynectis-OpenTrust
Web Site	www.opentrust.com
Product Name	SCM
Version & Platform	4.5
Product Description	Keynectis-OpenTrust's SCM is an all-inclusive life cycle management solution for digital credentials of users, devices and applications held on smart cards and tokens.
Product Category	Authenticator Management



OpenTrust has joined Keynectis

Solution Summary

Keynectis-OpenTrust SCM Administrator provides the IT Security and Administrative teams with an easy to use interface to manage the lifecycle of the RSA SID800.

Partner Integration Overview	
Interoperable through RSA Authentication Client	Yes
Pre-Boot Authentication	No
If Pre-Boot, which tokens are supported?	SID800 Rev D

Product Configuration for Interoperability

Interoperability between the RSA Authenticators and Keynectis-OpenTrust requires the installation of the RSA Authentication Client and Keynectis-OpenTrust.

Before You Begin

This section provides instructions for integrating RSA Authenticators with Keynectis-OpenTrust SCM. The document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

1. Login to the SCM Administrator and import the RSA SID800 PUK into the SCM to assign a Card Management Profile.

The screenshot displays the Keynectis-OpenTrust SCM Administrator interface. The top navigation bar includes the Keynectis-OpenTrust logo and the OpenTrust CMS logo. The main content area is titled 'Add Trusted Serial Numbers' and contains the following elements:

- Enrollment Menu:** A sidebar menu with options for 'Add Trusted Serial Numbers', 'Manage Trusted Serial Numbers', and 'Other Tasks'.
- Informational Message:** A yellow box with an information icon stating: 'Card serial numbers must be added to the trusted list before cards can be self-enrolled. Upload a CSV file containing serial numbers to be added to the trusted list. The CSV file must contain one serial number per line.'
- Upload File Section:** A form with radio buttons for 'Local Path' and 'URL', each followed by a text input field and a 'Browse...' button. Below these is an 'Upload File' button.
- Serial Number Selection:** A yellow box with an information icon stating: 'Choose a serial number to be added to the trusted list'.
- Form Fields:** A 'Trusted serial number' text input field, a 'Card Management Profile' dropdown menu (currently set to 'RSA SID 800 Self-enrollment'), and an 'OK' button.

- Use the default SCM settings for an RSA SID800 Self Enrollment.

General		Enrollment	Update	Unlock	Recovery	Revocation	OTP	Other Tasks	
Name	rsa_selfenrollment								
Description	rsa_selfenrollment								
Title	Default RSA SID 800 Self-enrollment							Add More	
Card Enrollment or Migration	Enabled								
Card Vendor Profile	rsa_sid800 (RSA SID 800)								
Applications	Public Key Infrastructures								
	<input type="checkbox"/>	pki_test_auth (OpenTrust PKI)							
	<input checked="" type="checkbox"/>	RSA Authentication 2048 (OpenTrust PKI)						Rank 2	
		Renewal Period (in days) 5,000							
		Keep application data on smart cards on renewal <input type="checkbox"/>							
	<input checked="" type="checkbox"/>	RSA Encipherment 2048 (OpenTrust PKI)						Rank 3	
	Number of keypairs to recover on enrollment 0								
	Renewal Period (in days) 5,000								
	Keep application data on smart cards on renewal <input type="checkbox"/>								
	CA Certificates								
<input checked="" type="checkbox"/>	OpenTrust PKI Test Bundle (Certification Authorities Bundle)						Rank 1		
PIN Policy	simple_pin_policy (simple_pin_policy)								
Security Question Authentication Scheme	security_questions (LocalSecurityQuestions)								
Maximum number of card(s) per holder	10								
Language Identification Rules	en							Modify	
Zone Identification Rules	Configure Zone Identification Datasource Fields								

- Using the SCM Client, login as a SCM user to assign an RSA SID800 smart card.

Card 3534100384242833

Card Activation

i You are about to activate your smart card. The following steps will generate the elements that your card requires to function.

💡 Please enter your authentication credentials.

Authentication parameters

User Identifier

Password

[Continue](#) ➔

4. Provide answers to security questions.

The screenshot shows the 'Card Activation' page for card 3534100384242833. It features the Keynectis and OpenTrust logos at the top. Below the card number, there is a section titled 'Card Activation' with an information icon and text: 'You are about to activate your smart card. The following steps will generate the elements that your card requires to function.' Below this is a lightbulb icon and text: 'Please choose the questions and answers that will allow you to be authenticated by your Help Desk.' The main area is titled 'Choice of questions / Enter answers' and contains two dropdown menus. The first dropdown is 'What is your favorite film?' and the second is 'What are the last four digits of your car serial number?'. To the right of each dropdown is a text input field. At the bottom of this section are 'Back' and 'Continue' buttons.

