

RSA Ready Implementation Guide for RSA | SecurID®

Smart Verify

Peter Waranowski, RSA Partner Engineering
Last Modified: November 4th, 2016

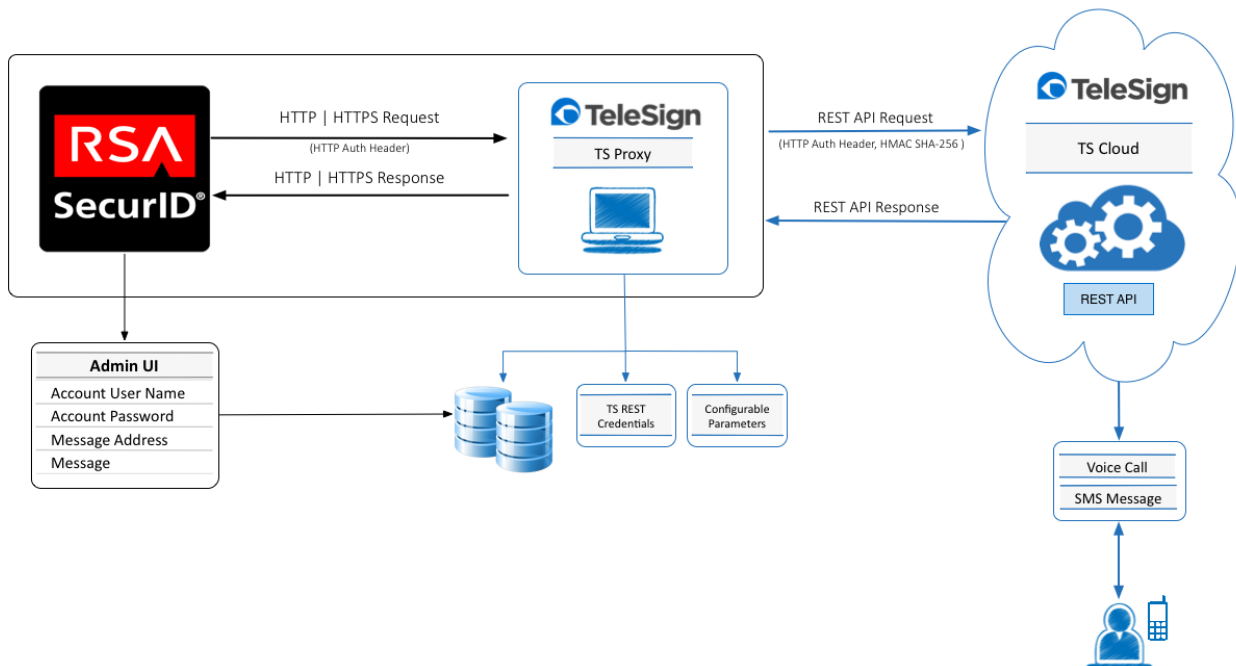
Solution Summary

RSA Authentication Manager can be configured to utilize TeleSign Smart Verify for delivery of on-demand tokencodes to be used in on-demand authentications.

When a user authenticates to an agent using his/her username and on-demand PIN, the RSA Authentication Manager sends the on-demand tokencode and phone number to Telesign TS-proxy which relays the request to TeleSign Smart Verify. TeleSign Smart Verify then determines whether the destination is a land line or mobile device. If the destination is a land line, Smart Verify will deliver the on demand token via phone call. If the destination is a mobile device, Smart Verify will deliver the on demand tokencode to the user's mobile device via Short Message Service. The authentication process is completed when the user enters the on-demand tokencode into the agent's prompt for next tokencode.

| RSA HTTP Plug-In Supported Functions | |
|--|-----|
| TeleSign Smart Verify | |
| Integrates with HTTP Plug-In via HTTP | No |
| Integrates with HTTP Plug-In via HTTPS | Yes |

! > Important: For security reasons, TeleSign recommends to deploy the TS Proxy in the same network that hosts the RSA Authentication Manager, and make sure this machine is hardened from a security perspective



RSA Authentication Manager Configuration

RSA Authentication Manager can be configured to integrate a supported Short Message Service (SMS) provider using HTTP, HTTPS, or XML-over-HTTP to deliver on-demand tokencodes to a user's mobile phone.

