Symantec™ Validation & ID Protection (VIP) Service Description

Introduction

Symantec™ Validation & ID Protection (VIP) Service provides online service providers and enterprises with increased security of their applications in the form of two-factor authentication and better protection for their End Users against identity theft. The VIP Network enables End Users to utilize a single, second-factor authentication credential across all VIP-enabled enterprises. The VIP Network is governed by the VIP Network Policy (VIP Policy), which may be accessed from the repository link on www.verisign.com. This service description outlines the primary elements of the VIP Service and describes the VIP Network roles and responsibilities.

The VIP Service leverages a shared validation infrastructure operated by Symantec that enables enterprises to deploy and accept second-factor authentication without bearing the entire burden of managing and operating their own self-standing authentication infrastructure. By allowing End Users to leverage a single device to secure their transactions at multiple enterprises, the VIP Network helps make it simpler for End Users to adopt stronger authentication.

Key components include:

- One Time Password (OTP) credentials (VIP Credentials)
- VIP Intelligent Authentication, a risk-based authentication module which analyzes the risk of log-in transactions based on user and device behavior
- Web Services API
- Centralized, off-site provisioning and validation service leveraging Symantec's trust infrastructure
- *VIP Manager*, a Symantec hosted web portal providing VIP Service customers with Service configuration, reporting and management capabilities
- *VIP Self-Service Portal*, a Symantec hosted web portal providing End Users of VIP Service customers with credential lifecycle services
- *VIP Enterprise Gateway*, an enterprise-hosted software component providing integration with enterprise applications and directories

1. VIP Roles and Responsibilities

a. Network Operator

Symantec, as the Network Operator, operates the infrastructure to support the use of VIP Credentials across the VIP Network.

b. Relying Party

A Relying Party means any entity that accepts VIP Credentials for second-factor authentication.

c. Credential Issuer

A Credential Issuer means any entity that has the authority under the VIP Network to issue a VIP Credential.

d. End User

An End User of a VIP Credential means an individual in proper possession of a VIP Credential that can be relied upon by any Relying Party for second-factor authentication.

2. VIP Service Components

a. Credentials

A VIP Credential consists of both a shared key and a unique VIP Credential ID. The shared key is protected by, and/or embedded in, a token or a software or hardware device (Device) in the physical possession of an End User, which the End User may use at any Relying Party website. Using a known cryptographic algorithm, the VIP Credential is used by the Device and the Network Operator

to generate an OTP value. The OTP generated by the Device can then be compared to the OTP value generated for such Device at the Network Operator, and if the values match, the VIP Credential will be validated. The VIP Credential is anonymous and provides a second authentication factor when it is bound to a local user identity of a Relying Party.

In addition to OTP credentials, VIP supports a software based device ID credential, VIP Registered Computer. The Registered Computer credential utilizes a browser plug-in to manage an anonymous device certificate stored in a proprietary keystore on the end user's PC. This certificate is validated in real-time by the VIP Service and is used as a second authentication factor when it is bound to a local user identity at a Relying Party.

b. VIP Credential Provisioning

A token or hardware Device contains a VIP Credential that is provisioned during manufacturing or through dynamic post-production provisioning and known only to the Network Operator. VIP Credentials are not accessible from outside the Device. Within the Device, there is space to store the VIP Credential and only the application inside can access it. Accessing the VIP Credential would necessitate physically breaking into the Device, which would render the VIP Credential unusable. In the case of a VIP Credential stored in a software Device, the VIP Credential is stored encrypted using an encryption key only accessible to the software Device.

As part of the VIP Credential Provisioning process described above, the Network Operator securely stores a copy of the VIP Credential in encrypted form in the Network Operator's datacenter. The VIP Credential is encrypted using a TripleDES encryption algorithm.

c. VIP Credential Issuance and Distribution

Credential Issuers are responsible for issuing VIP Credentials to End Users. The logistics involved in the distribution of such VIP Credentials are controlled and implemented by each Credential Issuer.

