



RSA SMS HTTP Plug-In Implementation Guide

Last Modified: November 19th, 2014

Partner Information

Product Information	
Partner Name	CellTrust
Web Site	www.celltrust.com
Product Name	SMS Gateway
Version & Platform	3.18
Product Description	CellTrust mobile solutions and technologies can be used in a wide range of applications, from enterprise developed, content management systems or to add mobile as a channel to an existing website regardless of the technology you are currently using. The CellTrust 2-Way SMS Gateway facilitates communication between your applications and mobile carriers around the world.

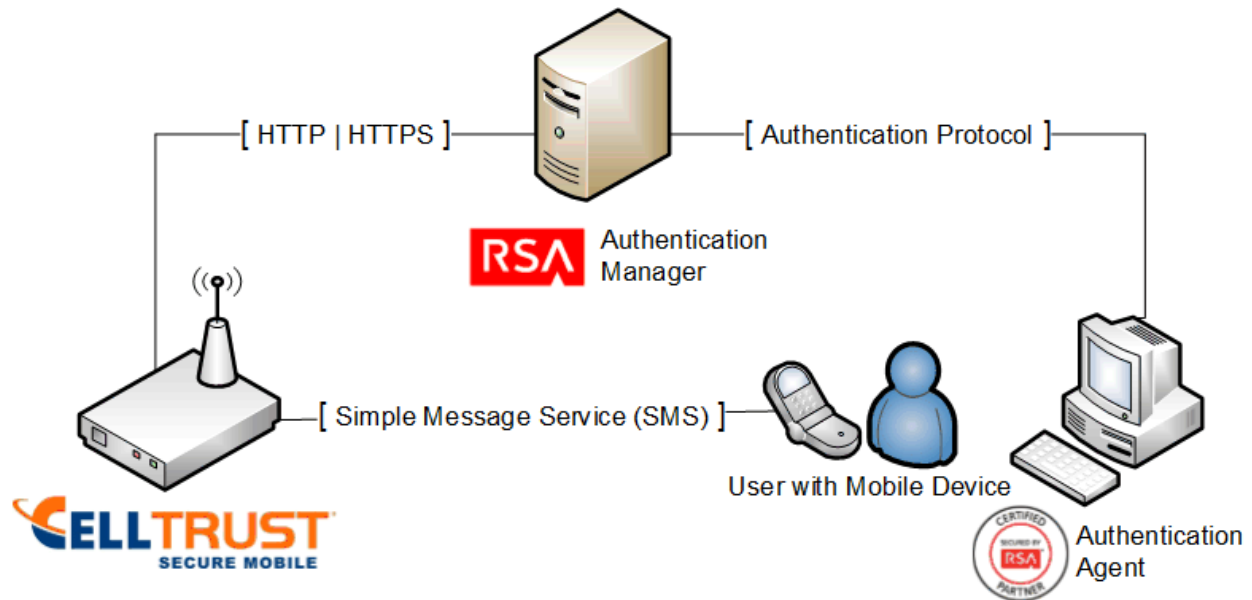


Solution Summary

RSA Authentication Manager can be configured to utilize CellTrust SMS Gateway 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 mobile number to CellTrust SMS Gateway using the HTTP or HTTPS protocol. CellTrust SMS Gateway then delivers the on-demand tokencode to the user's mobile device via Short Message Service (SMS.) 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	
CellTrust SMS Gateway	
Integrates with HTTP Plug-In via HTTP	Yes
Integrates with HTTP Plug-In via HTTPS	Yes



SMS HTTP Plug-In 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

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 by SMS

- 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	
② Delivery by SMS:	<input checked="" type="checkbox"/> Enable the delivery of on-demand tokencodes using SMS service
② User Attribute to Provide SMS Destination: *	-- Choose One --
② Default country code: *	-- Lookup Country Code --
② SMS Plug-In: *	HTTP

SMS Provider Configuration

- Copy the following line into Base URL field.
`http://gateway.celltrust.net/TxtNotify/TxtNotify`
- Click Import Certificate to browse to and install an SMS certificate if you are configuring your base for HTTPS.
- Select POST from the HTTP Method drop-down menu.
- Copy the following string into the Parameters field.
`Username=$cfg.user&Password=$cfg.password&CustomerNickname=$cfg.user&PhoneDestination=$msg.address&Message=$msg.message&XMLResponse=true`
- Enter Account User Name for the SMS Provider.
- Enter Account Password for the SMS Provider.
- Copy the following line into the Success Response Code field.
`ACCEPTED`
- Copy the following line into the Response Format field.
`.+?<Status>(.*?)</Status>.*`

The screenshot shows the 'SMS Provider Configuration' web form. It includes the following fields and options:

- Base URL:** A text input field with a red asterisk. Below it, a note says 'RSA recommends using HTTPS to increase security.'
- Certificate:** A blue 'Import Certificate' button and a note: '(If you enter an HTTPS Base URL, you must import a certificate.)'
- HTTP Method:** A dropdown menu currently set to 'GET'.
- Parameters:** A large text area with a red asterisk.
- Account User Name:** A text input field with a red asterisk.
- Account Password:** A text input field with a red asterisk.
- Connection Timeout:** A text input field containing '5000' followed by 'milliseconds'.
- Success Response Code:** A text input field with a red asterisk.
- Response Format:** A text input field with a red asterisk.

SMS HTTP Proxy Configuration (optional)

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

The screenshot shows the 'SMS HTTP(S) Proxy Configuration' web form with the following fields:

- Proxy Hostname:** A text input field.
- Proxy Port:** A text input field.
- Proxy User:** A text input field.
- Proxy Password:** A text input field.

Click Update to save the SMS Configuration.

Certification Checklist for RSA HTTP Plug-In

Date Tested: November 13th, 2014

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
RSA Authentication Agent	7.2	Windows 7 Enterprise 64bit
CellTrust SMS Gateway		

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

PEW

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