MEK Software Technologies
SecurPBX

RSA SecurID Ready Implementation Guide

Last Modified: June 18, 2008

Partner Information

Product Information	
Partner Name	MEK Software Technologies Inc.
Web Site	**www.meksofttech.com**
Product Name	SecurPBX
Version & Platform	SecurPBX Version 4.2 for Windows 2000, 2003 or Windows XP
Product Description	RSA Secured® SecurPBX allows existing RSA SecurID token environments to offer token-based protection of long distance trunks, voice mail, maintenance ports, modem pools, conference bridging and IVR systems. SecurPBX functions as an RSA Authentication Agent. When placing a call to a protected telecom resource, users are asked to enter their SecurID® PIN and token code on the telephone keypad before being transferred.
Product Category	General Security Utilities

MEK Software Technologies Inc.

Solution Summary

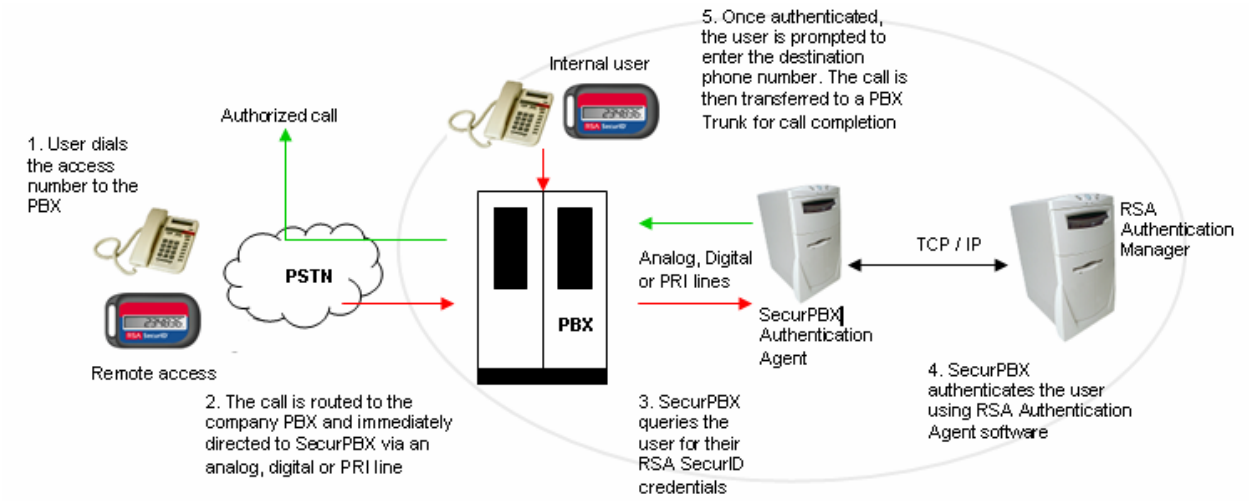
Millions of people use RSA SecurID tokens to securely access their organization's data network. A need was identified to extend the reach of the token to secure telecommunications resources.

The level of toll fraud theft is higher than ever. A 2003 survey by the Communications Fraud Control Association found that worldwide PBX and voice mail fraud now totals between 3.0 and 3.5 billion dollars a year.

To combat the growing allocation of resources towards telecom security, SecurPBX prevents, as opposed to detects, toll fraud and misuse, stopping unauthorized calls before they reach an organization's PBX.

Used in conjunction with RSA Authentication Manger and RSA SecurID token technology, SecurPBX allows existing RSA SecurID environments to offer token-based protection long distance lines, voice mail, maintenance ports, conference bridging, IVR systems and other custom functionality.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	6.0
RSA Authentication Manager Replica Support *	Full Replica Support
Secondary RADIUS Server Support	No
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	N/A



Product Requirements

Partner Product Requirements: SecurPBX	
CPU	Intel Pentium 4 or better, 2Ghz or better
Memory	Minimum 512MB
Storage	Hard Disk capacity 40GB or greater

Operating System	
Platform	**Required Patches**
Windows 2000	Service Pack 4 or greater
Windows 2003	Latest Service Pack
Windows XP	Service Pack 1, 2

Agent Host Configuration

To facilitate communication between the SecurPBX and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the SecurPBX within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the SecurPBX as Net OS. This setting is used by the RSA Authentication Manager to determine how communication with the SecurPBX will occur.

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

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	%WINDOWS_HOME%\system32
Node Secret	%WINDOWS_HOME%\system32
sdstatus.12	%WINDOWS_HOME%\system32
sdopts.rec	%WINDOWS_HOME%\system32

Go to the appendix of this document to get detailed information regarding these files.

Partner Product Configuration

Before You Begin

This section provides instructions for integrating the partners' product 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 vendor products/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 SecurPBX configuration requires the following on the SecurPBX Agent Host platform:

- Installation and test of the RSA Authentication Agent.
- Installation of the Telephony Board and associated telephony driver software.
- Installation of the MEK SecurPBX Configuration Manager.
- Installation of the MEK SecurPBX Application.
- Installation of the MEK SecurPBX Administrator Program.
- Provisioning of SecurPBX database, including configuration information and User's.

SecurPBX comes with a full documentation set containing step-by-step installation instructions.

The SecurPBX Administrator software must also be configured as it contains custom specifications. The SecurPBX Administrator software requires entry of the user population's Default Login and numeric User ID in order to authenticate users with the RSA Authentication Manager Server and to provide access to the specified resource. The Administrator sets group and individual settings to restrict user access to certain times, call types or other policies.

Certification Checklist For RSA Authentication Manager

Date Tested: June 18, 2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1.2	Windows 2003 Server R2
RSA Authentication Agent	6.1.1	Windows XP Professional
RSA Remote Authentication Client	6.1	Windows XP Professional
SecurPBX	4.2	Windows XP Professional

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
User Selectable	✓	User Selectable	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	N/A
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	N/A
4 Digit Password	✓	4 Digit Password	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
Name Locking Enabled	✓	Name Locking Enabled	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	N/A
Set Credential	N/A	Set Credential	N/A
Retrieve Credential	N/A	Retrieve Credential	N/A

BSD / PAR

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

Certification Checklist For RSA Authentication Manager 7.x

Date Tested: June 18, 2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows Server 2003 Enterprise
RSA Authentication Agent	6.1.1	Windows XP Professional
RSA Remote Authentication Client	6.1	Windows XP Professional
SecurPBX	4.2	Windows XP Professional

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	N/A
Deny Numeric PIN	✓	Deny Numeric PIN	N/A
PIN Reuse	✓	PIN Reuse	N/A
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	N/A
4 Digit Fixed Passcode	✓	4 Digit Fixed Passcode	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

BSD / PAR

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

Known Issues

1. Alphanumeric PINS are not supported as user input, as the telephony interface uses the telephones numeric keypad for entry, however System Generated Alphanumeric PINS are supported as these are “Spoken” by the SecurPBX.