Norton™ Secure Login Service

Credential Practices Statement (CrPS)

Version: 1.2

July 2014

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
+1 650.527.8000
www.symantec.com

Trademark Notices

TABLE OF CONTENTS

1. Introduction

1.1 Overview

Norton™ Secure Login (NSL) is a cloud-based identity service that provides identity proofing, credential issuance, credential validation, and single sign-on services. 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). The NSL service performs identity proofing and issues credentials at Assurance Levels 2 and 3 as defined in National Institute of Standards and Technology (NIST) Special Publication 800-63-2. In addition, the NSL service supports the identity federation concept defined in the National Strategy for Trusted Identities in Cyberspace (NSTIC).

Intended End Users of the NSL service include individual consumers or business representatives needing identity credentials for authentication at government or commercial websites. End Users of the NSL service receive federated 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 user credentials needed for access to their websites and applications.

1.2 Document Identification

This document is the Credential Practices Statement (CRPS) for the Norton Secure Login service. .

This document identifies policies for the issuance of identity credentials and the exchange of SAML messages with RPs in accordance with the *"FICAM SAML 2.0 Web SSO Profile*". The NSL service supports the following assurance levels distinguished by the corresponding FICAM-specified LOA URLs:

Assurance Level 2 (AL2)..... *http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel2*
Assurance Level 3 (AL3)..... *http://idmanagement.gov/icam/2009/12/saml_2.0_profile/assurancelevel3*

1.3 NSL Roles

This section provides a brief description each NSL role. The specific obligations of each role are more fully discussed later in this CRPS.

1.3.1 End User

An ***End User*** is an individual that has opted-in, successfully completed Identity Proofing and been issued a valid NSL identity credential.

1.3.2 Credential Service Provider

The ***Credential Service Provider*** provides user registration, credential issuance and authentication and single sign-on services for NSL credentials. Symantec, as the operator of the NSL service is the Credential Service Provider.

1.3.3 Relying Party

A ***Relying Party*** is an entity that accepts a NSL identity credential for authentication at a website or application. Each Relying Party that chooses to accept NSL-issued credentials must register and obtain an account with the NSL service.

1.3.4 Identity Proofing Agent

The ***Identity Proofing Agent*** is the third party entity responsible for performing remote Identity Proofing of individuals enrolling for a NSL identity credential. Symantec contracts with Identity Proofing service providers that have been certified by Kantara at Assurance Level 3.

1.3.5 NSL Administrator

The NSL Administrator is a Symantec employee responsible for registering and managing Relying Party accounts and administering End User accounts.

1.4 Credential Usage

A NSL credential is used by an End User to authenticate to a Relying Party website or application. A Relying Party specifies the Assurance Level (AL) required for authentication at its website or application. Typical usage for NSL credentials is as follows:

- The *Basic* credential is appropriate for use where strong Identity Proofing and a single factor authentication are required. The *Basic* credential is used for authentication at a Relying Party website that requires AL2.
- The *Enhanced* credential is appropriate where strong Identity Proofing and two-factor authentication is required. The *Enhanced* credential is used for authentication at a Relying Party website that requires AL3. An example of an appropriate use case for the *Enhanced* credential is remote access to personally identifiable data (PII) data on a Federal government website.

SAML assertions must be processed by the Relying Party in accordance with the *"FICAM SAML 2.0 Web SSO Profile"*. The authentication assertion exchanged using SAML 2.0 must never be used to give an End User access to an application with a higher AL requirement than is present in the assertion.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Symantec Corporation
350 Ellis Street
Mountain View CA 94043 USA

1.5.2 Contact Information

Norton Secure Login Product Manager
c/o Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA

+1 (650) 527-8000 (voice)
+1 (650) 527-8050 (fax)
practices@symantec.com

1.5.3 CRPS Approval Procedure

Symantec has established a Policy Management Authority (PMA) consisting of Manager-level members from cross-functional teams with authority and responsibility for the technical, operational, functional, and security aspects of the NSL service. This management body serves to formally review and approve proposed amendments to this Norton Secure Login CRPS document.

1.5.4 CRPS Amendment Procedure

Symantec reserves the right to revise this Norton Secure Login CRPS at any time without advance notice so long as the amendments are, in Symantec's sole discretion, not material (e.g., without limitation, corrections of typographical errors, changes to URLs, wording clarification that serve to retain the original meaning, changes to contact information and the like).

Symantec will directly notify End Users and Relying Parties of material changes in the Norton Secure Login Service CRPS. Symantec will send an email notice to End Users at the unique email address associated with their account. Notification shall occur at least fifteen (15) days prior to the effective date of the changes to allow End Users the opportunity to cancel their subscription, if so desired. Continued use of the Norton Secure Login Service after the fifteen (15) days shall constitute acceptance of the changes.

Symantec will solicit feedback and comments to proposed revisions of a material nature from Relying Parties. The comment period for any material revisions to the CRPS shall be fifteen (15) calendar days, starting on the date on which the Relying Parties are notified of the proposed revisions. Symantec shall consider all feedback and comments received and shall either (a) allow the proposed revisions to become effective without amendment; (b) adopt the solicited feedback by integrating into the proposed revisions and adopt the changes; or (c) withdraw the proposed revisions.

Unless the proposed revisions are amended or withdrawn, they shall become effective upon the expiration of the comment period. Revisions supersede any designated or conflicting provisions of the referenced version of the CRPS.

