# SOFTEL Communications

## Password Reset and Identity Management Suite

# RSA Secured Implementation Guide

Last Modified: May 8th 2008

## Partner Information

| Product Information | |
|---|---|
| **Partner Name** | SOFTEL Communications Inc |
| **Web Site** | www.softel.com |
| **Product Name** | SOFTEL Password Reset and Identity Management Suite |
| **Version & Platform** | V3.1 |
| **Product Description** | The SOFTEL Password Reset and Identity Management Suite provides comprehensive voice-enablement, ensuring secure access to enterprise resources using telephones as the access modality, complementing or replacing traditional channels.<br>Included in the solution are web portals for user registration, detailed reporting, management tools and self service applications like password reset.<br>The SOFTEL suite integrates into existing telephony infrastructures to provide users with multi-factor identification including speaker verification, ANI/IP authentication, challenge/response questions and token verification. Once authenticated, users can be granted access to secure resources, data, networks, or even physical access to premises. |
| **Product Category** | Networks and Communication<br>Provisioning |

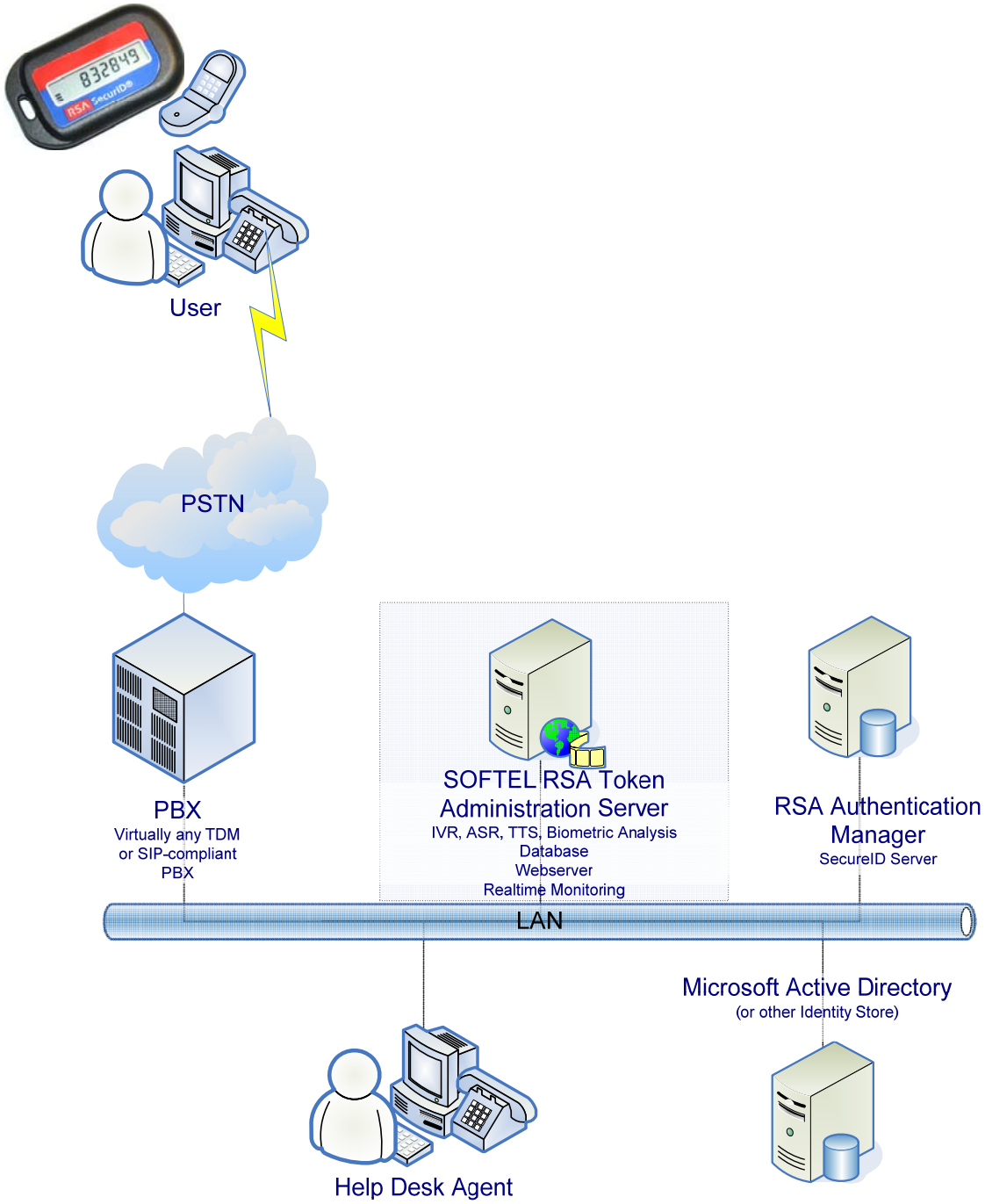
# Solution Summary

The SOFTEL Password Reset and Identity Management Suite integration with RSA Authentication Manager offers users convenience, efficiency and enhanced security. It provides voice-enabled provisioning and administration of RSA users, groups and SecurID tokens. With these features, an administrator can add users, enable, disable, assign and un-assign tokens and manage password policies over the telephone. The integration's self-service feature allows users to reset their PINS and passwords and declare their tokens lost and found.