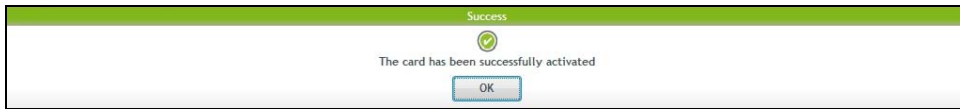
5. Set the PIN and provide the PIN confirmation in SCM for the RSA SID800 smart card.

The screenshot shows the 'Card Activation' page for card 3534100384242833. It features the Keynectis and OpenTrust logos at the top. Below the card number, there is a section titled 'Card Activation' with an information icon and text: 'You are about to activate your smart card. The following steps will generate the elements that your card requires to function.' Below this is a lightbulb icon and text: 'Please choose a new PIN according to the following rules:'. The rules listed are: 'Minimum Length: 4', 'Maximum Length: 4', 'Minimum Number of Unique Characters: 1', and 'Alphanumeric and symbols characters allowed'. Below the rules is another information icon and text: 'Once this step validated, the activation of your card may take up to several minutes, please wait.' The main area is titled 'Choice of PIN' and contains two text input fields. The first is labeled 'PIN' and the second is labeled 'PIN confirmation'. Both fields contain four asterisks. At the bottom of this section are 'Back' and 'Continue' buttons.

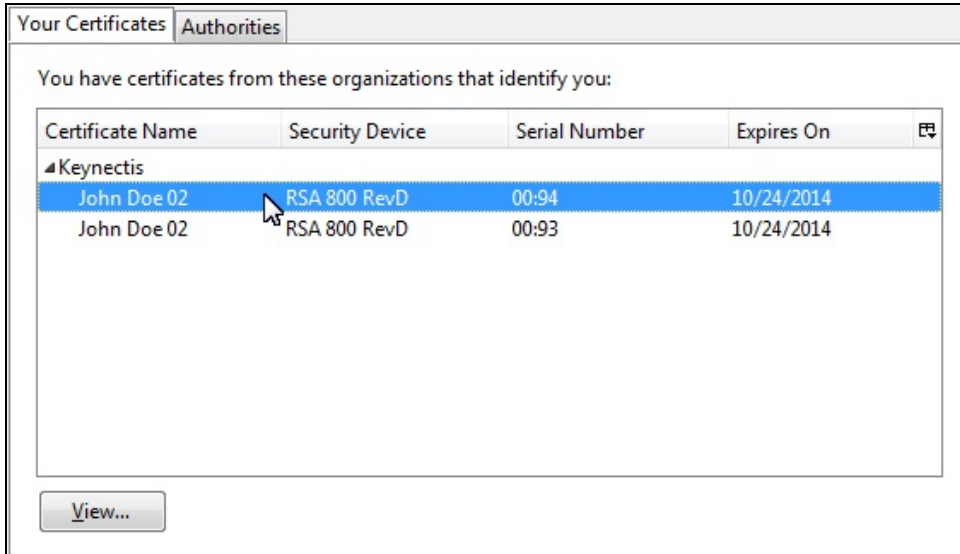
6. Allow the SCM Client to initialize the RSA SID800 smart card.

The screenshot shows the 'Card Activation' page for card 3534100384242833. It features the Keynectis and OpenTrust logos at the top. Below the card number, there is a section titled 'Card Activation' with an information icon and text: 'You are about to activate your smart card. The following steps will generate the elements that your card requires to function.' Below this is a lightbulb icon and text: 'Please choose a new PIN according to the following rules:'. The rules listed are: 'Minimum Length: 4', 'Maximum Length: 4', 'Minimum Number of Unique Characters: 1', and 'Alphanumeric and symbols characters allowed'. Below the rules is another information icon and text: 'Once this step validated, the activation of your card may take up to several minutes, please wait.' The main area is titled 'Operation in progress' and contains a progress bar. Below the progress bar is a text input field labeled 'Initializing card...'. Below this is a section titled 'Choice of PIN' and contains two text input fields. The first is labeled 'PIN' and the second is labeled 'PIN confirmation'. Both fields contain four asterisks. At the bottom of this section are 'Back' and 'Continue' buttons.

7. The SCM Client will prompt the user when the RSA SID800 smart card provisioning is complete.



8. The RSA SID800 smart card is now provisioned with the PKI Certificates.



Certification Checklist for 3rd Party Applications

Date Tested: November 2, 2012

Product	Operating System	Tested Version
RSA Authentication Client	Windows 7 SP1	3.5.5
Keynectis-OpenTrust SCM Client	Windows 7 SP1	4.5
Keynectis-OpenTrust PKI	RHEL 6	4.7.4
RSA SecurID 800 Revision D		3.7

Test Cases	Symmetric Keys	Asymmetric Keys
RSA SecurID 800		
Preboot Authentication	N/A	N/A
Disk/File Encryption	N/A	N/A
1024 Certificate	N/A	✓
2048 Certificate	N/A	✓
Write Key/Certificate	N/A	✓
Delete Key/Certificate	N/A	✓
Token Management		
RAC API		
Modify Token PIN		✓
Verify Token PIN		✓
Initialize Token		✓

DRP/PAR

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