



RSA SecurID Ready Implementation Guide

Last Modified: February 12th, 2015

Partner Information

Product Information	
Partner Name	Ericsson
Web Site	www.ericsson.com
Product Name	Telecom Server Platform (TSP)
Version & Platform	TSP 7
Product Description	Telecom Server Platform (TSP) is a platform for server and control nodes requiring the highest level of availability and scalability in existing and future IP multimedia networks. It offers a unique combination of scalable capacity, real-time characteristics, high availability, and service retainability. TSP is based on the concept of openness. The Operation and Maintenance (O&M) has an interface openness for the operators and uses Linux as the operating system. The Dicos operating system is used for the demanding real-time tasks. An open development environment based on several commercial tools is provided for application designers using the languages C, C++, or Java. TSP interoperates with applications on other types of platforms, and supports open protocols for network signaling such as SS7, Diameter, SCTP, TCP, UDP, or IP. TSP has a cluster of loosely coupled central processors that allows scaling from very small systems to nodes with multiple processors. Extremely powerful as well as small or medium sized server nodes can be created, and their capacity can be increased by adding new processors. High availability and reliability is achieved by the cluster software design and a distributed database. All board components — power and Ethernet ports, for example — are duplicated. The hardware can be swapped with zero downtime (hot-swapping) during operations.



ERICSSON

Solution Summary

Telecom Server Platform (TSP) can be integrated with the RSA SecurID product to provide one-time password authentication of its O&M users. By using one-time password based authentication, a higher level of password security can be reached as it eliminates some vulnerability of static passwords. One can use RSA SecurID integrated deployment to centralize the credential storage of multiple different nodes in a network.

TSP can be integrated with RSA SecurID product only through the RADIUS protocol. When an O&M user authenticates (and RADIUS authentication is configured), TSP performs RADIUS authentication of that user towards the RSA SecurID server. TSP fully supports one-time password based authentication on the Node Management Toolbox, TSP-CLI and SSH O&M interfaces and simple authentication on the LDAP interface.

RSA Authentication Manager supported features	
Ericsson Telecom Server Platform	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	No
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	No
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

Agent Host Configuration

To facilitate communication between Ericsson Telecom Server Platform 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 Telecom Server Platform and contains information about communication and encryption.

Ericsson Telecom Server Platform will be communicating with RSA Authentication Manager via RADIUS, so a RADIUS client that corresponds to the agent host record must be created in the RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

 **Note: The RADIUS client's hostname must resolve to the IP address specified.**

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Telecom Server Platform 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 Telecom Server Platform components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configure SecurID Authentication via TSP CLI

1. Open an SSH connection to the TSP server.

```
ssh <user_id>@<ip_address> -p 31310
```
2. Set autowizard mode (to get prompts for required parameters).

```
set autowizard true
```
3. Enter configuration mode.

```
configure
```
4. Add the primary RSA Authentication server. Replace <Primary RSA server> with your primary RSA server's name.

```
insert Node TspPlatform TspSecurity TspAuthentication TspRadiusAuthentication  
TspRadiusServer <Primary RSA server>
```
5. Enter the RADIUS server IP address when prompted.
6. Enter the RADIUS secret when prompted.
7. Enable the primary RSA Authentication server. Replace <Primary RSA server> with the name of your primary RSA server.

```
set Node TspPlatform TspSecurity TspAuthentication TspRadiusAuthentication  
TspRadiusServer <Primary RSA server> tspRadiusServerPriority 1
```
8. Add the replica RSA Authentication server. Replace <Replica RSA server> with your replica RSA server's name.

```
insert Node TspPlatform TspSecurity TspAuthentication TspRadiusAuthentication  
TspRadiusServer <Replica RSA server>
```
9. Enter the RADIUS server IP address when prompted.
10. Enter the RADIUS secret when prompted.
11. Enable the replica RSA Authentication server. Replace <Replica RSA server> with the name of your replica RSA server.

```
set Node TspPlatform TspSecurity TspAuthentication TspRadiusAuthentication  
TspRadiusServer <Replica RSA server> tspRadiusServerPriority 2
```
12. Enable RADIUS authentication method.

