Norton Secure Login

Service Description

August 2014

Service Overview

The Norton Secure Login Service (referred to herein as "NSL," the "NSL Service" or the "Service") is a cloud-based identity service that provides identity proofing, credential issuance, credential validation, attribute validation, and single sign-on services.

The Customer purchasing the NSL Service from Symantec acts as a Relying Party. Intended End Users of the NSL Service include individual consumers or business representatives of Customer needing identity credentials for authentication at government or commercial websites. End Users of the NSL Service receive identity credentials that can be used at multiple Relying Party websites. Relying Parties who agree to accept NSL-issued credentials avoid the cost and complexity of issuing and managing End User credentials needed for access to their websites and applications.

This Service Description, with any attachments included by reference, is part of any agreement which incorporates this Service Description by reference (collectively, the "Agreement"), for those Services which are described in this Service Description and are provided by Symantec.

Table of Contents

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Features

Key Components of the NSL Service include:

- Core Identity Services consisting of End User services, SAML Authentication, and Single Sign-on.
- Basic and Enhanced End User Identity Credentials
- Remote Identity Proofing, a FICAM-compliant identity proofing service, provided by Symantec's Identity Proofing Agent.
- Out-of-Band Authentication, a component of the Symantec Validation and Identity Protection ("VIP") service that creates and validates one-time passwords sent as short message service ("SMS"), voice messages, or via the VIP mobile application to an End User's cell phone.
- NSL Service Editor for NSL Administrators

The NSL Service meets Federal Identity and Access Management ("FICAM") requirements for remote access to federal agency websites, and is certified under the Kantara Trust Framework as a Credential Service Provider ("CSP") (for more information, please see https://kantarainitiative.org/). The NSL Service performs identity proofing and issues credentials at Assurance Levels 2 and 3 as defined in the National Institute of Standards and Technology ("NIST") Special Publication 800-63-2, located at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=914476 (the "NIST Publication"). In addition, the NSL Service supports the identity federation concept defined in the National Strategy for Trusted Identities in Cyberspace ("NSTIC") (for more information, please see http://www.nist.gov/nstic/).

A. Core Identity Services

The Core Identity Services consist of three components: End User services, SAML Authentication, and Single Sign-on services.

i) End User services include registration, account provisioning and credential management. Through SSL-protected web pages, End Users can create accounts, opt-in for identity proofing, perform the identity proofing process, choose passwords, enroll their cell phone numbers and receive identity credentials. After establishing an account and receiving an identity credential, End Users can also manage their accounts, reset or choose new passwords, delete their accounts, and register new cell phones.

ii) SAML Authentication is the primary mechanism for a Relying Party to request authentication of a NSL-issued credential. The typical scenario is that an End User accesses a Relying Party website and chooses to login with an NSL-issued credential. The Relying Party website redirects the End User to NSL using a SAML authentication request message. The End User then logs in to NSL and after successful authentication of the End User's credential, Symantec re-directs the End User back to the Relying Party website with a SAML assertion response message. NSL's SAML Authentication complies with the requirements specified in the FICAM SAML 2.0 Web Browser SSO Profile (for more information, please see http://www.idmanagement.gov/sites/default/files/documents/SAML20_Web_SSO_Profile.pdf).

iii) Single Sign-on is provided by NSL to enable an End User, who has successfully authenticated to a Relying Party website, to access another Relying Party website without repeating the login process. Unless a logout request is received from a Relying Party website, NSL maintains the authentication status of an End User for a fixed period of time. If a SAML authentication request message is received by NSL for that End User during that time period, NSL returns a success SAML authentication response message to the Relying Party website and the End User is authenticated without having to re-login to NSL.

B. End User Identity Credentials

NSL issues two types of End User identity credentials: Basic and Enhanced.

- The Basic End User credential consists of a username (the End User's email address) and a password. A Basic End User credential is issued only after the End User has successfully completed remote online identity proofing through Symantec's Identity Proofing Agent at Assurance Level 2 ("AL2," as defined in the NIST Publication).
- The Enhanced End User credential consists of a username (the End User's email address), a password, and a one time password ("OTP") message (provided either by the VIP mobile application, SMS, or voice message) that is sent to an End User's cell phone for use as a second authentication factor when the End User logs into a Relying Party website or application that accepts a NSL-issued credential. The OTP is a part of Symantec VIP Service, which is a component of the NSL Service. The Enhanced End User credential is issued only after the End User has successfully completed remote online identity proofing through Symantec's Identity Proofing Agent at Assurance Level 3 ("AL3," as defined in the NIST Publication).