In addition, SOFTEL has added SecurID two-factor authentication functionality to its security platform, thus giving SOFTEL users a stronger and more reliable level of authentication. For example, phone banking application users can add dynamic SecurID token codes to their static passwords. Since a token code changes every 60 seconds and is only displayed on the token itself, the static password becomes the weakest component in the authentication procedure. This provides a higher level of security and user confidence and a lower risk of fraud.

The SOFTEL RSA Token Management component is a Web Service that facilitates communication between Authentication Manager and the Identity Management Suite. It can be easily installed from an executable included with the SOFTEL software distribution. Please see the installation instructions below for details.

| Partner Integration Overview | |
|---|---|
| **Support for Standard Card, Key Fob, PINPAD, and SoftID** | Yes |
| **Add a user to the RSA Authentication Manager Database** | Yes |
| **Assign a token** | Yes |
| **Un-assign a user's token** | Yes |
| **Delete a user from the RSA Authentication Manager Database** | Yes |
| **Clear/Reset a token's PIN** | Yes |
| **Enable a token** | Yes |
| **Disable a token** | Yes |
| **Change User Authentication Method** | Yes |
| **Assign a password** | Yes |
| **Un-assign a password** | Yes |
| **Add a user to a group** | Yes |
| **Remove a user from a group** | Yes |




SOFTEL Communications Inc.
www.softel.com
Americas: 877.4.SOFTEL (877.476.3835)
UK: + 44 (0) 870.141.7145
moreinfo@softel.com

# Product Requirements

## *The SOFTEL RSA Token Management component requirements:*

- Apache HTTP Server 2.2 should be installed co-resident with the RSA Authentication Manager.
- The SOFTEL RSA Token Management component should be installed co-resident with the RSA Authentication Manager. This component is on the installation CD provided by SOFTEL. http://www.softel.com

**Partner Product Requirements:**

| SOFTEL Password Reset and Identity Management Solutions | |
|---|---|
| **CPU** | X86 2GHz or faster |
| **Memory** | 500 MB RAM |
| **Storage** | 50GB Hard Drive space |
| **Firmware Version** | N/A |

# Partner Agent Configuration

## Before You Begin

This section provides instructions for integrating the SOFTEL Password Reset and Identity Management Suite with RSA Authentication Manager. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has working knowledge of the two products to perform the tasks outlined in this section. Both products should be installed prior to the integration. Before proceeding, perform any tests necessary to ensure that they are functioning properly.

## The SOFTEL RSA Token Management component configuration:

1. Login to the RSA Authentication Manager Server with administrator privileges.
2. Insert the RSA Token Management CD provided by SOFTEL and run the setup.exe. This will copy the necessary files to the PC.
3. Go to the default Apache path (C:\Program Files\Apache Software Foundation\Apache2.2\cgi-bin) and verify that RSAWebService.exe is there.

After completing theses 3 steps, you can immediately call into the SOFTEL Password Reset and Identity Management Suite and login using your RSA SecurID token. Based on your privileges (administrator or user), a menu listing is provided.

As the administrator, you can continue to use RSA Authentication Manager to make changes or use the SOFTEL Token Management to update users over the phone.

# Certification Checklist

Date Tested: March 31st 2008

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| RSA Authentication Manager | 6.1 | Windows 2003 |
| SOFTEL Password Reset and Identity Management Suite | 3.1 | Linux |
| | | |

| Test | Result |
|---|---|
| 1st time connection to RSA Authentication Manager Database | ✓ |
| User Management | |
| Add a user | ✓ |
| Assign a token | ✓ |
| Un-assign a token | ✓ |
| Change Authentication Method | ✓ |
| Assign a password | ✓ |
| Un-assign a password | ✓ |
| Enable a user's token | ✓ |
| Disable a user's token | ✓ |
| Clear/Reset a user token's PIN | ✓ |
| Delete a user | ✓ |
| Add a user to a group | ✓ |
| Remove a user from a group | ✓ |

INIT / PAR

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