

RSA Secured Implementation Guide

Last Modified: December 8, 2008

Partner Information

Product Information	
Partner Name	SECUDE
Web Site	www.secude.com
Product Name	SECUDE FinallySecure
Version & Platform	9.2.2
Product Description	FinallySecure provides total Data-at-Rest security with software- or hardware-based Full Disk Encryption. FinallySecure is the first link in the End-to-End authentication chain, providing an Adaptive Technology with Risk Management and Productivity gains for end-to-end security. This complete security umbrella protects against loss of data, fines from non-compliance, and destruction of brand value. In addition, end user transparency results in an ROI from productivity gains and FinallySecure allows for migration from single user to enterprise and software to hardware. Balancing focus on central management and end-user experience will allow your business to survive, adapt, and grow in a heterogeneous IT eco-system.
Product Category	Disk/File Encryption

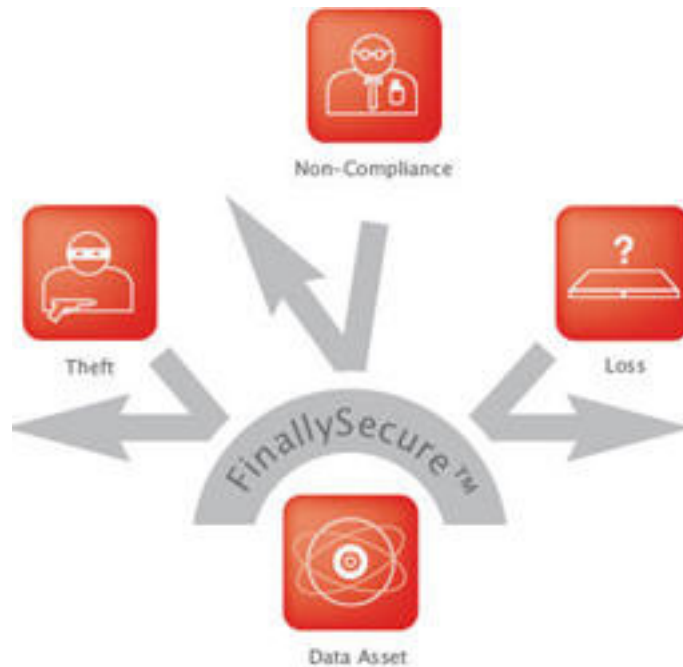




Solution Summary

RSA and Secude combine together to provide end-to-end protection using two factor authentication for pre-boot authentication and hard disk encryption. Users can store the keys necessary to unlock the encrypted data on their hard drive on the same device used to provide RSA SecurID authentication throughout the enterprise.

Partner Integration Overview	
Interoperable through RSA Authentication Client	Y
Pre-Boot Authentication	Y
If Pre-Boot, which tokens are supported?	SID800 v1 & v2
Supported Key type	Asymmetric





Product Configuration for Interoperability

Interoperability between the RSA Authenticators and SECUDE FinallySecure requires the installation of the RSA Authentication Client and FinallySecure.

Before You Begin

This section provides instructions for integrating the RSA Authenticator with SECUDE. 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.

RSA Authenticator Configuration

Before attempting the SECUDE FinallySecure installation, please ensure you have properly installed the correct RSA Authenticator client. Please consult the appropriate RSA documentation for client installation details.



Provision the RSA Authenticator

1. Upon completion of SECUDE FinallySecure open the Control Panel and the FinallySecure Enterprise. Select PBA Administration and login using the password set during the installation of FinallySecure.



2. Once logged into the FinallySecure application locate the Certificates tab and verify that the application is setup to use a similar key usage to the x.509 certificate provisioned on your token.





3. Locate the Smart card User tab and select the Self-initialization of first user enabled checkbox and reboot.



4. During the launch of the SECUDE pre-boot authentication the application will prompt the user for the SID800 token. Insert the token and when prompted enter the pin of the device to unlock the token. Once the token is unlocked the SID800 will allow SECUDE FinallySecure to access the key and unlock the pre-boot environment and boot the protected operating system.



Certification Checklist for 3rd Party Applications

Date Tested: December 8, 2008

Product	Operating System	Tested Version
RSA Authentication Client	Windows XP SP2	2.00
Secude FinallySecure	Windows XP SP2	9.2.2

Pre-boot Authentication	Result
SID800 (Combination Token)	✓
Symmetric Key	N/A
Asymmetric Key	✓
5200 (Smartcard w/SCR 331 reader)	N/A

DRP

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