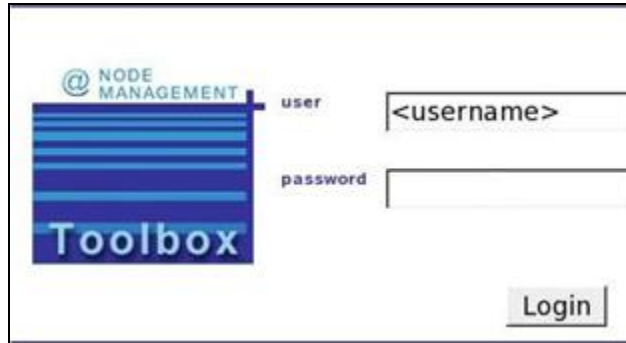
```
set Node TspPlatform TspSecurity TspAuthentication TspRadiusAuthentication  
tspProcessingOrder 1
```
13. Apply the configuration.

```
commit
```

14. Exit the configuration mode.
 exit
15. Exit the system.
 exit

RSA SecurID Login Screens

Login screen:



@ NODE MANAGEMENT

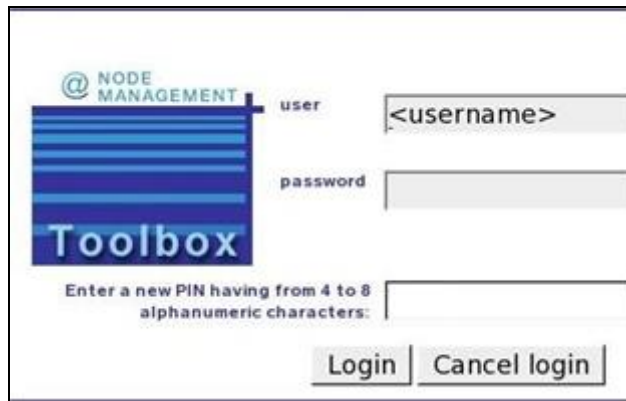
user

password

Toolbox

Login

User-defined New PIN:



@ NODE MANAGEMENT

user

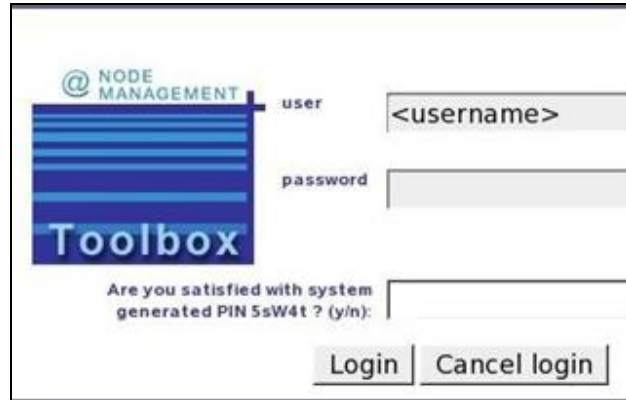
password

Toolbox

Enter a new PIN having from 4 to 8 alphanumeric characters:

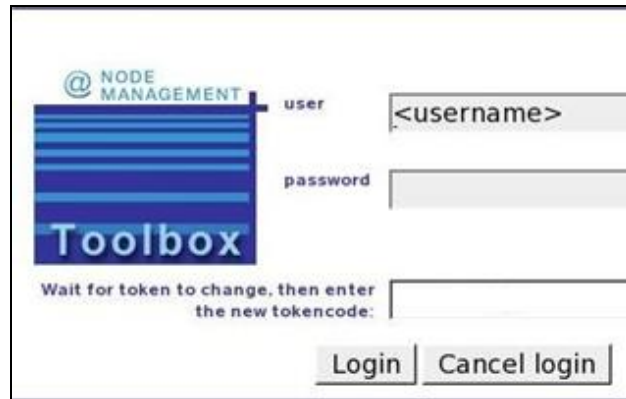
Login Cancel login

System-generated New PIN:



The screenshot shows the Node Management Toolbox login interface. On the left is a blue logo with the text '@ NODE MANAGEMENT' and 'Toolbox'. To the right are input fields for 'user' (containing '<username>') and 'password'. Below these is a text prompt: 'Are you satisfied with system generated PIN 5sW4t ? (y/n):' followed by an empty input field. At the bottom right are two buttons: 'Login' and 'Cancel login'.

Next Tokencode:



The screenshot shows the Node Management Toolbox login interface. On the left is a blue logo with the text '@ NODE MANAGEMENT' and 'Toolbox'. To the right are input fields for 'user' (containing '<username>') and 'password'. Below these is a text prompt: 'Wait for token to change, then enter the new tokencode:' followed by an empty input field. At the bottom right are two buttons: 'Login' and 'Cancel login'.

Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1 SP1	Virtual Appliance
Ericsson Telecom Server Platform (CLI)	TSP 7	Proprietary

RSA SecurID Authentication

Date Tested: February 3rd, 2015

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

PEW / PAR

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

Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1 SP1	Virtual Appliance
Ericsson Telecom Server Platform (SSH)	TSP 7	Proprietary

RSA SecurID Authentication

Date Tested: February 9th, 2015

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

PEW / PAR

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

Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1 SP1	Virtual Appliance
Ericsson Telecom Server Platform (Toolbox)	TSP 7	Proprietary

RSA SecurID Authentication

Date Tested: February 3rd, 2015

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

PEW / PAR

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