



RSA SecurID Ready Implementation Guide

Last Modified: November 1st, 2012

Partner Information

Product Information	
Partner Name	Infosys Limited
Web Site	www.infosys.com
Product Name	Finacle e-Banking
Version & Platform	11.0
Product Description	Finacle consumer e-Banking solution is a proven Internet and mobile solution for retail banking customers. Built on new-generation technology, it provides a single unified view ... of the customer's many relationships with the bank. The solution provides high flexibility for customization and robust security features.

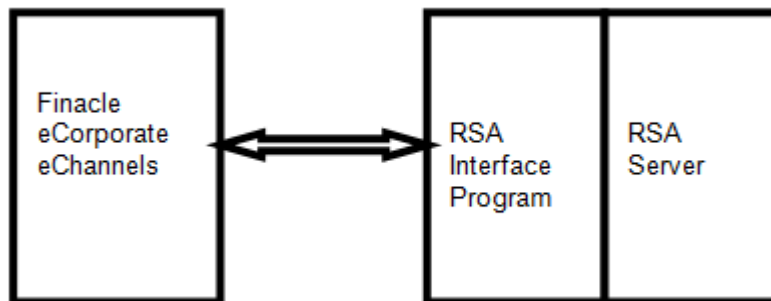


Solution Summary

In the Finacle eCorporate Channel when a corporate user makes a financial transaction, a user is authenticated using RSA SecurID. When the user makes a transaction, the e-Banking application will send a request to the RSA Authentication Manager server. The RSA Interface processes the request, invoking the suitable API call(s) to the SecurID server and then sending back the result to the end user.

RSA SecurID replaces the one-factor transaction password, which is used by the user to perform a e-Banking transaction(s) within the application, and enhances the security using RSA's two-factor, SecurID authentication process.

RSA SecurID supported features	
Finacle e-Banking 11.0	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:


- Hostname
- IP Addresses for network interfaces

Set the Agent Type to “Standard Agent” when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with the Finacle e-Banking server will occur.

 **Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	%windir%\system32
Node Secret	%windir%\system32
sdstatus.12	%windir%\system32
sdopts.rec	N/A

 **Note: The appendix of this document contains more detailed information regarding these files.**

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Finacle e-Banking server with RSA SecurID Authentication. This 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 Finacle e-Banking components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Documenting the Solution

The BankAway application interacts with the SecurID server through a message based interface. The message base interface is a limo-based server, developed by Infosys. The limo server listens on particular port number for incoming messages and sends it to RSA Authentication Manager where the actual authentication takes place. It sends a status message whether authentication succeeded or failed based on the parameters it received back to the application. This interface called RSA Interface needs to be installed on the RSA Authentication Manager server.

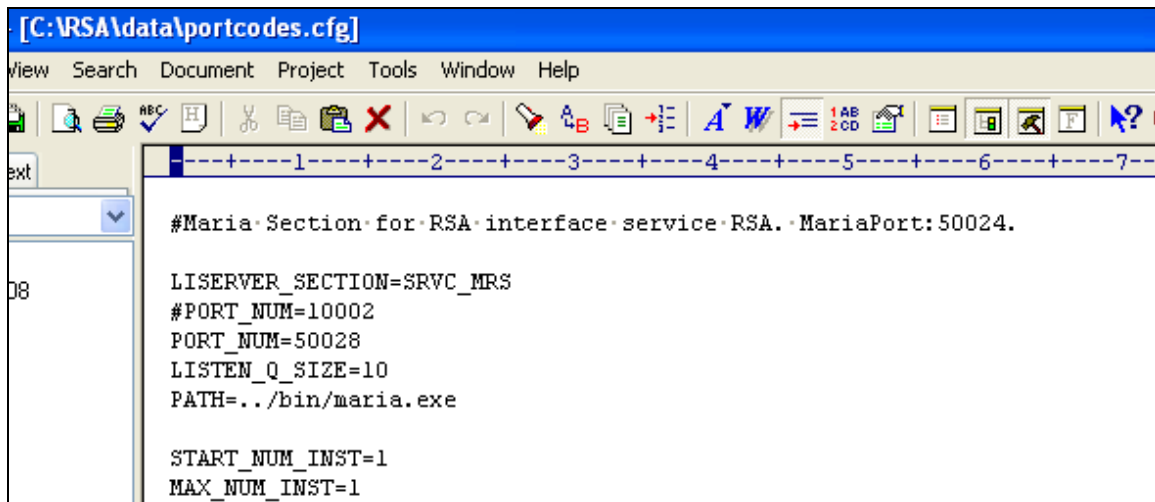
Installation of RSA Interface (Limo Service)

1. Copy the Infosys provided **RSA** folder (containing the RSA interface) to the RSA Authentication Manager server.
2. There are varies subdirectories within the **RSA** folder that was copied; including a '**bin**' folder containing the executables and a '**data**' folder containing the configuration files and log, scripts and work directories.
3. The following files shown below need to be copied from the respective UBS release and added in the bin folder above. For 681, it's has to be copied from UBS 10.1.X.

Name	Size	Type	Date Modified	Attrib
maria.exe	84 KB	Application	8/3/2008 2:39 PM	A
lisrvr.exe	52 KB	Application	8/3/2008 2:39 PM	A
limo.exe	48 KB	Application	8/3/2008 2:39 PM	A
arappmonitor.dll	32 KB	Application Extension	8/3/2008 2:38 PM	A
arlimoc.dll	128 KB	Application Extension	8/3/2008 2:38 PM	A
arbasic.dll	240 KB	Application Extension	8/3/2008 2:38 PM	A

4. In the RSA\data folder, open the **portcodes.cfg** file and edit the **PORT_NUM** variable (under the Maria section) to indicate what port the RSA Interface will listen on. This must be a port number that is not being used by any other application on the server.

5. Edit other parameters in the portcodes.cfg file like **MAX_NUM_INST**, **DUMP_RECV_BYTES=Y** according to your environment. The **START_NUM_INST** and **MAX_NUM_INST** should be 1 for both the Maria and LISERVER section. An example portcodes.cfg is shown below:



```
[C:\RSA\data\portcodes.cfg]
View Search Document Project Tools Window Help
#Maria Section for RSA interface service RSA. MariaPort:50024.
LISERVER_SECTION=SRVC_MRS
#PORT_NUM=10002
PORT_NUM=50028
LISTEN_Q_SIZE=10
PATH=../bin/maria.exe
START_NUM_INST=1
MAX_NUM_INST=1
```

6. Start the RSA Interface (Limo Service) by executing the **startRSA.bat** which exists in the RSA\bin folder.

Enabling BankAway Users for SecurID

From the Finacle application we can enable BankAway users for SecurID authentication. Once he/she is enabled for SecurID, whenever he/she performs a transaction, they will get an authentication screen where he/she will be asked to enter the SecurID passcode instead of a regular a password. This info will go to RSA Interface (Limo Service) and it sends the same info to the Interface program which communicates to the RSA Authentication Manager server using the RSA APIs.

In the Finacle e-Banking Database, the Database Administrator (DBA) must make the following changes to the PRPM table:

- Set the value of **SECURID_HOST** to the IP address of the machine where RSA is installed.
- Set the value of the **SECURID_PORT** to which the RSA Interface is listening to. This value can be obtained from the portcodes.cfg from the path RSA\data. The **PORT_NUM** under the Marie section will be the port on which it will be listening.

If the user is already created make sure the user has following values set:

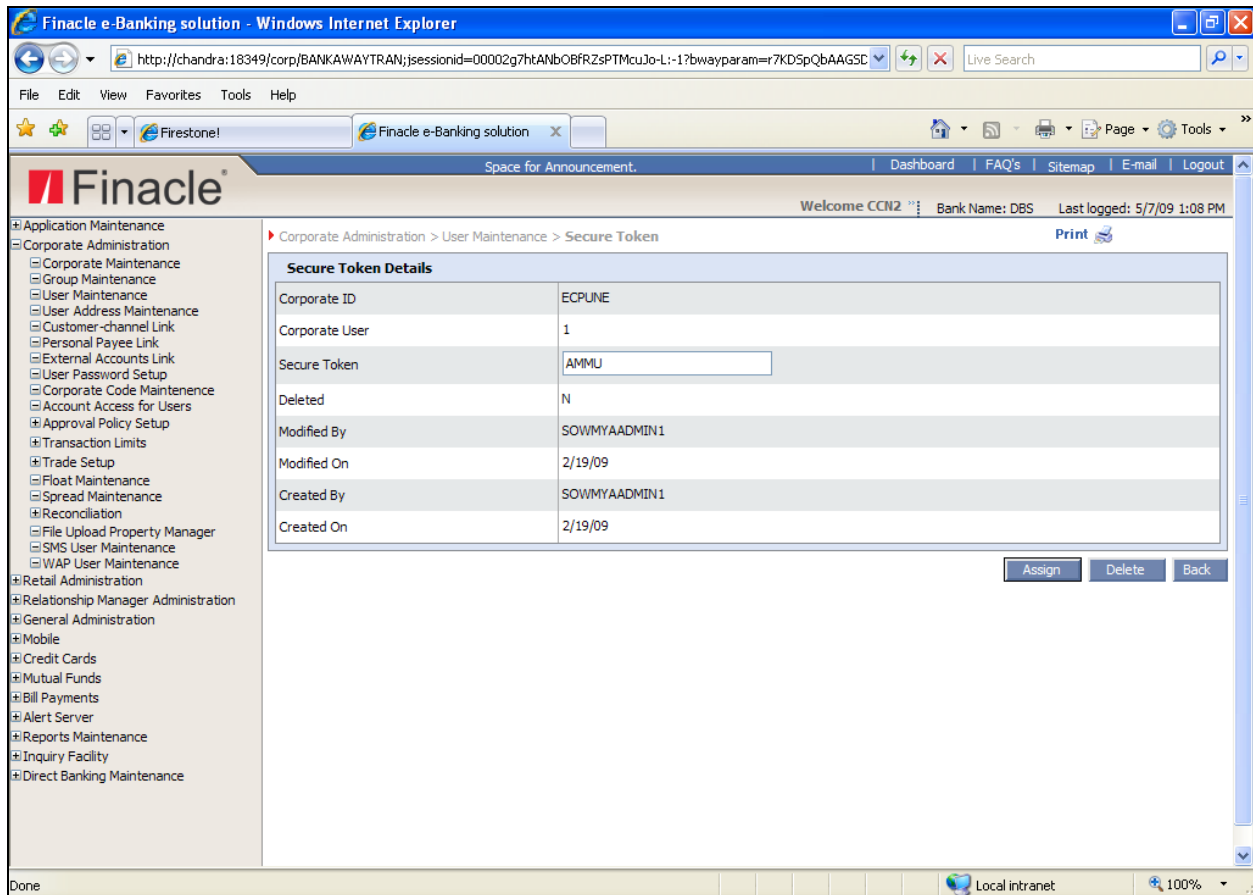
- Make sure the **authentication_mode** and **authorization_mode** have value **2(or SECD)**.
1. Login in to Finacle Administration and navigate to the **Corporate Administration → User Maintenance** for a corporate user or **Retail Administration → User Maintenance** for a retail user.
 2. Click on the **Retrieve** button.
 3. Select the user to whom SecurID should be enabled.

The screenshot shows the 'Corporate User List for "ecpune"' in the Finacle e-Banking solution. The table lists 10 users with their details and authentication status.