When issuing a VIP Credential to an End User, a Credential Issuer will:

- Obtain all the necessary End User identification information as mandated by the VIP Policy;
- Obtain all the necessary VIP Credential identification information as mandated by the VIP Policy and
- Bind the End User to terms and conditions of VIP Credential usage as provided by the Network Operator

d. VIP Credential Issuance and Distribution

Through the VIP website (ID Center), Symantec acts as a Credential Issuer and distributes VIP Credentials to End Users. The ID Center allows End Users to create an account protected by username and password, and purchase a VIP Credential. Symantec will send the purchased VIP Credential to the address indicated by the End User, in the case of a hardware token, or fulfill the request on existing hardware devices through other specific means (e.g., over-the-air provisioning and activation for mobile devices).

A Relying Party may instruct End Users to purchase VIP Credentials directly from the ID Center and may subsidize the price paid by such End Users by using ID Center coupons. These coupons can be purchased by a Relying Party at a percentage of the base price of a VIP Credential. This price does not include taxes or shipping costs, unless a Relying Party opts to fully subsidize an End User's purchase price for a VIP Credential. Symantec will be the Credential Issuer of any VIP Credential issued through the ID Center. Symantec provides an automated self-management interface, allowing End Users to perform certain operations on the ID Center to validate and activate the VIP Credential.

Hardware credentials purchased through the ID Center can only be shipped to US addresses.

e. VIP Credential Validation

Once an End User has completed the activation process with respect to its VIP Credential and has bound it to an identity at a Relying Party, the Relying Party will prompt such End User to communicate an OTP from such VIP Credential for second-factor authentication. The Relying Party will validate such End User's first factor credential, and will retrieve either the VIP Credential ID or the End User identifier from its local user store and will forward both the VIP Credential ID or the

End User identifier and the OTP to the Network Operator for validation. The Network Operator then returns a valid or invalid message to the Relying Party.

f. VIP Manager

VIP Manager is a web based portal, hosted by Symantec, for the configuration and management of the VIP Service. VIP Service customers are given access to this portal for the purposes of configuring service parameters, viewing reports, and managing credential lifecycle. *VIP Manager* provides the following lifecycle services for VIP Credentials:

- VIP Credential activation and deactivation
- Unlocking of VIP Credentials
- Testing and synchronization of VIP Credentials
- Temporary security code management for VIP Credentials
- Binding and unbinding of VIP Credentials to End User identifiers

Access to *VIP Manager* is controlled by validating (i) the administrator's email address, password, and VIP Credential, or (ii) the administrator's enterprise username and password through a single sign-on functionality enabled by either the *VIP Enterprise Gateway* or an enterprise-hosted SAML-compliant federation server, in addition to validating the administrator's VIP Credential.

g. VIP Self-Service Portal

VIP Self-Service Portal is a web based portal, hosted by Symantec, for end user credential lifecycle services. VIP Service customers can grant direct access to this portal to their end users for the purposes of managing credential lifecycle. *VIP Self-Service Portal* provides the following lifecycle services for VIP Credentials:

- VIP Credential activation and deactivation
- Testing and synchronization of VIP Credentials
- Binding and unbinding of VIP Credentials to End User identifiers

Access to *VIP Self-Service Portal* is controlled by validating the end user's enterprise username and password through a single sign-on functionality enabled by either the *VIP Enterprise Gateway* or an enterprise-hosted SAML-compliant federation server.

h. VIP Intelligent Authentication

VIP Intelligent Authentication analyzes log-in transactions and measures risk by user and by device. Depending on the risk associated with a particular log-in transaction, enterprises can "step up" authentication using out-of-band or two-factor authentication techniques supported within the enterprise or through the VIP Authentication Service. The risk scores take into account the following layers:

(i) Rules Engine

The rules engine establishes rules from known fraud patterns that factor into the ultimate risk score of a particular log in. These rules help to identify risky behavior as well as impossible log-in patterns (e.g., impossible travel). The rules also include general policy around log-ins from forbidden countries or known risky IP/geo locations.

