AT&T
Global Smart Messaging Suite

RSA SMS HTTP Plug-In Implementation Guide

Last Modified: April 30, 2012

Partner Information

Product Information	
Partner Name	AT&T
Web Site	www.att.com/smartmessagingsuite
Product Name	Global Smart Messaging Suite
Product Description	The AT&T Global Smart Messaging Suite is a powerful web-based messaging application designed for business communication. The AT&T Global SMS service enables 2-way SMS communication between company systems and mobile consumer subscribers at most wireless carriers globally. The platform can be integrated to work seamlessly with existing systems such as RSA's 2-factor authentication system, and can also enable a wide variety of additional integrated or stand-alone SMS applications, including workforce management and communication, mobile marketing campaigns, mobile commerce, HR functions, job placement and staffing, shift confirmations, scheduling reminders, voting, polling, surveying, sweepstakes and more. AT&T can help organizations get started using domestic short codes for cross-carrier SMS messaging and the AT&T platform can also be extended on a global scale for messaging to employees and consumers worldwide.

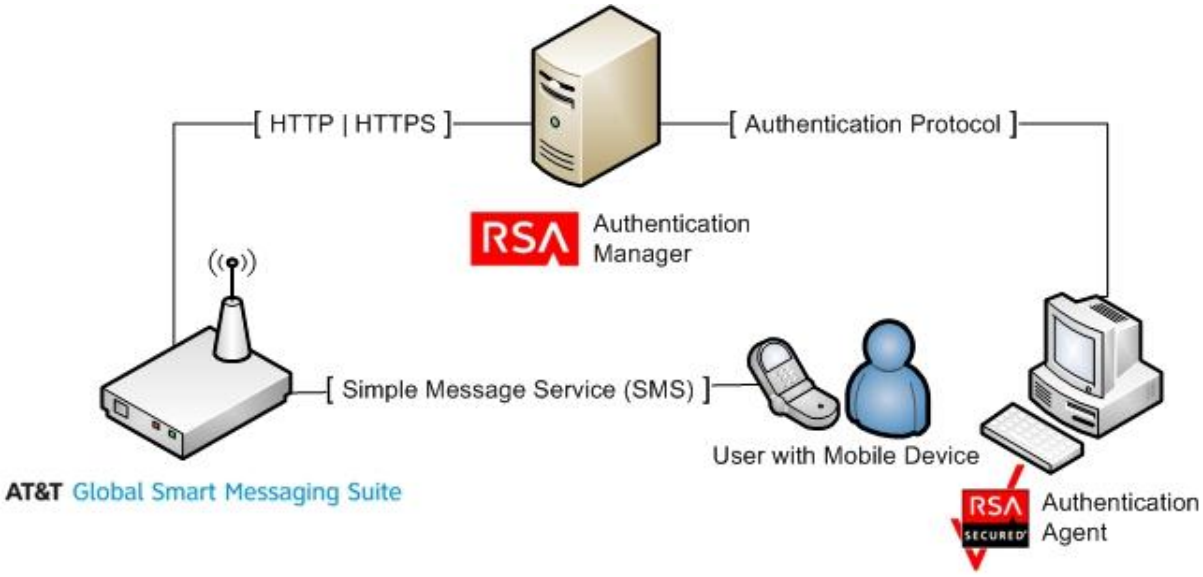
AT&T Global Smart Messaging Suite

Solution Summary

RSA Authentication Manager can be configured to utilize AT&T Global Smart Messaging Suite 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 AT&T Global Smart Messaging Suite using the HTTP or HTTPS protocol. AT&T Global Smart Messaging Suite 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	
AT&T Global Smart Messaging Suite	
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.

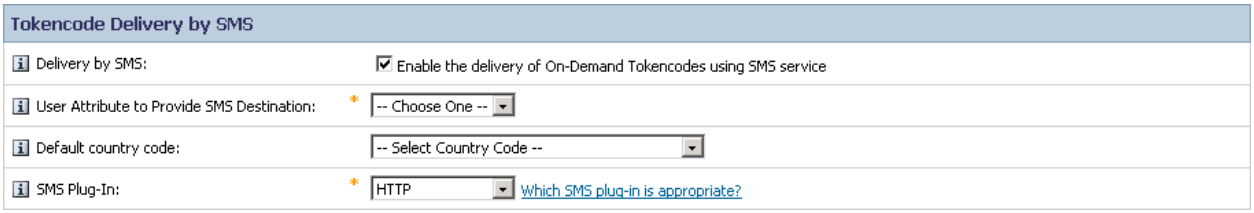
Required HTTP Plug-In Parameters	
Elements	**Description**
$cfg.user	Account User Name
$cfg.password	Account Password
$msg.address	User Attribute to Provide SMS Destination
$msg.message	On-Demand Tokencode Message

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.



SMS Provider Configuration

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

  ```
  http://na1.smartmessagingsuite.com/cgphttp/servlet/sendmsg
  ```

- Click Import Certificate to browse to and install an SMS certificate if you are configuring your base for HTTPS.
- Select GET from the HTTP Method drop-down menu.
- Copy the following string into the Parameters field.

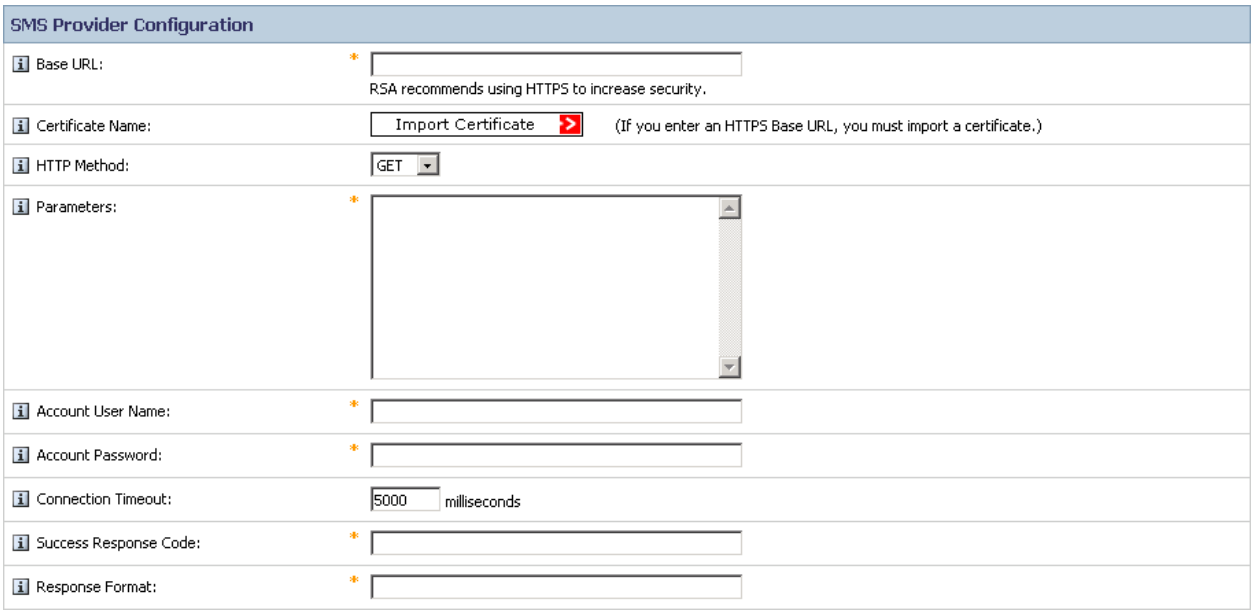
  ```
  to=$msg.address&text=$msg.message&username=$cfg.user&password=$cfg.password
  ```

- 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.

  ```
  OK
  ```

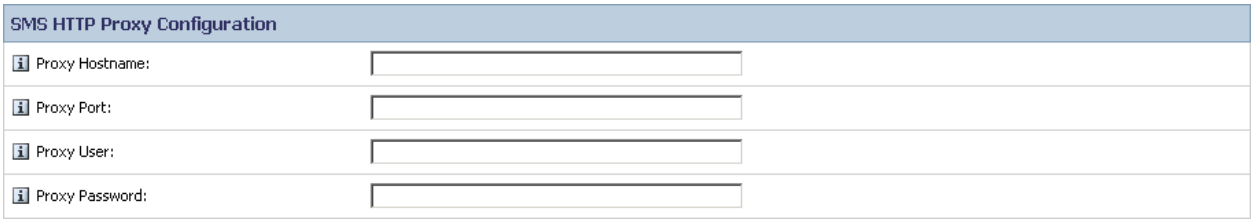
- Copy the following line into the Response Format field.

  ```
  [\d\s]*(.*)M*
  ```



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: April 30, 2012

Product Name	Certification Environment Version Information	Operating System
RSA Authentication Manager	7.1 SP4	Windows Server 2003
RSA Authentication Manager Express	1.0	Appliance
RSA Authentication Agent	7.1	Windows Server 2008 R2
AT&T Global Smart Messaging Suite	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