C. Remote Identity Proofing

The NSL Service utilizes a third-party FICAM-compliant remote identity proofing service provided to Symantec by the Identity Proofing Agent. The Identity Proofing Agent operates an identity proofing service that is remotely accessed by NSL. The internet link from the NSL service to the Identity Proofing Agent's identity proofing service is protected by an SSL certificate so that all data communicated over the link is encrypted.

Before the identity proofing process is initiated with the Identity Proofing Agent, an End User must opt-in and agree to the use of his/her identity data. The remote identity proofing service utilizes two services of the Identity Proofing Agent to make an identity proofing decision. The identity proofing decision is based on a comparison of identity information provided by an End User against information in his/her credit records and also his/her responses to knowledge-based questions generated from information in credit records and other databases of the Identity Proofing Agent. Upon successful completion of the identity proofing process, the Identity Proofing Agent returns a transaction ID and date/time stamp to NSL. The Identity Proofing Agent maintains audit records related to the identity proofing transaction, and NSL records the transaction ID and associated date/time stamp.

D. Out-of-Band Authentication

The Out-of-Band Authentication is a component of the Symantec VIP Service (itself a component of the NSL Service) that sends an OTP message to an End User's cell phone, either via the VIP mobile application, SMS message or voice message, to be used as a second factor for authentication of the End User's identity. This Out-of-Band Authentication is required for AL3 and optional for AL2. When an End User with an Enhanced identity credential logs into NSL, a two-factor authentication is performed. First, the End User's password is compared to the password stored in the End User's account, and then an OTP message is sent to the End User's registered cell phone either by the VIP mobile application, SMS or voice message. The End User must enter the OTP value into the login page. The OTP value is then sent to the VIP Service, which compares the End User-entered value with the value sent in the message and returns a valid or invalid message to NSL.

E. NSL Service Editor

The NSL Service Editor is a feature of NSL that is used by an NSL Administrator to register, configure and manage Relying Party accounts. Each Relying Party that chooses to accept NSL-issued credentials must register and obtain an account with the NSL Service. Each Relying Partying must securely exchange technical information (referred to as metadata) with NSL that includes URLs and digital certificates used for link protection and the signing of SAML messages. The NSL Administrator uses the NSL Service Editor to load the Relying Partying metadata into NSL.

Customer Responsibilities

Symantec can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, Symantec's performance of the Service may be delayed, impaired or prevented, as noted below.

- Setup Enablement: Customer must provide information required for Symantec to begin providing the Service. Specifically, Customer must provide valid metadata for Customer's production environment before Symantec can begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.

Customer Service-Specific Warranties

- Customer represents and warrants to Symantec that Customer: (i) has reviewed the NSL Credential Policy and understands the obligations of a Relying Party, and (ii) will use commercially reasonable efforts to comply with the obligations of a Relying Party as set forth in the NSL Credential Policy.
- Symantec's End User Terms of Service are included in the user interface for the Service, in such a way that End Users may not proceed through the NSL credentialing process without agreeing to the End User Terms of Service first. Customer represents and warrants that it will not interfere, alter, or disrupt any user interface containing the Symantec End User Terms of Service or interfere with the End User's ability to review and accept the End User Terms of Service. Customer will defend and indemnify Symantec against all claims and damages to Symantec caused by Customer's breach of this End User Terms of Service warranty.
- Customer represents and warrants that it will not make any false or misleading representations, warranties or guarantees with regard to Symantec, the Service or the NSL credentials.

Assistance and Technical Support

Customer Assistance**.** Symantec will provide the following assistance a part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support**.** The following technical support ("Support") is included with the Service.

- Support available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to resolve reported problems with the Service.

Maintenance. Symantec must perform maintenance from time to time. The following applies to such maintenance:

- *Planned Maintenance*. For Planned Maintenance, Symantec will use commercially reasonable efforts to give Customer seven (7) calendar days' notification, via email, SMS, or as posted on the Service Management Console ("SMC"). Symantec will use commercially reasonable efforts to perform Planned Maintenance at times when collective customer activity is low, in the time zone in which the affected Infrastructure is located, and only on part, not all, of the network. If possible, Planned Maintenance will be carried out without affecting the Service. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance in order to minimize disruption of the Service.

- *Emergency Maintenance.* Where Emergency Maintenance is necessary and is likely to affect the Service, Symantec will endeavor to inform the affected parties in advance by posting an alert on the applicable SMC no less than one (1) hour prior to the start of the Emergency Maintenance.

- *Routine Maintenance (SMC).* Symantec will use commercially reasonable efforts to perform routine maintenance of SMCs at times when collective Customer activity is low to minimize disruption to the availability of the SMC. Customer will not receive prior notification for these routine maintenance activities.

- Purchase of the NSL Service includes Support as described above. Support is provided and performed subject to the Support Terms as described in the certificate confirming customer's purchase of the NSL Service. All references to "Software" in the Support Terms shall be deemed references to the NSL Service, as applicable; provided, however, that any terms or deliverables in the Support Terms specific to software only shall not apply to support for the NSL Service.

- Support to Customer may be limited if Customer is using or working on an application that is not identified by Symantec as a "supported application" or if Customer is using an implementation of the NSL Service that was not installed or configured using Symantec processes.

SERVICE-SPECIFIC TERMS

No Auto-Renewal

Notwithstanding anything to the contrary in the Agreement, there is no automatic renewal of the NSL Service. Before the NSL Service expires, Customer must contact Symantec or its channel reseller partner to renew.

Rights Granted

Symantec Trademarks License Grant

- The marks "Symantec" and "Norton", either the word marks, the Symantec or the Norton logo, the applicable Symantec NSL Service trademarks and any other trademarks and service marks adopted by Symantec to identify the NSL Service (collectively, the "Symantec Trademarks") belong to Symantec. During the Term of the NSL Service, Customer shall have a non-exclusive, non-transferable license to use and display the Symantec Trademarks, solely in conjunction with Customer's use or promotion of the NSL Service and its acceptance of NSL credentials, and subject to Customer's compliance with Symantec's then-current trademark usage guidelines (the "Trademark Guidelines"). Customer will have no rights in such Symantec Trademarks except as expressly set forth herein and as authorized in writing by Symantec from time-to-time. Customer agrees not to use the Symantec Trademarks as any portion of Customer's trade name or trademark for its business, services or other products. Any goodwill in the Symantec Trademarks that results from Customer's use shall inure solely to the benefit of Symantec. Customer shall promptly cease or suspend use of Symantec Trademarks if Symantec notifies Customer in writing that the use of the Symantec Trademarks does not comply with Symantec's Trademark Guidelines.
- Symantec grants no rights in the Symantec Trademarks or in any other materials, trademark, trade name, service mark, business name or goodwill of Symantec except as licensed hereunder or by separate written agreement of the parties. Customer agrees that it will not at any time during the Term of the NSL Service or after the expiration or termination of the applicable Services Order assert or claim any interest in or do anything that may adversely affect the validity of the Symantec Trademarks or any other materials, trademark, trade name or product designation belonging to or licensed to Symantec (including, without limitation registering or attempting to register any trademark or copyright incorporated in the Symantec Trademarks).
- No Confusing Use. Customer will not use any trademark, trade name or product name confusingly similar to a trademark, trade name or product name of Symantec.
- No Continuing Rights. Upon expiration or termination of the NSL Service, Customer will immediately cease all display and use of the Symantec Trademarks and will not thereafter use, advertise or display any trademark, trade name or product designation which is, or any part of which is, similar to or confusing with any Symantec Trademarks or with any other materials, trademark, trade name or product designation associated with Symantec or any Symantec service or product.

Service Conditions

- In order for Symantec to perform the NSL Service, End Users enrolling for a NSL credential must have a cell phone that is able to receive SMS or voice messages, an unlocked credit file at the consumer credit bureau of the Identity Proofing Agent and a residential address in the United States.
- For enhanced reliability and security, the NSL Service is hosted in Symantec data centers located in the United States. The NSL Service shares common network and security infrastructure with other Symantec authentication services. The NSL Service is operated by Symantec personnel in accordance with the NSL Credential Policy.

- All significant events are recorded by NSL on a transaction-by-transaction basis. Details of identity proofing transactions are recorded by the Identity Proofing Agent, and all OTP generation and validation events are recorded by the Symantec VIP Service, as a component of the NSL Service. All records are time-stamped.
- Customer may represent itself as a Relying Party, but Customer must not represent that it is otherwise affiliated with Symantec. Customer is authorized to represent only such facts about NSL and the NSL credentials as Symantec posts on its website and in other published materials.
- You may not disclose the results of any benchmark tests or other tests connected with the Service to any third party without Symantec's prior written consent.
- Except as otherwise specified in the Service Description, the Service may use open source and other third party materials that are subject to a separate license. Please see the applicable Third Party Notice, if applicable, at http://www.symantec.com/about/profile/policies/eulas/.
- Symantec may update the Service at any time in order to maintain the effectiveness of the Service.
- Customer may not integrate the NSL Service, in its entirety or any of its components, with any other software or service unless expressly agreed by Symantec in writing, or unless otherwise expressly licensed by Symantec to Customer.
- **Disclaimers:** 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 (the "Network"). SYMANTEC SHALL NOT BE LIABLE FOR ANY INTERRUPTION, DELAY, SUSPENSIONS, AND OTHER ACTS AND/OR OMISSIONS BY SUCH THIRD PARTIES THAT ARE NOT WITHIN SYMANTEC'S CONTROL.