(ii) Behavioral Engine

The behavioral engine stores typical user behavior and employs a heuristic engine to map subsequent log-ins against these known patterns of behavior. For each user, VIP Intelligent Authentication has a stored pattern of behavior including operating system, browser type, IP address, network and geographic location to assess anomalies in a particular log-in event.

(iii) Device Engine

The device engine analyzes the specific characteristics of the end user's device (PC, mobile or tablet) and employs a heuristic engine to compare these characteristics on subsequent log-in transactions. In addition to passive device fingerprinting, VIP Intelligent Authentication stores a persistent tag in the end user's browser or leverages pre-existing Symantec endpoint software on the end user's device to aid in identifying devices across log-in transactions.

(iv) Network Intelligence

VIP Intelligent Authentication uses the global reach of Symantec's products by taking in specific intelligence with a known correlation to detecting fraud and including it with the log-in analysis that calculates overall risk. The Symantec Global Intelligence is garnered from visibility into over two billion IT events daily, 100,000 security events logged annually, and over 120 million threats/viruses reported. The specific intelligence utilized includes IP addresses for suspected bots by patterns, bots by contact, command and control (C&C), phishing hosts, and top 1000 attacking IPs.

(v) Transaction Monitoring

Transaction monitoring capabilities in VIP Intelligent Authentication can help financial institutions prevent fraudulent activities like man-in-the-middle attacks by providing an additional layer of security besides login risk analysis. If the transaction monitoring option is enabled in VIP Intelligent Authentication, it also analyzes monetary transactions for the end user. It takes in to account anomalies related to daily amount transfer, frequency of amount transfer, and new destination accounts for the end user.

Personal Information Collected by VIP Intelligent Authentication

If VIP Intelligent Authentication is activated, Symantec will collect and process the following information about the user and the user's machine:

- Operating system
- IP address
- Browser type
- Network
- Geographic location, which may include city, state or country
- Existing Symantec endpoint software stored on the machine

In addition to the information collected above, if Transaction Monitoring is activated, Symantec will collect and process the following information about the user and the user's machine:

- Account information (ID, name, type, creation date, Bank ID)
- Transaction information (amount, type, time, destination account ID)

To collect such information Symantec utilizes a persistent tag in the end user's browsers and cookies. The information is processed for the purpose of determining the user's typical pattern of behavior. During the authentication process, the stored pattern is compared with the actual behavior in order to assess anomalies in a particular log-in event. The information is stored on Symantec's servers in the United States. Symantec does not share, transfer, sell, rent or lease to third parties any of the information collected for VIP Intelligent Authentication.

3. VIP Software Components

APIs may be provided for the development of custom applications on the VIP Network. This includes functionality for VIP Credential validation, synchronization, and all VIP Credential lifecycle management functions.

The *VIP Enterprise Gateway*, a software component deployed on-premise by a VIP Network member may be provided for the integration of enterprise applications and directories with the VIP Network. The *VIP Enterprise Gateway* supports two-factor authentication by utilizing a first and second-factor of authentication. The first factor, "what you know," can be a password associated with each end-user, which is stored in the enterprise directory. The second-factor, "what you have," is an OTP generated by a VIP Credential. OTP validation is performed by the VIP Service. For each validation request sent to the *VIP Enterprise Gateway*, the first-factor validation is performed locally at the enterprise directory. The *VIP Enterprise Gateway* then forwards the End User identifier and OTP value to the VIP Service. The VIP Service validates the OTP value, *i.e.*, second-factor.

The VIP Service also includes documentation and custom plug-ins (where necessary) that layer two-factor authentication on top of many popular enterprise applications that require end-user based access.

The respective documentation and custom plug-ins (where necessary) are distributed on-line. The website is updated on a regular basis with new integrations.

