Symantec™ SMS OTP Authentication Service Description

Introduction

Symantec™ SMS OTP Authentication Service provides online service providers and enterprises with the ability to securely issue One Time Password credentials as SMS text messages to mobile phones. Symantec SMS OTP Authentication Service requires use of either the VIP Authentication Service or the Unified Authentication OTP Service.

The key components of this service include:

- SMS One Time Password credentials (SMS OTP Credentials)
- Web Services API for provisioning and validating Credentials

This service description outlines the primary elements of the SMS OTP Authentication Service including the software and service components described below. This service description does not provide details of the VIP Authentication Service or the UA OTP Service, which are described in their respective service descriptions.

1. SMS OTP Authentication Service Components

a. SMS OTP Credentials

An SMS OTP Credential consists of both a shared key and a unique mobile phone number. The shared key is stored and protected by the validation infrastructure, hosted at the enterprise or at Symantec's data center. Using a known cryptographic algorithm, the SMS OTP Credential is used by Symantec to generate an OTP value. The OTP generated is delivered to the End User's mobile phone handset through an SMS network. This OTP received can then be compared to the OTP value generated, and if the values match, the Credential will be validated. The SMS OTP Credential is anonymous and provides a second authentication factor when it is bound to a local user identity.

b. SMS OTP Credential Provisioning

SMS OTP Credentials are dynamically generated by Symantec upon request by the enterprise to register a new mobile phone number. Symantec then generates the Credential and sends an OTP to the End User's mobile phone to verify that the End User is in possession of that phone. Once possession is confirmed through an additional API call made by the enterprise, the SMS OTP Credential is available for use for future authentications. The service securely stores a copy of the Credential in encrypted form in the enterprise's or Symantec's data center. The Credential is encrypted using a TripleDES encryption algorithm.

c. SMS OTP Credential Issuance and Distribution

Customers are responsible for issuing Credentials to End Users. The logistics involved in the distribution of such Credentials are controlled and implemented by each enterprise.

When issuing a Credential to an End User, an enterprise shall:

- Obtain all the necessary End User identification information;
- Obtain all the necessary Credential identification information;
- Bind the End User to terms and conditions of Credential usage.

d. SMS OTP Credential Validation

Once an End User has completed the activation process with respect to its SMS OTP Credential and has bound it to an identity at the enterprise's website, the enterprise will prompt such End User to communicate an OTP from such SMS OTP Credential for second-factor authentication. The enterprise will validate such End User's first-factor credential, and will retrieve the Mobile Phone Number from its local user store and will forward both the Mobile Phone Number and the OTP to Symantec for validation. Symantec then returns a valid or invalid message to the enterprise.

e. Configuration and Management Console

The Configuration and Management Console, installed as part of the UA OTP software, contains functionality specific to SMS OTP Credentials:

- Disabling/enabling of SMS OTP Credentials
- Testing of SMS OTP Credentials

2. Audit Trails

Audit trails for SMS OTP Credentials are treated no differently than those issued to hardware-based credentials.

3. Service Level Agreement for SMS Delivery

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

a. Service Availability

The SMS OTP 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 OTP AUTHENTICATION SERVICE TERMS AND CONDITIONS

1. DEFINITIONS

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

2. CUSTOMER'S OBLIGATIONS

As a credential issuer, 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 SMS text messages, including the SMS OTP Credential 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.