Keynectis-OpenTrust

SCM

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 KEYNECTIS

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.

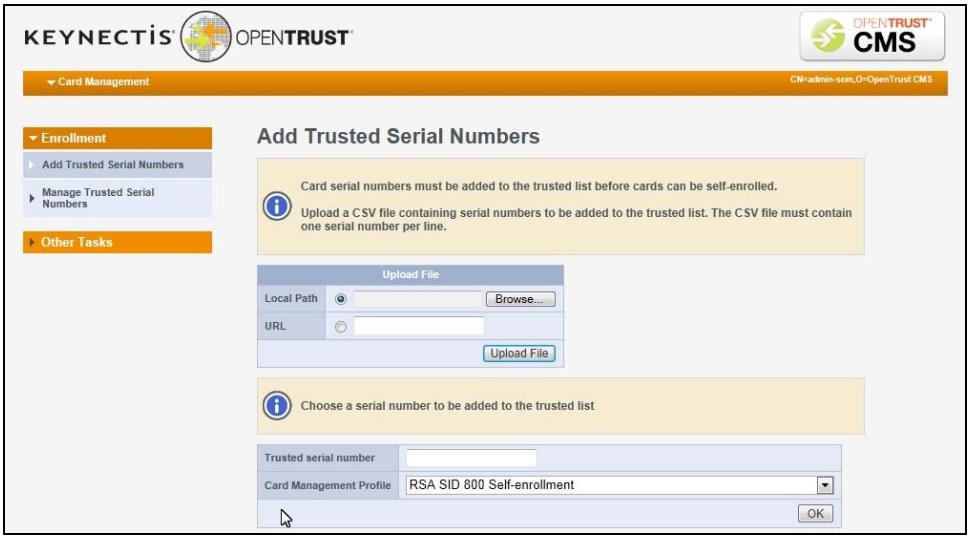
Before You Begin

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

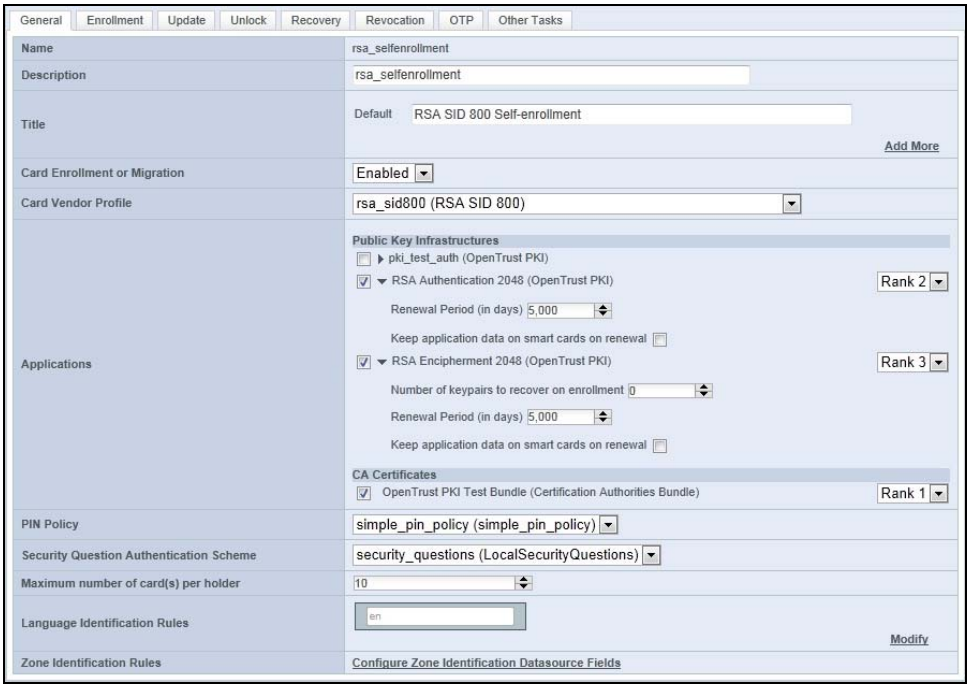
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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.