4. Audit Trails

Significant events are recorded by Symantec on a transaction-by-transaction basis. Symantec maintains audit records independently in multiple media depending upon the sensitivity of the event. Audit trails are created for all OTP transactions, including passed and failed validations, and passed and failed activations. In addition, *VIP Manager* keeps audit logs that record functions executed by individual administrators. The *VIP Enterprise Gateway* also records audit logs that record authentication events that are processed through it.

5. Support and Maintenance

The support and maintenance commitments of Symantec are described in the applicable Service Level Agreement available at: https://www.verisign.com/repository/service_description.

SYMANTEC™ VALIDATION & ID PROTECTION (VIP) SERVICE TERMS AND CONDITIONS

1. DEFINITIONS

For purposes of these VIP Service Terms and Conditions, the following capitalized terms shall have the meanings set forth below. Capitalized terms that are not defined herein shall have the meanings set forth in the Agreement (as defined below).

(a) "Agreement" means the master agreement or such other agreement entered into between Symantec and Customer under which any VIP products and services set forth in this Service Description are provided by Symantec to Customer.
(b) "Credential Issuer" has the meaning given in the VIP Policy.
(c) "Customer" means a party that is acting as a Credential Issuer and/or a Relying Party under the Agreement and the applicable Services Order.
(d) "Device" has the meaning given in the VIP Policy.
(e) "End User" has the meaning given in the VIP Policy.
(f) "Network Operator" has the meaning given in the VIP Policy.
(g) "Relying Party" has the meaning given in the VIP Policy.
(h) "Service Description" means the Symantec Validation & ID Protection (VIP) Service Description and Symantec Validation & ID Protection (VIP) Service Terms and Conditions, collectively.
(i) "**Service Period**" is each annual period within a Services Order Term.
(j) "Services Order" means the order executed by Symantec and Customer pursuant to which Customer purchases any or all of the VIP products and services.
(k) "**Services Order Term**" is Customer's committed period of VIP Service, as set forth in the Services Order.
(l) "Symantec Materials" means information provided by Symantec to Customer consisting of sales and marketing materials related to the VIP Network that Customer is authorized to use to promote, market, distribute and/or sell the VIP Network and VIP Credentials under this Agreement.
(m) "VIP Credential" has the meaning given in the VIP Policy.
(n) "VIP End User Agreement" has the meaning given in Section 5(a) below.
(o) "VIP Network" has the meaning given in the VIP Policy.
(p) "VIP Policy" means the policy document for the VIP Network as set forth on www.verisign.com, as amended from time to time in accordance with its terms.
(q) "VIP Service" means the VIP Credentials, VIP Manager, the VIP Software and any services provided by Symantec to Customer in connection with Customer's participation in the VIP Network as a Credential Issuer or Relying Party, as the case may be, as set forth in this Service Description.
(r) "VIP Software" means the software, if any, provided by Symantec to Customer under this Agreement.

2. APPOINTMENT AND AUTHORIZATION

(a) Appointment. Subject to the terms of the Agreement, Symantec grants Customer a non-exclusive and non-transferable right to participate in the VIP Network. In the event that Customer agrees to act as a Credential Issuer, Symantec grants a non-exclusive and non-transferable right to promote, market, sell and deliver the VIP Credentials to any End User.
(b) Authorization. Customer may represent itself as a participant in the VIP Network as a Relying Party and/or Credential Issuer, as applicable, but Customer shall not represent that it is otherwise affiliated with Symantec. Customer is authorized to represent only such facts about Symantec, the VIP Network

and the VIP Credentials as Symantec posts on its public website and in other published materials, including the Symantec Materials.

3. CUSTOMER'S OBLIGATIONS

(a) Relying Party. If Customer acts in the capacity of a Relying Party, Customer represents and warrants to Symantec that Customer (i) has reviewed the VIP Policy and understands the obligations of a Relying Party and (ii) will comply with the obligations of a Relying Party as set forth in the VIP Policy.