! > Important: HTTP connections are not secure. Sensitive information, such as a tokencode, may be exposed. For secure connections, configure HTTPS.

Before configuring the HTTP Plug-In, you must locate the configuration parameters and base URL. Contact your SMS provider for this information. You must include the following elements within your provider's parameters to retrieve data from the corresponding fields.

| Required HTTP Plug-In Parameters | |
|----------------------------------|---|
| Elements | Description |
| \$cfg.user | Account User Name |
| \$cfg.password | Account Password |
| \$msg.address | User Attribute to Provide SMS Destination |
| \$msg.message | On-Demand Tokencode Message |

The SMS HTTP Plug-In is configured in the RSA Authentication Manager's Security Console. The configuration page has three sections:

- Tokencode Delivery by SMS
- SMS Provider Configuration
- SMS HTTP Proxy Configuration (optional)

Tokencode Delivery

- Mark the **Delivery by SMS** checkbox to enable the delivery of On-Demand Tokencodes using SMS service.
- Select the **User Attribute to Provide SMS Destination** from the drop-down menu.
- (Optional) Select the **Default country code** from the drop-down menu.
- Select **HTTP** from the SMS Plug-In drop-down menu.

Tokencode Delivery by SMS

Delivery by SMS: Enable the delivery of on-demand tokencodes using SMS service

User Attribute to Provide SMS Destination: * -- Choose One --

Default country code: * -- Lookup Country Code --

SMS Plug-In: * HTTP

SMS Provider Configuration

- Copy the following line into the **Base URL** field and replace [IP or hostname] with the IP or hostname of your TS-Proxy server.
https://[IP or hostname]/TS-proxy
- Click **Import Certificate** to browse to and install the certificate.
- Select **POST** from the HTTP Method drop-down menu.
- Copy the following string into the **Parameters** field.
user=\$cfg.user&password=\$cfg.password&to=\$msg.address&text=\$msg.message&telesign_verify=smart&ucid=TRVF

Note: TeleSign Smart Verify is highly customizable. Refer to the documentation included with the TeleSign TS Proxy for more information on configuring the parameters field.

- Enter your Telesign **Customer ID** into the **Account User Name** field.
- Enter your Telesign **API Key** into the **Account Password** field.
- Copy the following line into the **Success Response Code** field.
200
- Copy the following line into the **Response Format** field.
.*"code":(\d*),.*

SMS Provider Configuration

Base URL: RSA recommends using HTTPS to increase security.

Certificate: (If you enter an HTTPS Base URL, you must import a certificate.)

HTTP Method: GET

Parameters:

Account User Name:

Account Password:

Connection Timeout: 5000 milliseconds

Success Response Code:

Response Format:

SMS HTTP Proxy Configuration (Optional)

Enter the configuration settings for your HTTP Proxy server if you are using one.

| SMS HTTP(S) Proxy Configuration | |
|---------------------------------|----------------------|
| ② Proxy Hostname: | <input type="text"/> |
| ② Proxy Port: | <input type="text"/> |
| ② Proxy User: | <input type="text"/> |
| ② Proxy Password: | <input type="text"/> |

Click **Update** to save the SMS Configuration.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the TeleSign Smart Verify with RSA HTTP Plug-In to deliver on-demand tokencodes. 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.

! > Important: For security reasons, TeleSign recommends to deploy the TS Proxy in the same network that hosts the RSA Authentication Manager, and make sure this machine is hardened from a security perspective

1. Acquire your Customer ID and API key from TeleSign.
2. Deploy the TeleSign TS-proxy web app on an Apache Tomcat application server that is configured for HTTPS with a trusted certificate.

Certification Checklist for RSA Authentication Manager

Date Tested: October 27th, 2016

| Certification Environment | | |
|----------------------------|---------------------|----------------------|
| Product Name | Version Information | Operating System |
| RSA Authentication Manager | 8.2 | Virtual Appliance |
| RSA Authentication Agent | 7.3.1 | Windows 7 Enterprise |
| TeleSign Smart verify | n/a | n/a |
| TeleSign TS-proxy | 0.7 | Windows 2k12R2 |

| Mandatory Functionality | |
|---|---|
| SMS Message Delivered | ✓ |
| On-Demand Authentication with SMS tokencode | ✓ |
| Success Code Received by HTTP Plug-In | ✓ |

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