HipLink
Communication Server

RSA SMS HTTP Plug-In Implementation Guide

Last Modified: March 13th, 2015

Partner Information

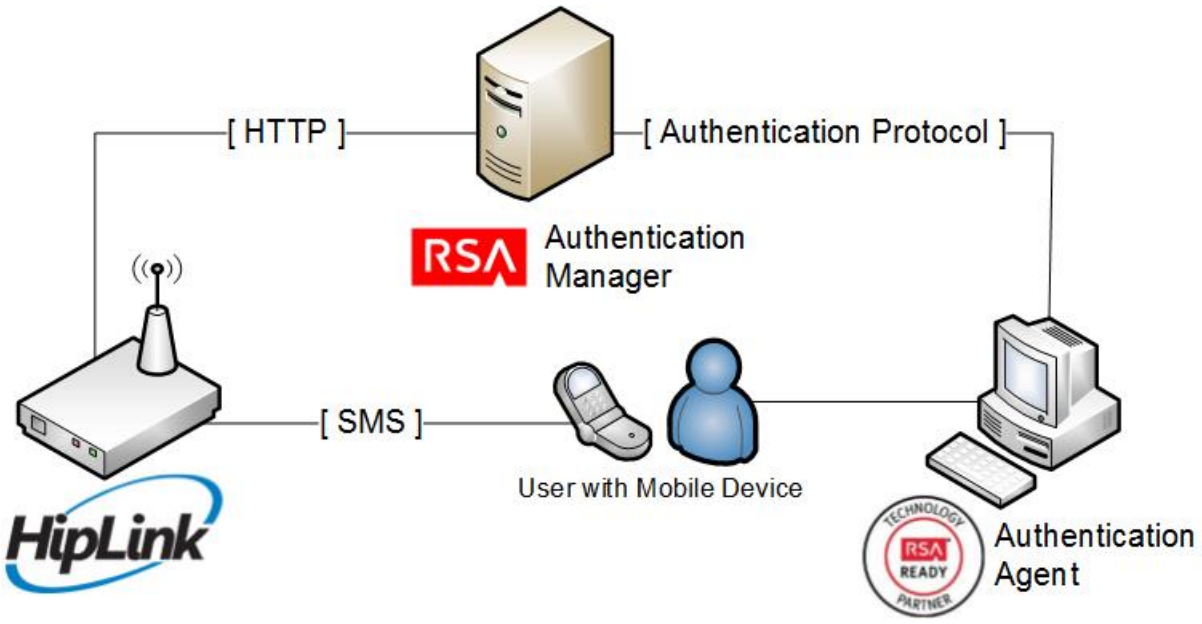
Product Information	
Partner Name	HipLink
Web Site	www.hiplink.com
Product Name	Hiplink Communication Server
Product Description	HipLink is a wireless messaging solution used successfully across all organizations, from large Fortune 1000 enterprises to small businesses and to local government agencies. It works seamlessly to integrate with existing network infrastructure and offers a wide range of flexible options through its modular design. As web-based software, HipLink provides SMS text and voice alerts to any wireless devices including pagers, cell phones, PDAs, land-line phones, fax machines, computer desktops, and smart phones. It can automate alerts so they reach individuals or groups of individuals that you designate. It allows for two-way messaging to ensure alerts received are confirmed and to initiate further communication.

Solution Summary

RSA Authentication Manager can be configured to utilize Hiplink Communication Server 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 Hiplink Communication Server using the HTTP protocol. Hiplink Communication Server 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	
Hiplink Communication Server	
Integrates with HTTP Plug-In via HTTP	Yes
Integrates with HTTP Plug-In via HTTPS	No



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. You must include the following elements within your provider's parameters to retrieve data from the corresponding fields.