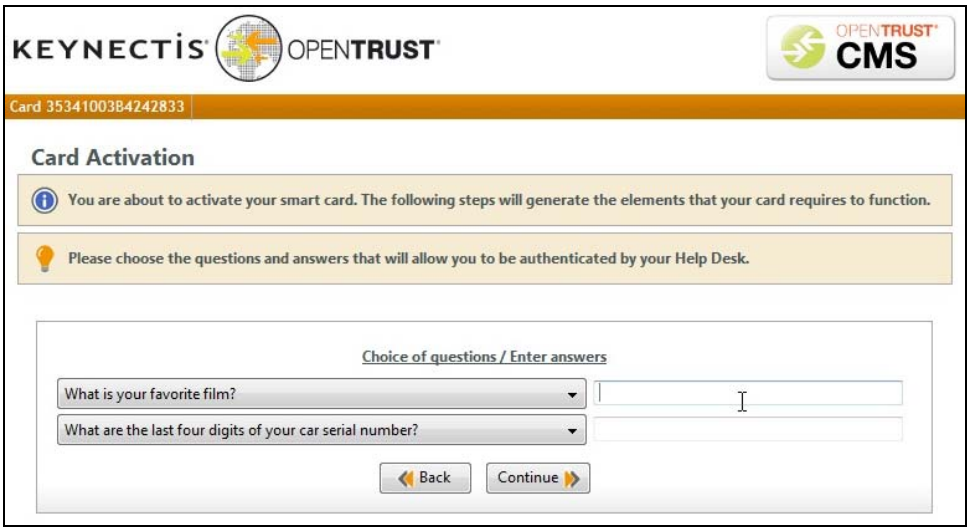


2. Use the default SCM settings for an RSA SID800 Self Enrollment.

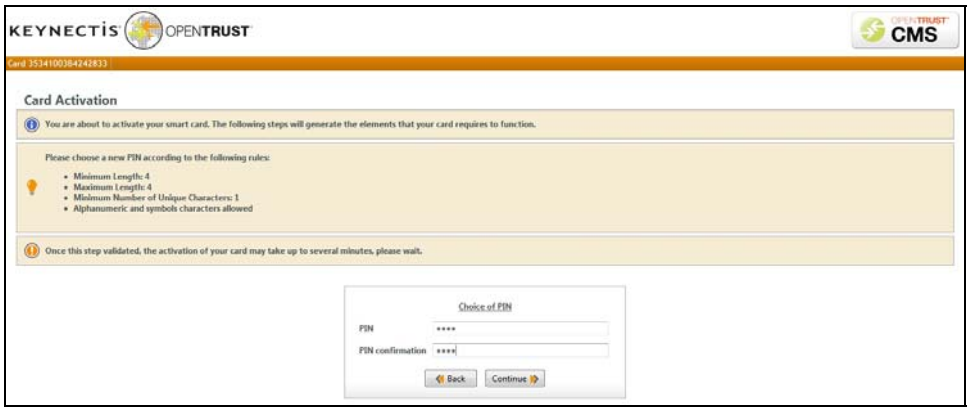


3. Using the SCM Client, login as a SCM user to assign an RSA SID800 smart card.

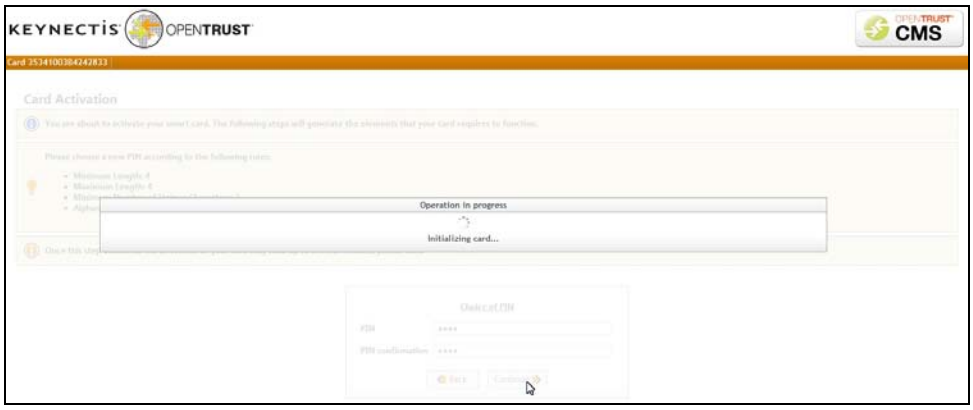
4. Provide answers to security questions.



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

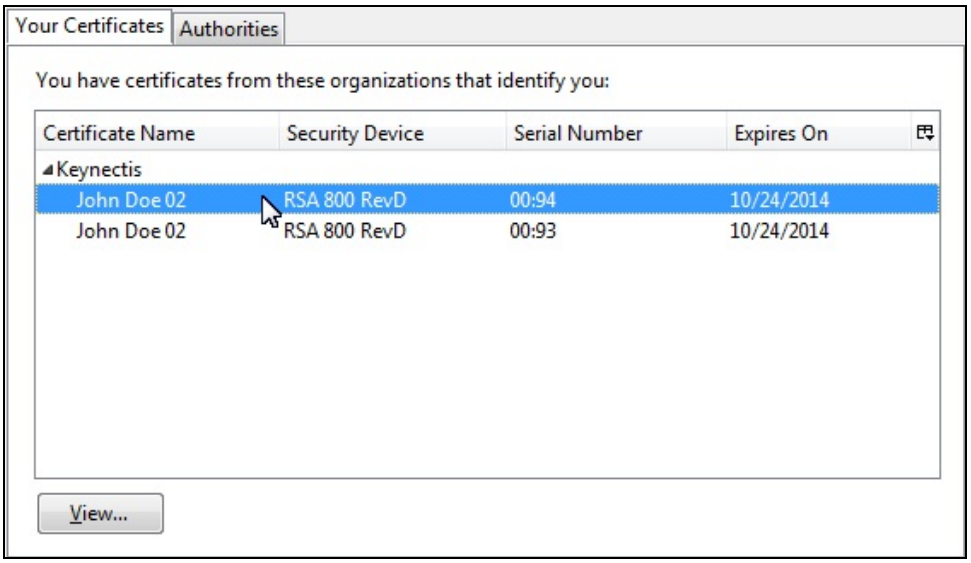


6. Allow the SCM Client to initialize the RSA SID800 smart card.



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