

RSA SecurID Ready Implementation Guide

Last Modified: May 26, 2009

Partner Information

Product Information	
Partner Name	TESIS SYSware GmbH
Web Site	www.thesis.de/sysware
Product Name	TESIS ASPR
Version & Platform	3.5
Product Description	TESIS ASPR is a web-based application that provides a user self-service interface. The interface allows users to reset forgotten passwords on multiple systems. Among other options, the RSA SecurID authentication is one method for users to authenticate and perform a password reset using a token generated one-time password (OTP).
Product Category	Web Applications & ERP





Solution Summary

TESIS SYSware offers a portfolio that is focused on IT security and identity management, a portfolio that consists of products, solutions, consulting, and operations. We design business processes by using sustainable IT techniques that are cost effective, transparent and secure.

TESIS|ASPR (available in several languages) allows users to reset forgotten passwords on multiple systems utilizing a user self-service interface. IT users have to cope with many different passwords and PIN codes. Consequently, passwords are kept simple, static, mirrored on other systems, and are recorded and stored insecurely.

Password policies offering more complexity—such as password ageing and history—can enhance security, but they can also complicate the handling of passwords for the end-user. As a result passwords are often forgotten.

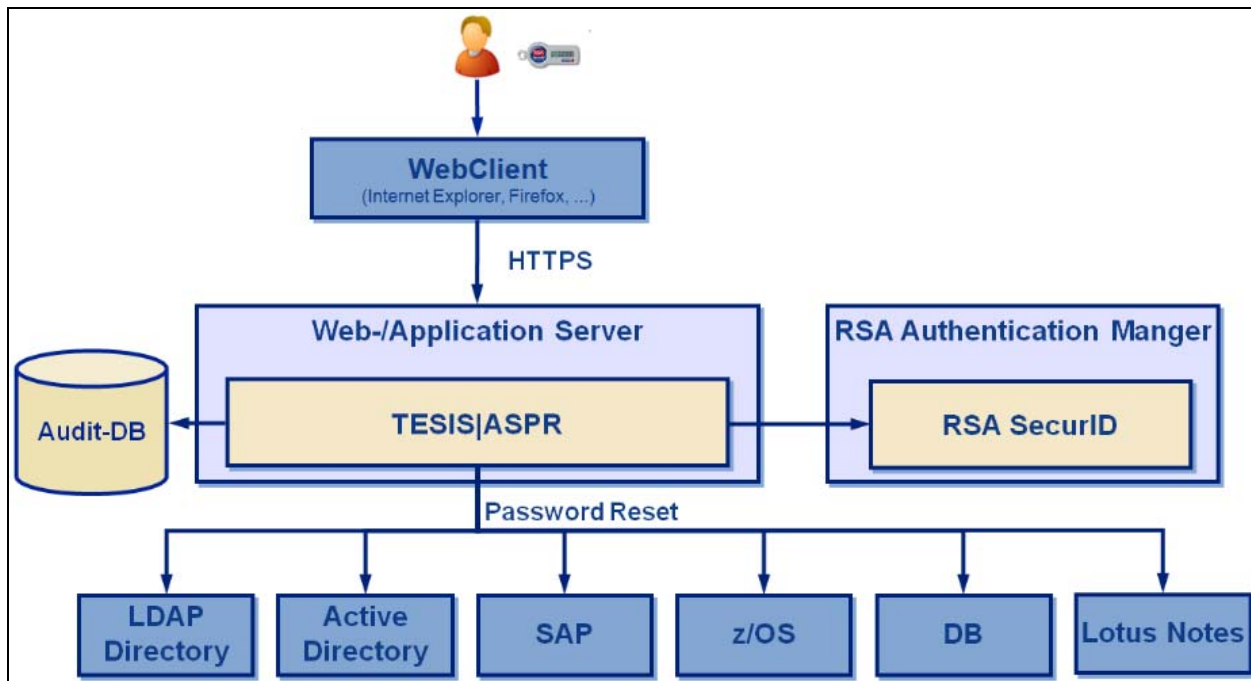
TESIS|ASPR allows users to reset their various passwords quickly, securely and independently.