SERVICE LEVEL AGREEMENT

Up Time is calculated on a rolling 90-day basis as a percentage equal to: (i) the total number of minutes in any such 90-day period that the NSL Service is available and capable of receiving and processing data from customers, divided by (ii) the total number of minutes in such period. Symantec's Up Time percentage for the NSL Service throughout each such 90-day period will be no less than ninety-nine percent (99%). This service level agreement will not operate during any SLA Exclusion Periods.

DATA PRIVACY NOTICE

Automatically Collected and Transmitted Data. The Service collects from Customer's environment and automatically transmits to Symantec data, which may include, without limitation, Customer's certificate, DNS, URL and public key information ("Transmitted Information"). The Transmitted Information will be used for the purposes of: (i) establishing an online connection between Customer and Symantec and (ii) encrypting data to be sent between Customer and Symantec.

Technical Support. In the event that Customer provides information to Symantec in connection with a technical support request ("Technical Support Information"), such information will be processed and used by Symantec for the purpose of providing the requested technical support, including performing error analysis.

Sharing and Transfer. The Transmitted Information and the Technical Support Information (collectively, the "Collected Information") may be transferred to Symantec Corporation, its affiliates and contractors in the United States or other countries that may have less protective data protection laws than the region in which Customer is situated (including the European Union) and will be stored and processed manually and electronically through global systems and tools for the purposes above. The Collected Information may be accessible by Symantec employees or contractors on a need-to-know basis, exclusively to be used in accordance with the purposes described above. For the same purposes the Collected Information may be shared with partners and vendors that process information on behalf of Symantec. Symantec has taken steps so that the Collected Information, if transferred, receives an adequate level of protection.

Customer's Obligation to Personal Information. It is Customer's responsibility to ensure that any disclosure by Customer to Symantec of personal information of Customer's users or third parties is in compliance with national laws governing the collection, use and protection of personal information applicable to Customer's country or region of operation. In particular, it is Customer's responsibility to inform users and third parties that Customer are providing their information to Symantec, to inform them of how it will be used and to gather appropriate consents required for such transfer and use.

Disclosures to Law Enforcement. Subject to applicable laws, Symantec reserves the right to cooperate with any legal process and any law enforcement or other government inquiry related to Customer's use of the Service. This means that Symantec may provide documents and information relevant to a court subpoena or to a law enforcement or other government investigation.

Contacting Symantec about Customer's Privacy. For any inquiry about in the Collected Information or about Symantec's privacy policies, please contact Symantec at privacy@symantec.com.

DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Services Description, have the meaning given below:

"Customer" means a party that is acting as a Relying Party under the Agreement and the applicable executed Services Order.

"**Emergency Maintenance**" means unscheduled maintenance periods which during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure or any maintenance for which Symantec could not have reasonably prepared for the need for such maintenance, and failure to perform the maintenance would adversely impact Customer.

"End User" means an individual that has opted-in, successfully completed identity proofing and been issued a valid NSL credential.

"**End User Terms of Service**" means the terms and conditions provided by Symantec to the End User of the NSL Service, which the End User must accept prior to proceeding with the NSL credential process.

"**Identity Proofing Agent**" means Symantec's third party service provider responsible for performing remote identity proofing of individuals enrolling for a NSL credential.

"**Infrastructure**" means any Symantec or licensor technology and intellectual property used to provide the Service.

"**NSL Administrator**" means a Symantec employee responsible for registering and managing Relying Party accounts and administering End User accounts.

"NSL Credential Policy" means the then-current NSL Credential Practices Statement as set forth in the repository on http://www.symantec.com/about/profile/policies/repository.jsp, as may be amended from time to time.

"**Planned Maintenance**" means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure.

"Relying Party" means an entity that accepts an NSL credential for authentication at such entity's website or application.

"SLA Exclusion Periods" means any of the following events: (i) periods of Planned Maintenance or Emergency Maintenance; (ii) periods of non-availability due to force majeure or acts or omissions of either Customer or a third party; (iii) periods of suspension of the NSL Service by Symantec in accordance with the terms of the Agreement; (iv) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (v) Customer has not configured the NSL Service in accordance with the Agreement.

"**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligations related to the Service: a Symantec Certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes or follows the Service.

"Support Terms" means Symantec's then-current technical support terms, policies and processes.

"Up Time" means the percentage of time that Symantec's systems are available and capable of receiving and processing data from customers in connection with the Service, excluding any SLA Exclusion Periods.

END OF SERVICE DESCRIPTION