Vanguard Integrity Professionals
ez/Token

RSA SecurID Ready Implementation Guide

Last Modified: March 18, 2014

Partner Information

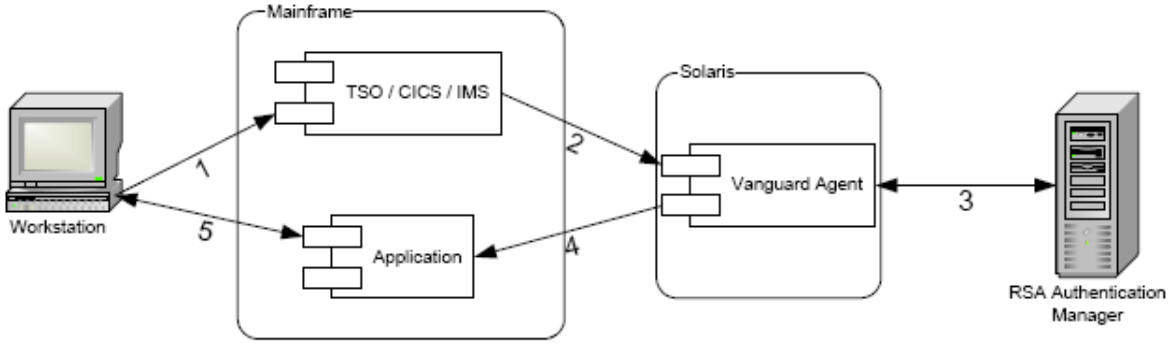
Product Information	
Partner Name	Vanguard Integrity Professionals
Web Site	www.go2vanguard.com
Product Name	ez/Token
Version & Platform	2.1 – Windows
Product Description	Vanguard ez/Token is a two-factor RSA authentication solution that allows users to authenticate through RSA SecurID tokens to the zSeries Server or other application currently using RACF authentication.

VANGUARD
Integrity Professionals
Information Security Experts

Solution Summary

ez/Token™ is a two-factor authentication solution integrated with RACF for users logging on to the mainframe. This solution provides a more secure alternative than the usual RACF user ID/password combination by allowing users to authenticate with RSA SecurID tokens. This allows for seamlessly integrating the mainframe with existing RSA SecurID infrastructures and can allow users to access their mainframe applications using their RSA SecurID tokens.

RSA Authentication Manager supported features	
ez/Token	
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
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	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



1. A user attempts to authenticate to the mainframe via TSO, CICS, or some other protocol. The user provides their RACF user ID and either a password, or if they are a RSA SecurID user, a PASSCODE.
2. Vanguard Mainframe Authentication Exit intercepts the authentication request, and checks the RACF user ID to see if the user requires RSA SecurID authentication.

> **Note: If this is an RSA SecurID user, the PASSCODE is sent to the Vanguard Authentication Agent for validation. If it is not an RSA SecurID user, the request is passed through to RACF.**

3. The Vanguard Authentication Agent passes the provided user ID and PASSCODE to the RSA Authentication Manager server.
4. Once the user is authenticated, his credentials are passed on to the requested application.
5. The user accesses the requested application.

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 ez/Token will occur.

RSA SecurID files

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

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 ez/Token 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 ez/Token components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Integration Overview

The Vanguard ez/Token solution is composed of 4 parts, which should be installed in the following order:

1. Security On Demand Host Server (VIPMAIN)
2. Identity and Access Manager Server (IAMEZTSV)
3. ez/Token Agent
4. ez/Token Authentication Exit (ICHRIX01)
5. ez/Token Website

Root authority on the Solaris servers, or Administrative authority on the Windows server is required for installation. Authority to install a RACF Exit is required on the mainframe. An IIS Web Server capable of servicing a CGI application is required to host the ez/Token Website.

Enable RACF users for RSA SecurID Authentication

Users can be enabled for authentication with RSA SecurID by authorizing the users to a RACF resource.

1. Obtain the RSA Authentication Manager's sdconf.rec configuration file from the RSA Security Console and copy it to the following directory on the server running the ez/Token Agent.

   ```
   %systemroot%\system32
   ```

2. Define the ez/Token resource to RACF using the following command:

   ```
   RDEFINE MDSNUF EZTOKEN.SECURID UACC(NONE)
   ```

3. Create two RACF groups using the following commands:

   ```
   AG (TOKNPIN) Users in this group require a PIN and Tokencode
   AG (TOKNONLY) Users in this group require a Tokencode only.
   ```

4. Give the groups access to the EZTOKEN.SECURID resource created in Step 3 above:

   ```
   PE EZTOKEN.SECURID CLASS(MDSNUF) ACCESS(READ) ID(TOKNPIN)
   PE EZTOKEN.SECURID CLASS(MDSNUF) ACCESS(UPDATE) ID(TOKNONLY)
   ```

5. Connect users to the relevant group. Any users NOT connected to one of these groups will use native RACF authentication.

```
CONNECT (USERID01) GROUP(TOKNPIN)
CONNECT (USERID02) GROUP(TOKNONLY)
```

See the Vanguard Security Solutions Installation Guide Chapter 12 for more information on how to set this up.

Note: Users must have SecurID usernames on the ez/Token Agent Host that match their RACF user names.

Certification Checklist for RSA Authentication Manager

Date Tested: March 18, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1	Virtual Appliance
ez/Token	2.1.04	Windows Server 2008

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	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	✓	Deny Alphanumeric PIN	N/A
Deny PIN Reuse	✓	Deny 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
On-Demand Authentication			
On-Demand Authentication	N/A	On-Demand Authentication	N/A
On-Demand New PIN	N/A	On-Demand New PIN	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

PEW / PAR

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

Known Issues

New PIN / Next Tokencode

ez/Token is capable of integrating with existing logon interfaces, such as TSO. As these screens cannot be changed, it is not possible to perform new pin or next tokencode functions when authenticating through the ez/Token Mainframe Authentication Exit from these screens. A website is provided to allow users to perform these functions.

On Demand Authentication

Because of reasons related to the above issue, ez/Token is unable to perform On Demand Authentications.

Appendix

Partner Integration Details	
RSA SecurID API	5.3.0.747
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Node Secret:

The node secret file is stored in the Windows Registry. Delete the NodeSecret registry key from the following location to reset the node secret.

```
[HKEY_LOCAL_USER\SOFTWARE\SDTI\ACECLIENT]
```

sdconf.rec:

The sdconf.rec file is stored in the following location. Delete or overwrite this file to remove or update the RSA server configuration file.

```
%systemroot%\system32\sdconf.rec
```

sdopts.rec:

The sdopts.rec file is stored in the following location. Delete or overwrite this file to remove or update the RSA agent options file.

```
%systemroot%\system32\sdopts.rec
```

sdstatus.12:

The sdstatus.12 file is stored in the following location. Delete this file to reset the server list.

```
%systemroot%\system32\sdopts.rec
```

Agent Tracing:

To enable agent tracing set the following environment variables on your system. Please refer to RSA agent documentation for more information about agent tracing.

```
RSATRACELEVEL=15
RSATRACEDEST=<log file name>
```