TESIS|ASPR

- Utilizes a user self-service to reduce password reset requests to the help desk
- Expedites the password-reset process through a user-friendly web based application, allowing employees to quickly generate a new password without compromising work efficiency
- Eliminates request protocols and faxed authenticity procedures—and it's always available, working around limited help desk service hours
- Improves your IT security since the entire password reset process is protected from abuse

RSA SecurID authentication makes TESIS|ASPR even more flexible. In addition to other authentication methods such as: question/answer pairs, PKI/certificates, four-eye principle, or using an alternative password to suit different requirements and systems, RSA SecurID allows two-factor authentication.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
RSA SecurID Library Version Used	5.0.3_176 (Java)
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	No
RSA Authentication Agent Host Type for 6.1	Communication Server
RSA Authentication Agent Host Type for 7.1	Standard Agent
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No



Product Requirements

Partner Product Requirements: TESIS ASPR Server	
CPU	Single CPU
Memory	1 GB
Storage	40 GB

Operating System	
Platform	Required Patches
Windows 2003 Server or higher	All Patch Levels Supported
all UNIX Platforms	All Patch Levels Supported
Solaris 8 or higher	All Patch Levels Supported

Additional Software Requirements	
Application	Additional Patches
Sun Java Runtime Environment (JRE) 1.5.0	All Patch Levels Supported
Application/Webserver Apache Tomcat 5.5 or higher IIS BEA Weblogic 8.1 or higher Others supporting Servlet-Specification 2.3 and JSP-Specification 1.2	All Patch Levels Supported
Database Oracle 9i or higher MS SQL Server 2005 or higher MySQL 5.0 or higher Others supported by Hibernate 3.0	All Patch Levels Supported



Agent Host Configuration

! > Important: “Agent Host” and “Authentication Agent” are synonymous. “Agent Host” is a term used with the RSA Authentication Manager 6.x servers and below. RSA Authentication Manager 7.1 uses the term “Authentication Agent”.

! > Important: All “Authentication Agent” types for 7.1 should be set to “Standard Agent”.

To facilitate communication between the TESIS|ASPR 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 TESIS|ASPR 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

Before adding the agent host record, you should set TESIS|ASPR as the Communication Server. This will allow the RSA Authentication Manager to determine how the communication with TESIS|ASPR will occur

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must point 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	Path which is configured in rsa_api.properties
Node Secret	Path which is configured in rsa_api.properties
sdstatus.12	Path which is configured in rsa_api.properties
sdopts.rec	Path which is configured in rsa_api.properties



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

Integration of RSA Authentication Service in TESIS|ASPR

The library `authapi.lib` must be registered in the application server classpath. On the file system of the application server, the files `rsa_api.properties` and `sdconf.rec` must be stored in a directory that the application server has write access to.

TESIS|ASPR's configuration contains a section to add other authentication methods. To add RSA SecurID, place the following configuration into this section.

```
<object name="auth-securi d"
  class="de. tesi s. aspr. auth. securi d. Securi dAuthServi ce">
  <param name="i d"
    val ue="auth-securi d"/>
  <param name="rsa-properti es-path"
    val ue="C: \\RSAsecurID\\rsa_ api . properti es"/>
  <param name="max-rsa-user-sessi on-time"
    val ue="250"/>
</obj ect>
```

The path to `rsa_api.properties` must match the path where the properties file is stored on the file system of the application server.

After successfully configuring RSA SecurID, the service will be available to all users and will allow them to perform a password reset on the target systems that contain their accounts.



Perform password reset with RSA Authentication in User Self Service

Step 1: Enter UserID

ASPR.
Perform reset: Step 1.

Enter user ID System Selection Method Selection Authorization Summary Result

Please enter the user ID to be reset

User ID
Example: MaxUser, MrModel, ...

Step 2: Select the target system for the password reset

ASPR.
Perform reset: Step 2.

Enter user ID System Selection Method Selection Authorization Summary Result

Summary of the reset data

For the user Peter Wright (TESIS SYSware)
a password reset should be performed.

Please select the target system for which the reset is to be performed.

peterwright Active Directory Services

Step 3: Select the authorization method for the password reset

ASPR.
Perform reset: Step 3.

Enter user ID System Selection Method Selection Authorization Summary Result

Summary of the reset data

For the user Peter Wright (TESIS SYSware)
on the target system Active Directory Services (peterwright)
a password reset should be performed.

Please select the method by which the password reset is to be authorized.

Self-authorization (User authorizes password reset for his own account)
 Authorization using of the four-eyes principle



Step 4: Authenticate with RSA SecurID

ASPR.
Perform reset: Step 4.

Enter user ID | System Selection | Method Selection | **Autho-
rization** | Summary | Result

Summary of the reset data

For the user	Peter Wright (TESIS SYSware)
on the target system	Active Directory Services (peterwright)
with the authorization method	Self-authorization

a password reset should be performed.

Please enter the requested authentication information.

RSA SecurID | SAP Test System | Security Question

User ID (SecurID)	peterwright
Passcode (PIN+tokencode)	*****

Back | Cancel | Next

The user will be prompted if the token is no longer valid. If the token is invalid, the user will need to enter the next token code.

ASPR.
Perform reset: Step 4.

Enter user ID | System Selection | Method Selection | **Autho-
rization** | Summary | Result

Information
You now have to enter the next displayed tokencode.

Summary of the reset data

For the user	Peter Wright (TESIS SYSware)
on the target system	Active Directory Services (peterwright)
with the authorization method	Self-authorization

a password reset should be performed.

Please enter the requested authentication information.

RSA SecurID | SAP Test System | Security Question

User ID (SecurID)	peterwright
Passcode (PIN+tokencode)	*****
Please enter the next tokencode	

Back | Cancel | Next

Users can enter a new PIN code themselves if it has to be changed.



ASPR.
Perform reset: Step 4.

1 Enter user ID 2 System Selection 3 Method Selection **4 Authorization** 5 Summary 6 Result

Information
Please enter a new PIN (4 - 6 numbers).

Summary of the reset data
For the user **Peter Wright (TESIS SYSware)**
on the target system **Active Directory Services (peterwright)**
with the authorization method **Self-authorization**
a password reset should be performed.

Please enter the requested authentication information.

RSA SecurID SAP Test System Security Question

User ID (SecurID) **peterwright**
Please enter a new PIN:

If the new PIN code is accepted by the system, then the user must re-authenticate using the new PIN and the next token code.

ASPR.
Perform reset: Step 4.

1 Enter user ID 2 System Selection 3 Method Selection **4 Authorization** 5 Summary 6 Result

Information
The new PIN has been accepted. Please re-authenticate with new PIN and next displayed tokencode.

Summary of the reset data
For the user **Peter Wright (TESIS SYSware)**
on the target system **Active Directory Services (peterwright)**
with the authorization method **Self-authorization**
a password reset should be performed.

Please enter the requested authentication information.

RSA SecurID SAP Test System Security Question

User ID (SecurID) **peterwright**
Passcode (PIN+tokencode)

In all other cases, the RSA server will generate a new PIN. TESIS|ASPR will then display the newly generated PIN code.



ASPR.
Perform reset: Step 4.

1 Enter user ID 2 System Selection 3 Method Selection 4 **Authorization** 5 Summary 6 Result

Information
The system has assigned you a new PIN. Please memorize the new PIN: 8888

Summary of the reset data
For the user **Peter Wright (TESIS SYSware)**
on the target system **Active Directory Services (peterwright)**
with the authorization method **Self-authorization**
a password reset should be performed.

Please enter the requested authentication information.

RSA SecurID SAP Test System Security Question

User ID (SecurID) **peterwright**
Please enter a new PIN:

Back Cancel Next

Step 5: Overview and optional comment for the password reset

ASPR.
Perform reset: Step 5.

1 Enter user ID 2 System Selection 3 Method Selection 4 Authorization 5 **Summary** 6 Result

Summary of the reset data
For the user **Peter Wright (TESIS SYSware)**
on the target system **Active Directory Services(peterwright)**
with the authorization method **Self-authorization**
a password reset should be performed.

Please store a comment for this password reset.

Comment:

Back Cancel Next



Step 6: Result and initial password on the target system

The authentication process is completed and the new password, assigned by TESIS|ASPR on the target system, is displayed to the user. The user and—if necessary—the user’s manager are notified about the password reset by email. NOTE: The new password is not included in the email.

ASPR.
Perform reset: Step 6.

Enter user ID System Selection Method Selection Authori- zation 5 Summary **6 Result**

Result

For the user **Peter Wright (TESIS SYSware)**
on the target system **Active Directory Services (peterwright)**
with the authorization method **Self-authorization**
a password reset was performed.

The initial password is **iDabitZ4**

▶ The new password has expired. Please alter your password immediately!

The following parties have been informed about the reset:

▶ Standard Notification: peter.wright@tesis.de
▶ List Notification: support.sysware@tesis.de

Next

Certification Checklist for RSA Authentication Manager v6.x

Date Tested: 05/07/2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1.3	Windows Server 2003 Enterprise
RSA Java API	5.0.3.176	Java 1.5.0_14
TESIS ASPR-Kernel	3.5.7	i686 i386 GNU/UNIX 2.6.18-92.1.18.el5
TESIS ASPR-Application	3.5.4	i686 i386 GNU/UNIX 2.6.18-92.1.18.el5

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
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<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
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input type="checkbox"/> N/A
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input type="checkbox"/> N/A
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Credential	<input type="checkbox"/> N/A	Set Credential	<input type="checkbox"/>
Retrieve Credential	<input type="checkbox"/> N/A	Retrieve Credential	<input type="checkbox"/>

BSD / PAR

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

Certification Checklist for RSA Authentication Manager 7.x

Date Tested: 05/08/2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows Server 2003 Enterprise
RSA Java API	5.0.3.176	Java 1.5.0_14
TESIS ASPR-Kernel	3.5.7	i686 i386 GNU/UNIX 2.6.18-92.1.18.el5
TESIS ASPR-Application	3.5.4	i686 i386 GNU/UNIX 2.6.18-92.1.18.el5

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
PIN Reuse	<input checked="" type="checkbox"/>	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
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
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

BSD / PAR

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