3. NSL Credential Enrollment and Issuance

3.1 Process Overview

The following describes the step by step process for user registration and credential issuance.

Step 1: An End User accesses a Relying Party website and chooses to login using a NSL credential. The End User is re-directed to NSL with a SAML request for authentication at AL2 or AL3.

Account Creation:

Step 2: If the End User does not already have a *Basic or Enhanced* credential, the End User must first create a Norton account by entering an email address and choosing a password at the Norton Account Sign Up page. Prior to submitting the email address and password, the End User must read and agree to the NSL End User Agreement.

Step 3: After the End User submits their email address and password, NSL sends a message to the End User's email address to confirm the validity of the email address. The message contains a link to a NSL webpage used for verifying an email address. When the user accesses the link, NSL verifies the email address and activates the End User account. The End User is then directed to the NSL login page for Identity Proofing.

Identity Proofing:

Step 4: The End User logs into their account using the verified email address and password and is directed to the Identity Proofing page. For AL2, the End User must enter identity information. For AL3, the End User must enter identity information as well as a valid credit card number and a cell phone number.

Step 5: NSL sends the End User identity information to the Identity Proofing Agent where the user identity data is compared to information in the End User's credit record. At AL3, the Identity Proofing Agent also confirms that the name and address associated with the credit card record matches the name and address contained in the End User's credit record.

Step 6: The Identity Proofing Agent then returns a set of multiple-choice knowledge-based questions derived from information in the credit and non-credit records.

Step 7: The End User answers the questions and the answers are forwarded to the Identity Proofing Agent. The Identity Proofing Agent determines whether the End User has passed the Identity Proofing.

Step 8: The Identity Proofing Agent returns to NSL an Identity Proofing result (success or failed) and a time-stamped Transaction ID.

Credential activation:

Step 9: At AL2 after successful Identity Proofing, the End User's *Basic* credential is activated and the End User is re-directed back to the Relying Party website with a SAML message asserting that the End User has been authenticated at AL2.

Step 10: At AL3 after successful Identity Proofing, the Identity Proofing Agent mails a letter to the End User to confirm the End User's postal address. The letter contains a Transaction ID and a URL for a link at NSL where the user must enter the Transaction ID to initiate the process for activating the End User's *Enhanced* identity credential.

Step 11: After the user logs in at the specified URL and enters the Transaction ID, NSL sends a SMS or voice message to the End User's cell phone. The message contains a one-time password (OTP) that the user must enter at the NSL login webpage. If the OTP entered by the user matches the OTP sent by NSL, the End User's Enhanced credential is activated and the End User is re-directed to the Relying Party website with a SAML message asserting that the End User has been authenticated at AL3.

Thereafter, the End User may authenticate to the Relying Party website without repeating the Identity Proofing and activation steps. This registration process is further described in the subsections following.

3.2 Initial Registration

NSL accepts enrollment requests from individuals and needing an AL2 or AL3 identity credential for authentication at government or commercial websites or applications. The End User (Subscriber) enrollment process consists of:

- Creating an account at NSL with a username (email address) and password,
- Demonstrating ownership/control of the email address,

- Providing identity information for AL2; or at AL3, providing identity information, a financial account (credit card) number, and a cell phone number,
- Successfully completing remote Identity Proofing at AL2 or AL3
- Activating an AL2 (single-factor) *Basic* identity credential or activating a (two-factor) *Enhanced* identity credential,
- Verifying possession of a valid cell phone number with the capability to receive an SMS or Voice OTP message to be used as the second factor for authentication of the *Enhanced* identity credential.

3.2.1 Account Creation

The Subscriber first creates an account at NSL by entering the following information:

- Country (currently restricted to United States only)
- First and Last Name
- Email Address (used as the username)
- Password (minimum of 8-alphanumeric characters). The password is entered twice to ensure accuracy.

All Subscribers shall agree to the terms and conditions contained within the NSL End User Agreement. Account creation does not proceed until the Subscriber has agreed to the NSL End User Agreement.

The Email Address serves as the Subscriber unique identity and is validated by NSL to be unique within the NSL service's user domain, including identities of previously terminated or revoked Credentials other than re-assignment to the same Subscriber.

NSL confirms the Subscriber's email address is valid and associated with (bound to) the individual Subscriber by sending an email message to the Subscriber that contains a URL with a validation code. Upon receipt of the email message, the Subscriber responds to the message by clicking the link contained within the message and is directed to the NSL email verification page. NSL verifies the code contained in the URL, and creates the Account.

3.2.2 Identity Proofing

Identify proofing commences only following successful Account Creation. By acceptance of the NSL End User Agreement, the Subscriber has effectively opted-in to the Identity Proofing process and agreed to allow use of their personal identity data for NSL Identity Proofing.

The Subscriber must provide additional information required for Identity Proofing to receive either an AL2 and/or AL3 Credential as set forth in Appendix A:

An End User may possess both an AL2 and AL3 Credential simultaneously within their account.

3.2.3 Credential Activation

Credential activation commences only following successful Identity Proofing. Once "*Activated*", the Credential can be used for authentication at Relying Party resources in accordance with the NSL End User Agreement and this CRPS.

3.2.3.1 Basic Credential (AL2)

The ***Basic*** Credential consists of a username (email address) and password established by the Subscriber and provides single-factor authentication.

Activation of the *Basic* Credential is contingent upon successful Identity Proofing at Assurance Level 2 (AL2).

3.2.3.2 Enhanced Credential (AL3)

The ***Enhanced*** Credential consists of a username (email address) and password combination as well as a SMS or Voice OTP. The NSL *Enhanced* Credential provides two-factor authentication.

Activation of the *Enhanced* Credential is contingent upon:

- successful Identity Proofing at Assurance Level 3 (AL3),
- successful binding of the Subscriber to the Account postal address, and
- successful binding of the Subscriber to the Account cell phone number via SMS or Voice OTP.

Upon successful Identity Proofing, the NSL generates a hardcopy message containing a Transaction ID and URL that is addressed and mailed to the Subscriber's postal address. Upon receipt, the Subscriber must go online to the designated URL, log in using their account username and password and enter the Transaction ID. This successfully binds the individual to the postal address within the Account.

Upon the Subscriber entering the correct Transaction ID, NSL transmits an SMS or Voice message containing a one-time password (OTP) to the Subscriber's cell phone. Upon receipt, the Subscriber must enter the OTP on the authentication webpage. If the entered OTP matches that which was transmitted by NSL, authentication is successful and complete. This successfully binds the individual to the cell phone number within the Account and the *Enhanced* Credential is "*Activated*".

The SMS and Voice OTPs are issued by the Symantec Out-of-Band Authentication Service, a component of the Symantec VIP Service. The Symantec VIP Service is operated in accordance with the Symantec VIP Authentication Network Policy published at *www.symantec.com/about/profile/policies/repository.jsp*

3.3 Credential Validity Period

An NSL Credential has a validity period of 5 years. After 5 years, the End User must enroll for a new credential and repeat the Identity Proofing process.

4. Credential Validation and Identity Assertion

The End User uses the NSL Credential for authentication to a Relying Party website.

4.1 Credential Validation Process

A Relying Party website may present multiple options for End User login/authentication. Upon selecting Norton Secure Login, the End User is redirected to the NSL login page for credential validation.

Two types of user identity credentials can be presented by the End User for validation.

- *Basic* credential – the End User submits a username and a password (single factor authentication) which is compared to a username/password combination for a user account.
- *Enhanced* credential – the End User submits two factors of authentication as follows:

1) a username/password combination is compared to a username/password combination for a user account. Upon a successful match, an SMS or Voice OTP message is sent to the user's registered cell phone in the account.
2) The End User receives the SMS or Voice message on their cell phone and enters the OTP value in the message into the User Login page. The entered value is transmitted to the Out-of-Band Authentication Service to compare against the OTP value sent to determine if it is a successful match.

An unsuccessful login results if the End User exceeds the threshold of login attempts in accordance with section 5.2.3.

Upon completion of the Credential Validation process, NSL re-directs the End User back to the Relying Party webpage with a SAML 2.0 assertion response message containing an HTTP Post transmission indicating either success or failure result of the validation of the End User Credential.

NSL returns a set of attributes within the successful identity assertion message including the End User's firstname, lastname, email address, home address, phone number and Assurance Level. The unique NSL identifier is also transmitted.

4.2 Security of Protocols

The result of the End User Login is transmitted to the Relying Party as a SAML 2.0 Assertion via an HTTP Post transmission. SAML2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about the End User between the NSL service and the Relying Party web service to enable secure web-based authentication and authorization at the RP web page. Each SAML assertion is unique to a single transaction.

The SAML 2.0 assertion is digitally signed using a certificate issued from a Symantec Non-Federal SSP CA cross-certified with the Federal Bridge PKI. HTTP Post transmission occurs over a certificate-based mutually-authenticated SSL session.

At Relying Party Registration, the Relying Party exchanges meta-data with NSL that includes the URLs and authentication certificates used in HTTP Post transmissions. Relying Party Registration also requires the Relying Party's acceptance of the "Norton Secure Login Service Terms and Conditions".

4.3 Accuracy and Reliability

Should the NSL service experience a system failure during a NSL Credential Validation event, no assertion will be transmitted.

4.4 Assertion Lifetime

The SAML assertion has a lifetime of ten (10) minutes. The SAML assertion may be used for single sign-on with the NSL Relying Parties within the minute period following the time of creation of the SAML assertion.

5. Credential Lifecycle

The NSL Credential may transition to different states/statuses as a result of events and actions. The NSL Credential may have the following states over its lifetime:

- Pending
- Activated
- Locked
- Revoked

5.1 Latency and Availability of Credential Status

A change in Credential status is instantaneously made available within the NSL service.

5.2 Lifecycle Events

The following subsections describe events that occur over the lifecycle of the Credential and the effect (if any) on the state/status of the Credential and if/how such status affects the operation of the Credential.

5.2.1 Credential Activation

The NSL Credential is placed in "*Activated*" state in accordance with section 3.2, initial registration. Activation is the process of binding the End User to the Account information (i.e., email address, postal address, cell phone #).

5.2.3 Failed Login

The Subscriber Account is '*Locked'* if too many consecutive failed authentication attempts have been made at the NSL Login page. NSL uses the following mechanism for blocking brute force guessing of username and passwords..

If there are more than five unsuccessful login attempts for the same username or from the same IP address, system will show a CAPTCHA to the user in order to slow down the process and to block any automatic programs to attack the system by guessing usernames and passwords. Once the cumulative number of unsuccessful login attempts reaches ten for the same username, the account is blocked for an hour. Fifty unsuccessful attempts within an hour from same IP address (with likely several usernames) will also result in blocking that IP address for one hour.

Additionally, SMS and Voice OTP have a configurable validity window, defaulted to eight (8) hours. NSL uses a configurable threshold for authentication attempts, not to exceed ten (10) within the validity window of the SMS or Voice OTP. The issuance of OTPs has a threshold limit of no more than ten (10) per hour and an OTP is only sent upon the End User entry of a valid username/password.

If the login attempt threshold is exceeded, the NSL responds with a message stating that login has failed and the Account has been locked. An unsuccessful login returns an authentication failure via SAML assertion to a Relying Party webpage. The Account remains in '*Locked'* state for a one hour period following the Lock event during which the NSL Credential cannot be used in authentication.

To avoid locking the Account, the End User may reset their password as set forth in section 5.2.5.

5.2.4 Modify Account Information

The End User may modify their Account information to reflect real-world changes. The End User authenticates to their NSL Account using the associated *Basic* or *Enhanced* Credential corresponding to the Account information. The stored End User Account information that is available for modification is specific to the assurance level of the Credential as follows:

Level of Assurance	End User Account Information
AL2 *Basic* Credential	First and Last Name
	Email address (username)
AL3 *Enhanced* Credential	First and Last Name
	Email address (username)
	Postal Address (street, city, state and postal zip code)
	Phone number
	Cell phone number

If the End User modifies their Account information, he or she must repeat Identity Proofing as set forth in section 3.2.

5.2.5 Reset Password

The End User may choose to reset their password at any time by logging on to their NSL Account and entering their new password twice.

5.2.6 Lost/Stolen/Forgotten Password

The End User may reset their Password, if it is lost, stolen or forgotten, by clicking the "Forgot Password" link. NSL searches for a match of a Norton Account to the username (email address) entered, generates a random password for the Account, and sends an email message to the End User email address.

The email message contains a notice of the password reset together with the generated random password. Upon receipt of the random password, the End User logs into their account using the random password and repeats Identity Proofing as per initial registration as set forth in section 3.2. Upon successful Identity Proofing, the End User changes their password from the random password to one of their own choosing.

5.2.6 Revocation

Revoking a NSL Credential changes the state of the Credential from "*Active"* to "*Revoked"*. A *Revoked* Credential is deemed invalid for all Relying Party authentication (preventing it from being used).

5.2.6.1 Circumstances Requiring Revocation

The following individuals may request revocation of a Credential for situations that warrant the *Revocation* of a NSL Credential as follows:

- End User –After receipt of an e-mail notification from NSL or a postal mail notification from the Identity Proofing Agent, the End User may report that an Identity Proofing was falsely performed.
- Law Enforcement – law enforcement representative may present a court order or other legal documentation in support of a need to prohibit use of a NSL Credential.

- Credential Service Provider – Symantec may revoke a credential in its sole discretion, based on suspicious activity detected by the NSL service that deems that a user account is compromised (for example, based on information from security logging, etc.).

5.2.6.2 Revocation Process

Revocation is supported through the following scenarios.

- Revocation by End User.

  An End User initiates a request for revocation of a NSL Credential by contacting NSL Customer Support by telephone at the 800 number provided for Norton Product Support. To authenticate their identity to Symantec, the End User must provide information from the previously received Identity Proofing confirmation letter including their name, address, email address and transaction ID. NSL Customer Support agent files a ticket containing the information provided by the End User.

  The ticket is assigned to the NSL Administrator. Upon receiving the ticket, the NSL Administrator searches for the account information provided within the ticket and compare the information in the ticket against the information in the NSL user database. If all data matches, the NSL Administrator deletes the account and the ticket is closed. All revocation requests received by the NSL Administrator will be processed within 24 hours.

- Revocation by Law Enforcement for reasons of unlawful activity.

  A law enforcement representative is required to submit legal documentation supporting the revocation request in the form of a court order, or equivalent, stating that an Account is being used for malicious or unlawful purposes. Symantec establishes the authority/authorization of the representative and the legal process/reason for revocation through consultation with management and legal counsel, as appropriate.

  Once the request has been authorized as legitimate, a notice is sent to NSL Customer Support to file a ticket containing the information provided identifying the account(s) to be revoked (i.e. email address).

  The ticket is assigned to the NSL Administrator. Upon receiving the ticket, the NSL Administrator verifies that the originator of the ticket is a representative of the Information Security team. The NSL Administrator searches for the account information provided within the ticket and upon locating an account match, the account is deleted and the ticket is closed.

- By Symantec for reasons of suspicious activity.

  Symantec performs security reviews on logs to detect any suspicious activity. Upon identifying malicious or suspicious activity, the offending account is flagged for revocation. The security reviewer files a ticket containing account information identifying the offending account(s) to be revoked (i.e. email address).

  The ticket is assigned to the NSL Administrator. Upon receiving the ticket, the NSL Administrator verifies that the originator of the ticket is a representative of the Information Security team. The NSL Administrator searches for the account information provided within the ticket and upon locating an account match, the account is deleted and the ticket is closed.

Records are retained in the ticketing system in accordance with section 6.3.

6. Facility and Operational Controls

6.1 Physical Controls

6.1.1 Physical Access Controls

The NSL service is hosted and operated in the same secured data facilities as other Symantec authentication services. Such Symantec operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

Symantec also maintains a disaster recovery site for NSL operations. Symantec's disaster recovery facility is protected by physical security comparable to those of Symantec's primary facility.

6.1.2 Secure Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal.

6.2 Procedural and Personnel Controls

6.2.1 Security Roles and Responsibilities

6.2.1.1 Trusted Roles Requirement

The roles and responsibilities for personnel for each service-related and security-relevant task of the NSL service are documented. Certain security-critical roles that have the capacity to materially affect trust in NSL Credentials are identified as Trusted Roles.

Trusted persons include, but are not limited to:

- customer service personnel,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

Trusted persons must successfully complete background screening requirements.

6.2.1.2 Roles and Responsibilities

Within the context of trusted positions, Symantec defines the following security-relevant roles to securely and efficiently operate and manage the data center operation. Individuals assigned to one of these operational roles are not permitted to perform in another trusted role. Symantec maintains lists, including names, organizations and contact information, of those who act in these Trusted Roles, and makes them available during compliance audits.

Security-relevant roles include:

- *NSL Administrator* is responsible for registering and managing Relying Party accounts, and administering End User Accounts (including disabling inactive and expired accounts, revoking

credentials, etc.)

- *Engineering Maintenance and Escalation (EME)* is responsible for developing the NSL system initial setup/configuration, system accounts and all configuration changes. *EME* applies cryptographic checksum to all initial software and changes to the NSL system to ensure the integrity of all software code. EME-developed system initial setup/changes are provided to Production Services for upload to the NSL system.

- The *IT Audit Manager* reports to the Symantec *Director of Security*, who is in a department separate from engineering, operations and system administrators. The *IT Audit Manager* is responsible for overseeing the IT security audit including performing or overseeing internal compliance audits to ensure that the NSL service is operating in accordance with the CRPS.

- The *IT Security Officer* reports to the Symantec *Chief Information Security Officer*, who is in a department separate from engineering, operations and system administrators. The *Chief Information Security Officer* is responsible for managing IT Security Policy. The *IT Security Officer* is responsible for overseeing daily security of NSL operations including reviewing, maintaining and archiving audit logs.

- The *Operations* role is split across multiple roles for NSL and is fulfilled by teams of trusted individuals from the Symantec *Productions Operations* organization. Symantec Production Operations personnel are responsible for the routine operation of Symantec-hosted IT equipment, including system administration, system backups and recovery, database administration, and changing recording media. Multiple Symantec trusted employees perform this function through three operational shifts.

6.2.1.3 Persons Required per Task

The most sensitive operational and administrative tasks require at least two trusted employees. Multiparty control of NSL operations shall exclude personnel that serve in the Auditor Trusted Role.

The Symantec maintains an IT policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. No person assigned to a Trusted Role has more than one identity on the NSL system.

6.2.2 Personnel Qualifications

Symantec requires that personnel present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Established HR practices enforce all requisite position requirements when hiring and contracting personnel.

Symantec provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. Re-training is performed, as required, as new system functionality is deployed, or if there is any substantive change in NSL security or operational procedures. Symantec's training programs are tailored to the individual's responsibilities and records of such training are maintained. Symantec periodically reviews and enhances its training programs as necessary.

Any Symantec subcontractor employed in a position is held to the same functional and security criteria as if he or she were a full-time Symantec employee. All subcontractors shall comply with the requirements of this CRPS.

6.2.3 Staffing Levels

Symantec maintains adequate staffing levels to operate and maintain the NSL service on a 24/7 basis as set forth in this CRPS.

6.3 Event Logging

Symantec maintains a log of all relevant security events for the NSL service, together including a record of the time at which the event occurred. Automated log data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by Symantec personnel.

Symantec retains such records with appropriate protection and controls as set forth in section 6.5 to ensure successful retrieval as designated by Symantec Security Policy and as required by law.

6.3.1 Types of Events Recorded

NSL logs Credential Enrollment information including:

- User information, including unique username, of the End User submitting the Enrollment request
- Reference to the verification process performed and data and time of verification.
- Type and reference numbers(s) of documentation checked in Identity Proofing
- The Subscriber's acknowledgement of the terms and conditions of the End User Agreement prior to issuing the Credential.

NSL logs the following Credential Revocation information manually:

- The Requestor's full name
- The authority of the Requestor to revoke.
- The Subscriber identity associated with the credential being revoked
- The reason for revocation.

NSL logs Credential Lifecycle Event information including:

- Enrollment event and End User acknowledgement of End User Service Agreement
- End User Activation response event
- Lifecycle events: Modification, Lock, Revocation, etc.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Description/kind of entry.

6.3.2 Event Processing

The NSL servers and audit logs are continuously monitored to provide real time alerts of significant security and operational events. Real-time alerts are investigated by reviewing the audit logs for suspicious or unusual activity.

Audit log processing consists of a review of the audit logs and documentation of all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, an inspection of log entries for suspicious or unusual activity, and investigation of any alerts or irregularities identified in the logs. Actions taken based on audit log reviews are also documented.

6.3.3 Risk Assessments

Risk Assessments are conducted by Symantec to determine the application of controls to reduce threats to an acceptable risk level. Risk Assessments are conducted every 6 months

6.4 Records Protection and Retention

6.4.1 Data Protection

Logical and physical access controls as set forth in sections 6.1, 7.1 and 7.2 protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any credential data repositories or credential management processes.

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

Symantec protects archives so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The integrity of the information is verified when it is restored. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CRPS.

6.4.2 Retention Period of Archives

Records of the identity verification and revocation events are retained securely for a period of 7.5 years after the end of the End User's Account. The following End User personal information captured at verification is retained for 7.5 years from the end of the End User's Account: name, postal and email addresses and telephone number.

Electronic audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived for at least a period of 7.5 years following the date the Credential expires or is revoked.

6.5 Business Continuity

Symantec has created and maintains business continuity plans so that in the event of a business disruption, critical business functions may be resumed. Symantec maintains a Disaster Recovery Facility (DRF) located at a facility geographically separate from the primary Production Facility. The DRF meets the same Symantec's security standards as the primary data center facility.

Symantec maintains redundant hardware and backups of its NSL infrastructure system software at its disaster recovery facility. Symantec maintains offsite backups of important data for the NSL includes, but is not limited to: Subscriber Application data, audit data, and database records for all Credential issued.

In the event of a natural or man-made disaster requiring permanent cessation of operations from Symantec's primary facility, the Corporate Symantec Business Continuity Team and the Symantec Incident Management Team will coordinate with cross functional management teams to make the decision to formally declare a disaster situation and manage the incident. Once a disaster situation is declared, restoration of Symantec's Production services functionality at the DRF will be initiated.

Symantec has developed a Disaster Recovery Plan (DRP) for NSL services. The DRP identifies conditions for activating the plan and what constitutes an acceptable system outage and recovery time. The DRP defines the procedures for the teams to reconstitute Symantec NSL operations using

backup data and backup copies of the NSL Repositories. The target recovery time for restoring critical NSL Production service functionality is no greater than 24 hours.

6.6 Availability of Services

Symantec maintains redundant architecture and real time monitoring to ensure 99.0% service availability on a 24x7x365 basis. Service Availability refers to the up-time of the services excluding scheduled down-time and events occurring outside Symantec's span of control.

6.7 Termination of Services

In the event that it is necessary for the NSL service to cease operation, Symantec makes a commercially reasonable effort to notify End Users, Relying Parties, and other affected entities of such termination in advance of the termination. Symantec will develop a termination plan to minimize disruption to End Users, and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of an advance notice to End Users and Relying Parties affected by the termination with sufficient notice to obtain alternative Credentials from a successor Identity Provider,
- Revocation of unexpired unrevoked Credentials of End-User Subscribers,
- Protection and preservation of the archives and records for the time periods required in this CRPS,
- Refunding (if necessary) Subscribers whose active Credentials are revoked under the termination plan or provision, and
- Revocation of the Certificates used by the NSL components.

7. Technical Security Controls

7.1 Network Security

Symantec protects all communications of sensitive information through the use of encryption and digital signatures.
.

7.2 Computer Security Controls / Access Control

Symantec ensures that the systems maintaining NSL software and data files are secure om unauthorized access. Symantec implements system-level controls that provide for identification and authentication, discretionary access controls, and audit of security critical events. Symantec limits access to production servers to only those trusted individuals with an approved business reason for such access.

7.3 Key Management

The NSL service uses Public Key Cryptography Certificates for authentication, integrity and confidentiality of all transmissions exchanged between NSL components and Participants, including the ID Proofer and the Relying Party. SSL Certificates are issued by the Symantec Trust Network (STN) CAs governed by the policy and practices documented within the STN CP and CPS at www.symantec.com/about/profile/policies/repository.jsp

The SAML Assertion is signed by Certificate issued to NSL by the Symantec Non-Federal SSP PKI governed by the policy and practices documented within the Federal Bridge Certificate Policy and the Symantec Non-Federal SSP CPS at www.symantec.com/about/profile/policies/repository.jsp

NSL uses cryptographic modules that meet the requirements of FIPS 140-2 Level 1 or higher. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal.

7.4 Information Security Management and Lifecycle Controls

Symantec IT security policies and related procedures are established to govern the rules of operation of systems, and networks to ensure confidentiality, integrity and availability of information for NSL service. Risk assessments, as described in section 6.3.3, serve to ensure the completeness of security policies and that they are completely enforced.

8. Compliance Audit

8.1 Internal Service Audit

The NSL service shall undergo internal audits on at least an annual basis to monitor adherence to its CRPS requirements and to control its service quality. The audit shall be conducted by the Global Security Organization, a department separate and independent of the Engineering and Operations organization.

8.2 Independent Audit

Symantec shall undergo a Kantara Assessment conducted by a certified Kantara Assessor. Such assessments will be conducted on at least a two year basis to ensure conformity to the Kantara Initiative Service Assessment Criteria (SAC) at Assurance Levels 2 and 3.

Symantec shall retain records of conducted audits for a period of no less than 36 months. Such records are protected against unauthorized access, loss, alteration, public disclosure, or unapproved destruction in accordance with section 6.4.

9. Legal

For Legal stipulations, refer to the Service Description, the Terms of Service and End User Agreement documents for the Norton Secure Login product.

Glossary of Terms

TERM	DEFINITION
AL	See *Assurance Level*
Applicant	An individual or person acting as a proxy for a machine or corporate entity who is the subject of an Identity Proofing process.
Approved service	A certified service which has been granted an approval by the Kantara Initiative Board of Trustees.
Assertion	A statement from a verifier to a relying party that contains identity or other information about a subscriber.
Assessment	A process used to evaluate an electronic trust service and the service provider using the requirements specified by one or more Service Assessment Criteria for compliance with all applicable requirements.
Assurance Level (AL)	A degree of certainty that a claimant has presented a credential that refers to the claimant's identity. Each assurance level expresses a degree of confidence in the process used to establish the identity of the individual to whom the credential was issued and a degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four assurance levels are: Level 1: Little or no confidence in the asserted identity's validity Level 2: Some confidence in the asserted identity's validity Level 3: High confidence in the asserted identity's validity Level 4: Very high confidence in the asserted identity's validity
Attack	An attempt to obtain a subscriber's token or to fool a verifier into believing that an unauthorized individual possesses a claimant's token.
Attribute	A property associated with an individual.
Audit Organization	An organization which undertakes assessments of entities and their services to establish their conformity to or compliance with specific standards or other widely-recognized criteria. Specifically, in the context of the AAS, entities providing credentialing or identity management services which are claiming conformance to the
Authentication	Authentication simply establishes identity, not what that identity is authorized to do or what access privileges he or she has.
Authentication protocol	A well-specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.
Authorization	Process of deciding what an individual ought to be allowed to do.
Certification	The ARB's affirmation that a particular credential service provider can provide a particular credential service at a particular assurance level based on a certification report from an accredited assessor.
Certified service	An electronic trust service which has been assessed by a Kantara - accredited assessor and found to be compliant with the applicable SACs.
Credential	An object to be verified when presented in an authentication transaction. A credential can be bound in some way to the individual to whom it was issued, or it can be a bearer credential. Electronic credentials are digital documents that bind an identity or an attribute to a subscriber's token.
Credential management	A service that supports the lifecycle of identity credentials from issuance to revocation, including renewal, status checks, and authentication services.
Credential service	A type of electronic trust service that supports the verification of identities (Identity Proofing), the issuance of identity related assertions/credentials/tokens, and the subsequent management of those credentials (for example, renewal, revocation, and the provision of related status and authentication services).
Credential Service Provider (CSP)	An electronic trust service provider that operates one or more credential services. A CSP can include a Registration Authority.
Cryptographic token	A token for which the secret is a cryptographic key.

TERM	**DEFINITION**
Electronic credentials	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token.
Federal Information Processing Standards (FIPS)	Standards and guidelines issued by the National Institute of Standards and Technology (NIST) for use government-wide in the United States. NIST develops FIPS when the U.S. Federal government has compelling requirements, such as for security and interoperability, for which no industry standards or solutions are acceptable.
Grant Category	One of the specific purposes for which the Kantara Initiative Mark may be used by a third party, being one of: Approved Service; Accredited Assessor; Service Approval Authority (future work focus); or Certified Federation Operator.
Grant (of Rights of Use)	The Granting, by the Kantara Initiative Board of Trustees (KIBoT) or another authoritative body to which the KIBoT has given a delegated authority (itself via a Grant), to use of the Kantara Initiative Mark for a specific Grant Category.
Grantee	An organization to which a Grant of Rights of Use of the Kantara Initiative Mark has been awarded.
Identification	Process of using claimed or observed attributes of an individual to infer who the individual is.
Identifier	Something that points to an individual, such as a name, a serial number, or some other pointer to the party being identified.
Identity	A unique name for a single person. Because a person's legal name is not necessarily unique, identity must include enough additional information (for example, an address or some unique identifier such as an employee or account number) to make a unique
Identity Assurance Work Group (IAWG)	The multi-industry Kantara Initiative partnership working on enabling interoperability among public and private electronic identity authentication systems to foster the adoption of trusted on-line identity services.
Identity Assurance Framework (IAF)	The body of work that collectively defines the industry-led self- regulatory Framework for electronic trust services in the United States and around the globe, as operated by the Kantara Initiative. The Identity Assurance Framework includes documents which contain descriptions of criteria, rules, procedures, and processes.
Identity authentication	Process of establishing an understood level of confidence that an identifier refers to an identity. It may or may not be possible to link the authenticated identity to an
Identity binding	The extent to which an electronic credential can be trusted to be a proxy for the entity named in it.
Identity Proofing	The process by which identity related information is validated so as to identify a person with a degree of uniqueness and certitude sufficient for the purposes for which that identity is to be used.
Identity Proofing policy	A set of rules that defines Identity Proofing requirements (required evidence, format, manner of presentation, validation), records actions required of the registrar, and describes any other salient aspects of the Identity Proofing function that are applicable to a particular community or class of applications with common security requirements. An Identity Proofing policy is designed to accomplish a stated assurance level.
Identity Proofing service provider	An electronic trust service provider which offers, as a standalone service, the specific electronic trust service of Identity Proofing. This service provider is sometimes referred to as a Registration Agent/Authority (RA).
Identity Proofing practice statement	A statement of the practices that an Identity Proofing service provider employs in providing its services in accordance with the applicable Identity Proofing policy.
Information Security Management Systems (ISMS)	A system of management concerned with information security. The key concept of ISMS is the design, implement, and maintain a coherent suite of processes and systems for effectively managing information security, thus ensuring the confidentiality, integrity, and availability of information assets and minimizing
Issuer	Somebody or something that supplies or distributes something officially.
Kantara-approved assessor	A body that has been granted an accreditation to perform assessments against Service Assessment Criteria, at the specified assurance level(s).
Kantara-accredited service	A service which has applied for accreditation and completed a certified assessment at the specified assurance level(s).

TERM	**DEFINITION**
Kantara Initiative Mark	A symbol of trustworthy identity and credential management services at specified Assurance Levels, awarded by the Kantara Initiative Board of Trustees.
Level of Assurance (LOA)	See *Assurance Level*.
Network	An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties.
OID	Object identifier.
Password	A shared secret character string used in authentication protocols. In many cases the claimant is expected to memorize the password.
Practice statement	A formal statement of the practices followed by an authentication entity (e.g., RP, CSP, or verifier) that typically defines the specific steps taken to register and verify identities, issue credentials, and authenticate claimants.
Public key	The public part of the asymmetric key pair that is typically used to verify signatures or encrypt data.
Public key infrastructure (PKI)	A set of technical and procedural measures used to manage public keys embedded in digital certificates. The keys in such certificates can be used to safeguard communication and data exchange over potentially unsecure networks.
Registration	An entry in a register, or somebody or something whose name or designation is entered in a register.
Relying Party (RP)	An entity that relies upon a subscriber's credentials, typically to process a transaction or grant access to information or a system.
Role	The usual or expected function of somebody or something, or the part somebody or something plays in a particular action or event.
Security	A collection of safeguards that ensures the confidentiality of information, protects the integrity of information, ensures the availability of information, accounts for use of the system, and protects the system(s) and/or network(s) used to process the
Service Assessment Criteria (SAC)	A set of requirements levied upon specific organizational and other functions performed by electronic trust services and service providers. Services and service providers must comply with all applicable criteria to qualify for Kantara Initiative approval and earn the Kantara Initiative Mark.
Signatory	A party that opts into and agrees to be bound by the AAS-defined agreements according to the specified procedures.
Subject	An entity that is able to use an electronic trust service subject to agreement with an associated subscriber. A subject and a subscriber can be the same entity.
Subscriber	A party that has entered into an agreement to use an electronic trust service. A subscriber and a subject can be the same entity.
Threat	An adversary that is motivated and capable to violate the security of a target and has the capability to mount attacks that will exploit the target's vulnerabilities.
Token	Something that a claimant possesses and controls (typically a key or password) that is used to authenticate the claimant's identity.
Verification	Establishment of the truth or correctness of something by investigation of evidence.

Appendix A – Identity Proofing Procedure

Symantec contracts with Identity Proofing service providers that have been certified by Kantara at Assurance Level 3. The following sub-sections describe the Identity Proofing procedure specific to each Identity Proofing Agent providing services to NSL.

1. Identity Proofing Agent

Using the Identity Proofing Agent, the Subscriber must provide the following additional information required for Identity Proofing to receive an AL2 Credential:

- Address (including street, city, state and postal zip code)
- Phone number
- Date of Birth (DOB)
- Social Security Number (SSN)

To receive an AL3 Credential, the Subscriber must provide the following additional information required for Identity Proofing:

- Address (including street, city, state and postal zip code)
- Phone number
- Date of birth (DOB)
- Social Security number (SSN)
- Financial account number (credit card number only)

and the Subscriber must also provide the following data needed to receive the AL3 credential:

- Cell phone number

NSL does not store the Date of Birth, Social Security Number or Financial account number. This information is collected for use in Identity Proofing only, and is held by NSL in memory only for the duration of the online Identity Proofing session.

NSL forwards the Identity Proofing information to the Identity Proofing Agent remotely***.*** The Identity Proofing decision is based on a comparison of identity information provided by the Subscriber matched against information within the Identity Proofing Agent records.

The level of Identity Proofing corresponds to the level of assurance of the Credential requested. For both AL2 and AL3, Identity proofing compares the information provided by the Subscriber, including name, address, DOB and SSN, against the information contained in the Subscriber's credit record. For successful Identity Proofing all elements must match. Additionally, for an AL3 Credential, Identity Proofing compares the name and address supplied by the Subscriber against the name and address associated with the credit card number. For successful Identity Proofing, both elements must match.

The Identity Proofing Agent then formulates a set of multiple-choice knowledge-based questions derived from the Subscriber's information in the credit and non-credit records, also corresponding to the level of assurance of the Credential requested. The Subscriber's responses are checked for accuracy based on the information within the Identity Proofing Agent records.

Using a proprietary scoring algorithm, the Identity Proofing Agent determines whether the Subscriber has passed Identity Proofing. On completion of the Identity Proofing process the Identity Proofing Agent returns a result (success or failed) and a date/time stamped Transaction ID to NSL. If Identity Proofing has failed, the Subscriber's Credential Request is denied and rejected.

If Identity Proofing is successful, NSL accepts the request and proceeds to activate the Credential. For federal agency Relying Parties, NSL may optionally send certain Subscriber personal data[1], previously submitted by the Subscriber for Identity Proofing, to the federal agency Relying Party. Prior to transmission, the Subscriber is presented with a notice requesting their consent and if the Subscriber does not consent, the data is not transmitted and registration is rejected.

The Identity Proofing Agent maintains audit records related to the Identity Proofing transaction. NSL records the Identity Proofing event together with the proofing result and the date/time stamped Transaction ID in accordance with section 6.3.

[1] Depending on the federal agency, such personal data transmitted includes but may not be limited to, name, postal and email addresses, telephone number, Social Security number and date of birth.