Sl. No.	User ID	User Name	Login Enabled?	Transaction Enabled?
1	1	Parul Rana	Y	Y
2	AKHIL	ФЛРЩД ФПФКЦФД	Y	Y
3	AKHILCORP10	akhil agarwal	Y	Y
4	AKHILCORP9	akhil ag	Y	Y
5	AKIAKICORP	aki ag	Y	Y
6	AKICORP111	akhil ag	Y	Y
7	AKICORP19	aki ag	Y	Y
8	AKIEC	aki aga	Y	Y
9	AKSHAY	sharathkbaa K B d	Y	Y
10	AMOL	AMOL MENDHI	Y	Y

Below the table, there are buttons for 'Create New', 'View/Update', 'Cust. ID', 'Division', 'Secure Token', 'SMS-based MobiToken', and 'Device-based MobiToken'. There are also buttons for 'Set Login Time Restrictions', 'Enable/Disable Menu', 'Enable/Disable User', 'Delete', 'Delete Multiple...', and 'Back'. The page number is 1 of 25.

- Click on the **Secure Token** button. The below screen is then displayed where you can edit the **Secure Token** field.



- In the **Secure Token** field, enter the username of the SecurID user you wish to enable. The username must match the same username which exists in the RSA Authentication Manager server.
- Click on the **Assign** button. The record will be sent for approval if the Maker Checker functionality is enabled. Approve it using the other Admin user.

7. For enabling the user for login, click on the **Enable/Disable User** button from the window in step 3.
8. Check the enable radio buttons for **Login Password**, **Transaction Password** and **Secure Token**.

The screenshot shows the 'Enable/Disable Corporate User' page in the Finacle e-Banking solution. The page is accessed via Internet Explorer and displays the following details:

- Corporate ID:** ecpune
- User ID:** USHACORP 1
- First Name:** usha
- Last Name:** corp
- Remarks:** (Empty text area)

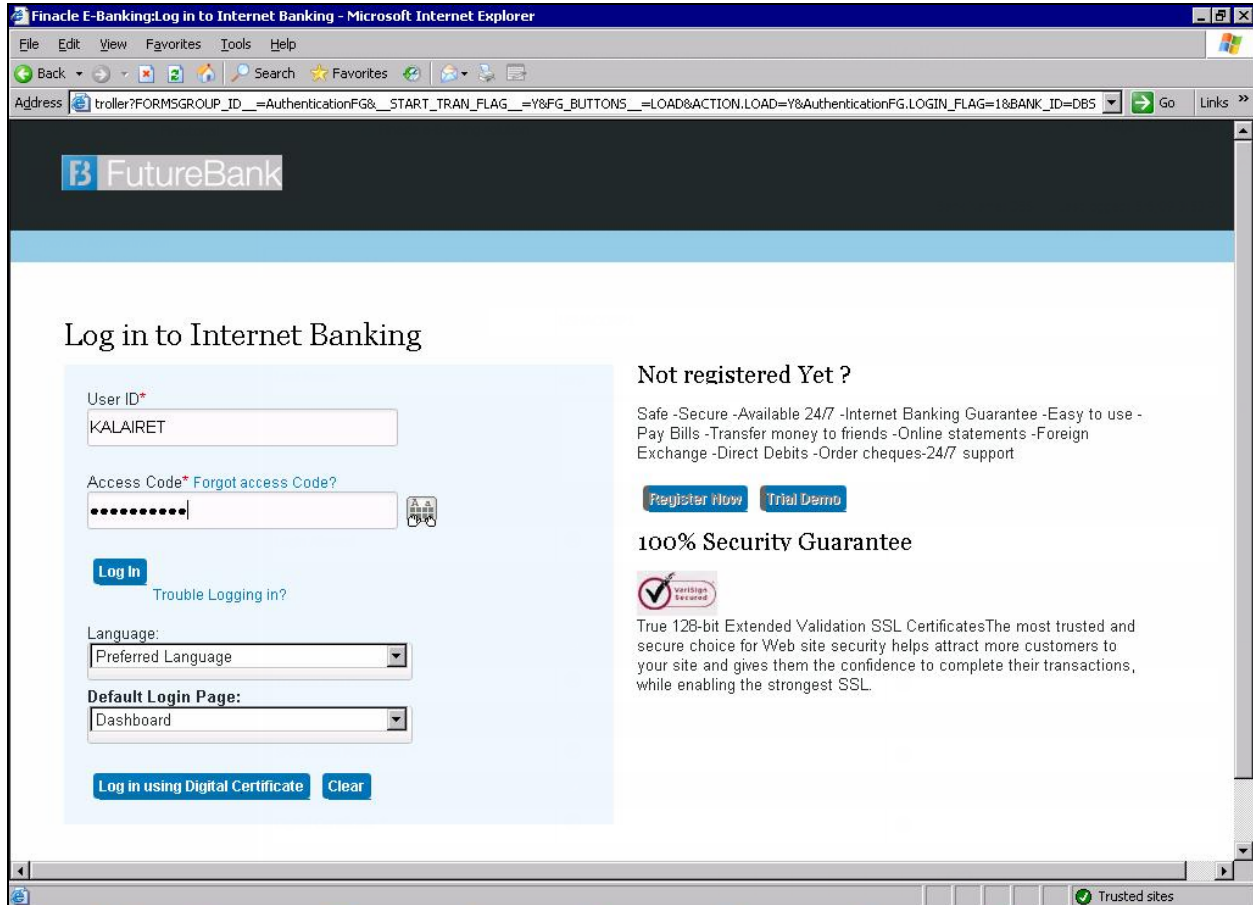
The configuration table below shows the status of various services:

	Yes	No
Login Allowed	<input checked="" type="radio"/>	<input type="radio"/>
Transaction Allowed	<input checked="" type="radio"/>	<input type="radio"/>

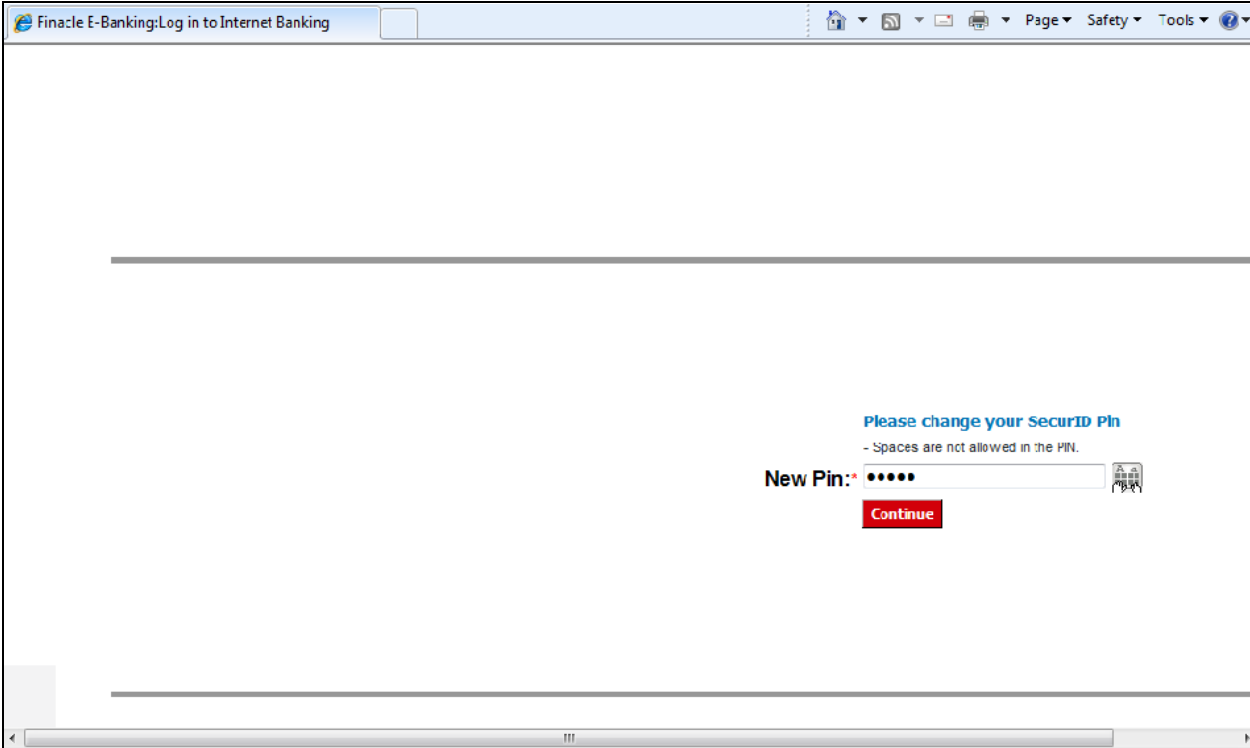
Mode	Enable	Disable
Login Password	<input checked="" type="radio"/>	<input type="radio"/>
Transaction Password	<input checked="" type="radio"/>	<input type="radio"/>
Secure Token *	<input checked="" type="radio"/>	<input type="radio"/>
SMS-based MobiToken *	<input type="radio"/>	<input checked="" type="radio"/>
Device-based MobiToken *	<input type="radio"/>	<input checked="" type="radio"/>
Digital Certificate *	<input type="radio"/>	<input checked="" type="radio"/>

Sample Login Screens

Login screen:



User-defined New PIN:



System-generated New PIN:

FutureBank

[FEBAU0023] [102908] Please use the pin 0Xd2D7 to proceed along with the token code

Log in to Internet Banking

User ID*
TXNRET3

Access Code* [Forgot access Code?](#)

Log In [Trouble Logging in?](#)

Language:
Preferred Language

Default Login Page:
Dashboard

Log in using Digital Certificate **Generate OTP** **Clear**

Not registered Yet ?

Safe -Secure -Available 24/7 -Internet Banking Guarantee -Easy to use -Pay Bills - Transfer money to friends -Online statements -Foreign Exchange -Direct Debits -Order cheques-24/7 support

Register Now **Trial Demo**

100% Security Guarantee

Yatitiga Secured

True 128-bit Extended Validation SSL CertificatesThe most trusted and secure choice for Web site security helps attract more customers to your site and gives them the confidence to complete their transactions, while enabling the strongest SSL.

Finacle e-banking Solutions is a Trademark of Infosys Limited, India, 2009
Best viewed in 1024 x 768 resolution

Local intranet | Protected Mode: Off | 100%

Certification Checklist for RSA Authentication Manager

Date Tested: October 23rd, 2012

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1 SP4	Microsoft Windows Server 2003
Finacle e-banking	11.0	Microsoft Windows Server 2003

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input type="checkbox"/> N/A
Deny PIN Reuse	<input checked="" type="checkbox"/>	Deny PIN Reuse	<input type="checkbox"/> N/A
Passcode			
16-Digit Passcode	<input checked="" type="checkbox"/>	16-Digit Passcode	<input type="checkbox"/> N/A
4-Digit Fixed Passcode	<input checked="" type="checkbox"/>	4-Digit Fixed Passcode	<input type="checkbox"/> N/A
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
On-Demand Authentication			
On-Demand Authentication	<input checked="" type="checkbox"/>	On-Demand Authentication	<input type="checkbox"/> N/A
On-Demand New PIN	<input checked="" type="checkbox"/>	On-Demand New PIN	<input type="checkbox"/> N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A

JJO / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Appendix

Partner Integration Details	
RSA SecurID API	8.1.1
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

API Details:

The Finacle e-Banking application uses the RSA SecurID Authentication SDK v8.1.1 for C.

Node Secret:

The node secret (securid) is created after a successful authentication. The file resides in the %windir%\system32 directory where the RSA Interface runs.

sdconf.rec:

The sdconf.rec file is copied to the %windir%\system32 directory where the RSA Interface runs.

Result of requests for authentication (New PIN, Next Tokencode, validation) is logged in the file RSAInterface.log and errors will be logged in RSAInterface.err, in the log folder.