(b) Credential Issuer. If Customer acts in the capacity of a Credential Issuer, Customer represents and warrants to Symantec that Customer (i) has reviewed the VIP Policy and understands the obligations of a Credential Issuer and (ii) will comply with the obligations of a Credential Issuer as set forth in the VIP Policy.

(c) Manner of Performance. Customer will (i) use commercially reasonable efforts, at its option, to promote, market, distribute and/or sell the VIP Network and/or the VIP Credentials (as a Credential Issuer), (ii) conduct business in a competent and professional manner that reflects favorably at all times on the VIP Network and the goodwill and reputation of Symantec, (iii) not make any false or misleading representations, warranties or guarantees with regard to Symantec, the VIP Network or the VIP Credentials and (iv) comply with all applicable federal, state, regional, and local laws and regulations related to the performance of its duties hereunder. All use of VIP Software by Customer and Customer's End Users is governed by the terms and conditions specified in the Agreement.

(d) Marketing. Symantec will provide Symantec Materials to Customer for the purposes of promoting, marketing, distributing and/or selling the VIP Network and/or the VIP Credentials. Customer's use of the Symantec Materials is subject to the license granted in Section 6 below.

(e) VIP Network Promotion and Use of Logos. Customer may represent itself as a participant in the VIP Network as contemplated by the VIP Policy. Customer may prominently display the VIP logo on all web sites which accept VIP Credentials including, but not limited to, log-in pages and password entry pages. Customer agrees that, in its capacity as a Credential Issuer, any and all Devices purchased by Customer hereunder for use on the VIP Network shall have the VIP logo on such Devices, in a form approved by Symantec.

(f) Data Privacy. Customer is responsible for its use of the VIP Service in compliance with privacy and data protection requirements, including but not limited to providing adequate choice and notice to End Users as described in the Symantec Validation & ID Protection (VIP) Service Description.

4. SYMANTEC'S OBLIGATIONS

(a) Network Operator. As the Network Operator of the VIP Network, Symantec represents and warrants that it will use commercially reasonable efforts to comply with the obligations of a Network Operator as set forth in the VIP Policy.

(b) Manner of Performance. Symantec will (i) use commercially reasonable efforts to promote, market, distribute and/or sell the VIP Network, (ii) conduct business in a competent and professional manner that reflects favorably at all times on the VIP Network, (iii) not make any false or misleading representations, warranties or guarantees with regard to the VIP Network or to the VIP Credentials; and (iv) comply with all applicable federal, state, regional, and local laws and regulations related to the performance of its duties hereunder.

(c) VIP Network Promotion and Use of Logos. Customer hereby grants Symantec the right to display Customer's logo on Symantec's website(s) in one of the forms shown in Customer's trademark usage guidelines.

5. OBLIGATIONS WITH RESPECT TO VIP CREDENTIAL ORDERS

(a) End User Agreements. As a Credential Issuer, whether or not Device delivery functions are outsourced, Customer shall issue the VIP Credentials to End Users subject to a legally binding written agreement between the End User and the Credential Issuer (the **"VIP End User Agreement"**) which includes contractual provisions that at a minimum:

1. Obligate the End User to use the VIP Credential and any related service subject to and in compliance with the VIP End User Agreement, the VIP Policy (available at www.versisign.com/repository) and all applicable laws and regulations.
2. Obligate the End User to acknowledge and agree that (i) the VIP Credential is intended to assist with authentication of the End User to VIP Network participants and increase the level of security of End User's web transactions with such entities, and may be used solely for this purpose, (ii) the VIP Credential is not failproof nor can it be used as a substitute for official proof of End User's identity, (iii) there are inherent security risks with use of the Internet and (iv) End User is solely responsible for the degree to which End User chooses to rely on End User's VIP Credential.
3. Require the End User to provide accurate and complete information as reasonably requested by Symantec or the Credential Issuer.
4. Require the End User to maintain secure possession of the VIP Credential and promptly notify the Credential Issuer if End User loses possession of the VIP Credential for any reason (for example, loss of the mobile phone containing the VIP Credential or loss of the token or hardware device which stores the VIP Credential).
5. Prohibit the End User from transferring the VIP Credential to any other party or permitting use of the VIP Credential by any other party.
6. Permit Symantec and the Credential Issuer to revoke End User's VIP Credential upon breach of the VIP End User Agreement or if End User compromises the security or integrity of the VIP Network.
7. Disclaim, to the extent permitted by applicable law, (a) all warranties and representations relating to the VIP Credential and any related services and (b) Symantec's liability for any damages, whether direct, indirect, incidental or consequential, arising from use of the VIP Credential and any related services. End User's sole and exclusive remedy for any malfunction, deficiency or other dissatisfaction related to a VIP Credential or any related services is a claim against the Credential Issuer to issue a replacement VIP Credential.

Customer shall enforce the terms of the VIP End User Agreements against End Users and shall notify Symantec of any known breach of such terms. Customer will defend and indemnify Symantec against all claims and damages to Symantec caused by the failure to include the required contractual terms in each VIP End User Agreement.

(b) Discontinuation of VIP Network Offering. If Symantec discontinues the general availability of the VIP Service, Symantec must provide Customer no less than six (6) months' written notice. Upon receipt of such notice, Customer (i) in its capacity as a Relying Party, shall provide notice to End Users of such discontinuance on the Relying Party website(s) on which an End User's VIP Credential can be Activated and Bound (as defined in the VIP Policy) and (ii) in its capacity as a Credential Issuer, Customer shall promptly cease distribution of any VIP Credentials. Customer, in its capacity as a Credential Issuer, will have the option, subject to entering into a mutually agreeable agreement with Symantec, to purchase an in-premise version of the VIP Service for use with End Users to whom Customer has issued VIP Credentials.

(c) Effect of Termination or Expiration. Except as a result of Symantec's material default, in the case of any termination or expiration of Customer's obligations as a Credential Issuer, Symantec will become the Credential Issuer of any VIP Credential that was issued (as defined in the VIP Policy) by the Credential Issuer in accordance with the terms of the VIP Policy. Upon such expiration or termination, Credential Issuer shall cease promoting, marketing and selling the VIP Network and VIP Credentials.

6. SYMANTEC MATERIALS

(a) Symantec Materials License Grant. Symantec grants Customer a nonexclusive, non-transferable, non-sublicensable right and license to: (i) use the Symantec Materials during the Services Order Term solely in conjunction with the marketing, promotion and resale, as applicable, of the VIP Network and the VIP Credentials and (ii) modify certain of the Symantec Materials expressly designated for such purpose by incorporating Customer trademarks and/or brand features ("**Customer Branding**") in a manner consistent with branding guidelines provided by Symantec, and in each case subject to Symantec's prior written approval. All such modified materials will be deemed Symantec Materials under the applicable Services Order, provided, however, that Symantec will have no rights to the

Customer Branding. Symantec grants no right in the Symantec Materials 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 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 Materials 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 Materials, other than the Customer Branding).

(b) 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.

(c) No Continuing Rights. Upon expiration or termination of services contemplated in this Services Description, Customer will immediately cease (i) all use of any VIP Software and (ii) all display, advertising and use of all of the Symantec Materials 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 Materials (excluding Customer Branding) or with any other materials, trademark, trade name or product designation associated with Symantec or any Symantec product.

7. DISCLAIMER OF WARRANTIES

EXCEPT AS SPECIFICALLY PROVIDED IN THE SERVICES DESCRIPTION, THE AGREEMENT, THE VIP POLICY OR IN THE APPLICABLE SERVICES ORDER, THE VIP NETWORK AND THE VIP PRODUCTS AND SERVICES ARE PROVIDED "AS IS". SYMANTEC DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY AS TO ANY MATTER WHATSOEVER, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS.