Symantec™ SMS Out-of-Band Authentication Service Description

Introduction

Symantec™ SMS Out-of-Band (OOB) Authentication Service provides online service providers and enterprises with the ability to authenticate their end users by sending SMS text messages to mobile phones. Symantec SMS OOB Authentication Service requires use of the VIP Authentication Service.

The key components of this service include:

- Web Services API for sending and validating OOB authentication requests; and
- Symantec-hosted console (VIP Manager) for reporting and tracking OOB authentication requests.

This service description outlines the primary elements of the SMS OOB Authentication Service including the service components described below. This service description does not provide details of the VIP Authentication Service, which is described in its service description.

1. SMS OOB Authentication Service Components

a. Web Services API

The Web Services API allows an enterprise to send SMS text messages to specified mobile phone numbers. Each SMS text message contains a numeric one-time password (OTP), generated by Symantec, along with a message specified by the enterprise. The end user receives this message, and enters the OTP into the enterprise's application, which forwards it to Symantec for validation. Symantec then returns a valid or invalid message to the enterprise.

b. VIP Manager

VIP Manager provides reports detailing each SMS OOB authentication request and the result (valid or invalid).

2. Service Level Agreement for SMS Delivery

Notwithstanding anything to the contrary in the applicable VIP Authentication Service Level Agreement, delivery of SMS text messages shall be subject to the following (capitalized words shall have the meanings as defined in the Service Level Agreement):

a. Service Availability

The SMS OOB Authentication Service will be available 99.5%, 24x7x365. Service Availability means the Up Time of the Services excluding Scheduled Down Time and events occurring outside Symantec's span of control. Service Availability shall be measured upon commercial use of the Service, i.e., after Symantec makes the Service generally available to all Customers; commercial use does not include Customer-specific test or non-production environments.

b. Scheduled Down Time/Maintenance

Symantec will notify Customer of any Scheduled Down Time for the Services (including down time for Symantec to implement platform upgrades, patches and/or fixes), depending on the categories of Scheduled Downtime as follows:

i. "Regular Maintenance" means any planned maintenance for the Services conducted between the hours of 01:00 AM and 08:00 AM U.S. Eastern Time. Symantec will notify Customer of such Scheduled Down Time 72 hours prior to any Regular Maintenance.
ii. "Emergency Maintenance" means maintenance for the Services that must be performed promptly, regardless of time of day / busy hour, and unless practicable, without notice.

SYMANTEC SMS OUT-OF-BAND AUTHENTICATION SERVICE TERMS AND CONDITIONS

1. DEFINITIONS

Capitalized words used shall the meanings set forth in the Agreement or the applicable service description to which this service pertains to.

2. CUSTOMER'S OBLIGATIONS

Customer represents and warrants to Symantec that: (i) Customer has obtained the necessary consents, rights in, licenses to, and authority over all data, personal or not, required of End Users necessary for Customer to lawfully provide to Symantec and permit Symantec to receive and process the data as contemplated in this Service Description, including, but not limited to, transferring the data Customer provides to the United States and in other jurisdictions where Symantec maintains a presence for such processing; (ii) the data provided to Symantec does not and will not infringe, misappropriate, or violate any other third party's patent, copyright, trade secret, trademark, service mark, privacy right, publicity, or any other Intellectual Property Right; (iii) it shall use the Service only in compliance with all applicable law; (iv) it shall not use the Services in support of or for any illegal, fraudulent, or improper purpose, and shall immediately notify Symantec if Customer learns of any unauthorized use of the Service.

3. DISCLAIMERS

(a) Third-Party Factors. Customer acknowledges that, in provisioning the Services contemplated herein, Symantec depends on the facilities, networks, connectivity and other acts of third parties not under Symantec's control, including wireless carriers, government entities, and the like ("SMS Network"). SYMANTEC SHALL NOT BE LIABLE FOR ANY INTERRUPTION, DELAY, SUSPENSIONS, AND OTHER ACTS AND/OR OMMISSION BY SUCH THIRD PARTIES THAT ARE NOT WITHIN SYMANTEC'S CONTROL.

(b) Third-Party Charges. Customer shall advise End Users that they may incur additional charges from their wireless carriers, and shall be solely responsible for such charges when sending and/or receiving any SMS text messages, including the SMS text messages issued as part of this Service. Symantec shall not be responsible to reimburse Customer or to End Users for such charges including, but not limited to, inter-connection, access, termination, pager, wireless, landline or any phone charges in the provision of this Service.

(c) SMS Network Restrictions. Customer shall not use the Services to transmit: (i) junk mail, spam, or unsolicited material to persons or entities that have not agreed to receive such material or to whom Customer does not otherwise have a legal right to send such material; (ii) material or data that is illegal, harassing, coercive, defamatory, libelous, abusive, threatening, obscene, harmful to minors, excessive in quantity, or the transmission of which could diminish or harm the reputation of Symantec or any of the wireless carriers involved in the provision of the Services, including but not limited to material that is related to alcoholic beverages, tobacco, guns or weapons, illegal drugs, pornography, crime, violence, death, or any other questionable subject matter.