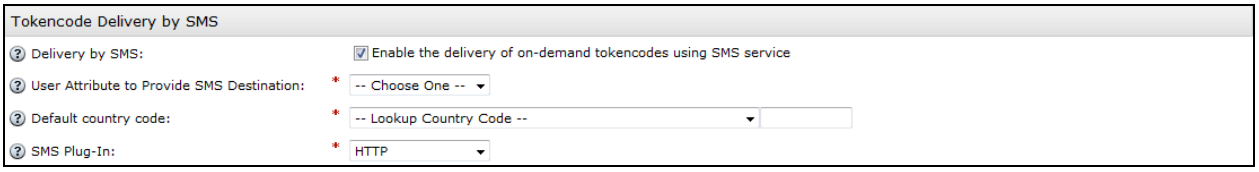
Required HTTP Plug-In Parameters	
Elements	**Description**
$cfg.user	Account User Name
$cfg.password	Account Password
$msg.address	User Attribute to Provide SMS Destination
$msg.message	On-Demand Tokencode Message

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.



SMS Provider Configuration

- Copy the following line into Base URL field and replace [IP or hostname] with the IP or hostname provided by Hiplink.

  `http://[IP or hostname]/cgi-bin/action.exe`

- Select GET from the HTTP Method drop-down menu.
- Copy the following string into the Parameters field.

  ```
  cmd=Cli&modid=cli&msgtype=quick&carrier_name=HipText-
  RSA&pin=$msg.address&message=$msg.message
  ```

- Enter anything into the Account User Name field.
- Enter anything into the Account Password field.

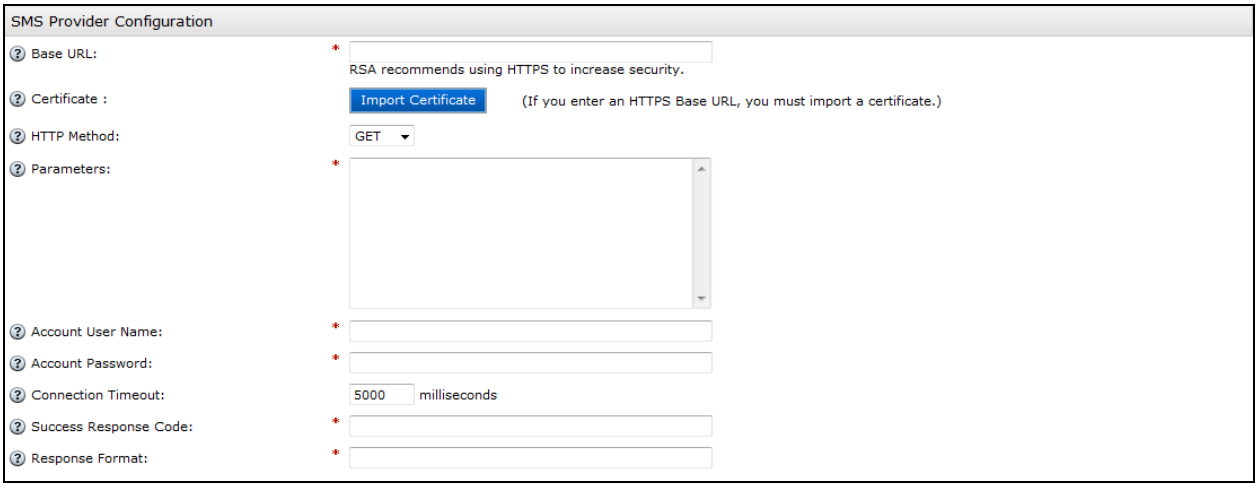
> **Note: Account Username and Account Password fields are required by the HTTP Plug-In configuration, however they are not used by Hiplink.**

- Copy the following line into the Success Response Code field.

  `200`

- Copy the following line into the Response Format field.

  `(...)`



SMS HTTP Proxy Configuration (optional)

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

Click Update to save the SMS Configuration.

Certification Checklist for RSA HTTP Plug-In

Date Tested: March 12th, 2015

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1 SP1	Virtual Appliance
RSA Authentication Agent	7.2.1.28	Windows 7 Enterprise
Hiplink Communication Server	N/A	N/A

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