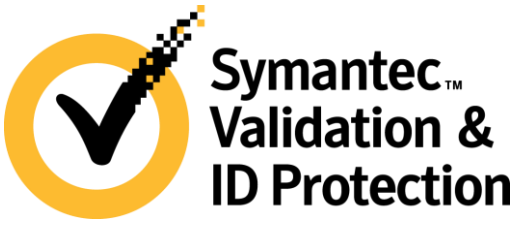
Symantec Validation and ID Protection (VIP) Authentication Network Policy

Version: 2.1
Effective Date: September 7, 2011



Trademark Notices

The Symantec logo and Symantec Validation and ID Protection Service Network are trademarks and service marks of Symantec Corporation. Other trademarks and service marks in this document are the property of their respective owners. Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of Symantec Corporation.

Notwithstanding the above, permission is granted to reproduce and distribute these Symantec Validation and ID Protection (VIP) Service Network Policies on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to Symantec Corporation.

Requests for any other permission to reproduce these Symantec Validation and ID Protection Network Policies (as well as requests for copies from Symantec) must be addressed to Symantec Corporation., 350 Ellis Street, Mountain View, CA 94043 USA Attn: Symantec VIP Network Product Manager. Tel: +1 650.527.8000 Fax: +1 650.527.8050 E-mail: ***vip-practices@symantec.com***.

TABLE OF CONTENTS

1 Introduction

Symantec Validation and ID Protection (VIP) Authentication Network ("VIP Network") is a network of online service providers and enterprises who promote the use of stronger authentication to increase the security of their applications and better protect consumers against identity theft. Operated by Symantec Corporation ("Symantec"), the VIP Network allows its participants to accept a shared second factor authentication credential. More specifically, the VIP Network enables consumers to utilize a single, two-factor authentication credential across all VIP-enabled Web sites of network members.

By leveraging two-factor authentication, the VIP Network increases security for financial assets, confidential information and personal identification information. For participating sites, the VIP Network greatly reduces the risk of stolen information being used to fraudulently log into a users online account. For consumers, the VIP Network provides the additional assurance that an imposter cannot simply log in to their service using a guessed or stolen username and password.

The VIP Network uses 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 consumers to use a single device to secure their transactions at multiple Web sites, the VIP Network makes it simple for consumers to adopt stronger authentication as part of their everyday web lifestyle.

This document, "The Symantec Validation and ID Protection Authentication Network Policy" ("Policy"), is the principal statement of policy governing the VIP Network. It sets forth the business, legal, and technical requirements for issuing, using, and managing second factor authentication credentials within the VIP Network. Capitalized terms used in this Policy without other definition shall have the meaning set forth in the Glossary of Terms at the end of this Policy, unless the context clearly requires otherwise.

2 VIP Network Participants and Interoperation

2.1 VIP Network Participants

This section provides a brief description of the various participants in the VIP Network (each a "VIP Participant") and the role of each VIP Participant in the VIP Network. The specific obligations of each VIP Participant are more fully discussed later in this Policy.

2.1.1 Network Operator

The Network Operator provides and manages the secure infrastructure supporting the use of VIP Credentials across the VIP Network. For purposes of the VIP Network and this Policy, Symantec is the Network Operator.

2.1.2 Relying Party

A Relying Party is any entity that accepts any VIP Credential for second factor authentication. In order to accept any VIP Credential, the Relying Party must, upon request from an End User, coordinate with the Network Operator to Activate such VIP Credential and Bind it to the identity of the End User within their local directory or user store. Since only a second factor of authentication is shared across the VIP Network, each Relying Party must also provide an End User with a local identity or first authentication factor that is unique to the Relying Party. Typically, the local identity consists of an End User's associated username and password already registered at the Relying Party's Web site.

A Relying Party manages the Credential Lifecycle Functions for VIP Credentials that the Relying Party has Activated (in coordination with the Network Operator) and Bound for use on its site.

With respect to VIP Credentials that a Relying Party Activates), the Relying Party is responsible for all Credential Lifecycle Functions related to any VIP Credential that is used at the Relying Party's site. Relying Parties maintain complete control and responsibility over the End User experience on their own Web site.

2.1.3 Credential Issuer

A Credential Issuer is an entity that has the authority under the VIP Network to issue a VIP Credential.

On the VIP Network, a Credential Issuer must also be a Relying Party and accept VIP credentials that have been issued by other VIP Participants unless, to the reasonable satisfaction of the Network Operator, it is determined that such VIP Participant does not have a website on which a VIP Participant can Activate and Bind a VIP Credential. In which case, the VIP Participant will not be required to be a Relying Party. If however, after becoming a Credential Issuer such VIP Participant develops the capability of Activating and Binding VIP Credentials, such VIP Participant will be required to become a Relying Party.

On the VIP Network, Symantec shall act as a Credential Issuer and have the obligations of a Credential Issuer, as set forth in this Policy, with respect to VIP Credentials that Symantec issues.

2.1.4 End User

An End User is an individual in proper possession of a VIP Credential. Each End User must coordinate the Activation and Binding of their VIP Credential with each Relying Party where the End User intends to use their VIP Credential.

2.2 Interoperation of VIP Participants

After a Relying Party has joined the VIP Network, it will configure some or all of its Internet applications to accept VIP Credentials and will recommend that some or all of its End Users obtain a VIP Credential to increase the security of online transactions. A VIP Credential is obtained from a Credential Issuer. Once an End User is in possession of the VIP Credential, the VIP Credential must be accepted by all Relying Parties on the VIP Network, subject to their individual Activation and Binding practices.

The following diagram shows the interaction of the various VIP Participants on the VIP Network.

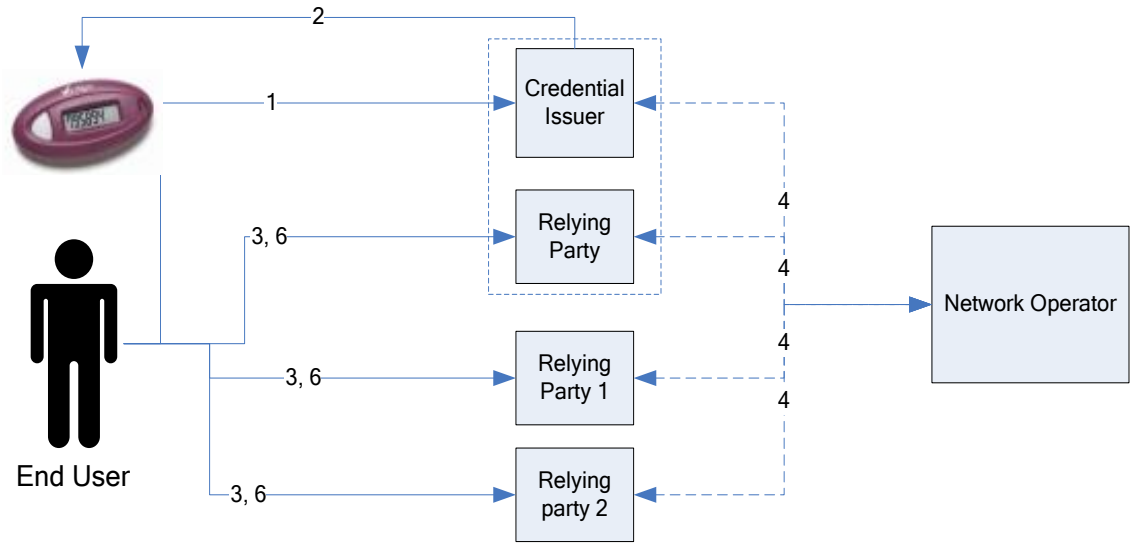


Figure 1: Operation of the Symantec Validation and ID **Protection (VIP) Network**

Step-by-Step Description

Step 1: End User applies for a VIP Credential from a Credential Issuer.

Step 2: Credential Issuer sends a VIP Credential to the End User.

Step 3: End User initiates the Activation and Binding of the VIP Credential to the End User's identity online at a Relying Party site.

Step 4: Relying Party requests the Network Operator to Activate the VIP Credential in the VIP Network, for use at that Relying Party.

Step 5: Relying Party then Binds the VIP Credential to the End User identity at the Relying Party website.

Step 6: End User can then use the VIP Credential at the Relying Party website

When *Activating* and *Binding* the VIP Credential with a Relying Party, an End User provides their first factor authentication information as well as the unique VIP Credential ID and one or two consecutive one time password values. The Activation and Binding process would be repeated at each Relying Party where the End User wishes to use their VIP Credential. Once the VIP Credential is Activated and Bound to a local identity at a Relying Party, the End User can then present their second factor one time password value in addition to their first factor identification to the Relying Party for stronger authentication. Relying Parties communicate the VIP Credential ID and one time password value supplied by the End User to the Network Operator for validation.

3 VIP Credentials

3.1 VIP Credentials

A VIP Credential consists of both a shared secret and a unique VIP Credential ID. The shared secret is protected by, and/or embedded in, a Device in the physical possession of an End User. The VIP Credential ID is an alphanumeric string that can vary in length from 12 to 16 characters which identifies both the VIP Credential manufacturer as well as the VIP Credential itself. The VIP Credential ID is known both to the Credential and the Network Operator. Using a known cryptographic algorithm, the VIP Credential is used by the Device to generate an OTP value. The OTP generated by the Device can then be compared to the OTP value generated for that Credential ID at the Network Operator, and if the values are the same, the VIP Credential is validated. The VIP Credential is anonymous and provides a second authentication factor when it is Activated and Bound to a local user identity at a Relying Party's Web site.

The VIP Network supports OATH (Initiative for Open Authentication) as well as other second factor authentication credentials. Before a Device is supported on the VIP Network it must be accredited by Symantec. The VIP Network is designed to support multiple types of Devices that include VIP Credentials. VIP Credentials may come embedded in dedicated security hardware Devices (e.g,. OTP tokens) and can also be embedded into consumer-oriented Devices, such as mobile phones, flash storage devices or credit cards.

3.2 Proof of Possession of a VIP Credential

Each VIP Credential has a unique identifier known as a VIP Credential ID, as well as an associated, but separate authentication mechanism (e.g., an OTP) that can be used to prove possession of the VIP Credential.

3.3 VIP Credential Provisioning and Protection

3.3.1 VIP Credential Provisioning

A Device contains a VIP Credential that is provisioned to the Device during manufacture.-or through dynamic post-production provisioning. VIP Credentials are not accessible from outside the Device. To provision the VIP Credential to the Device during manufacture, the manufacturer uses one of two processes:

1. The Device manufacturer securely requests VIP Credentials from the Symantec backend. As the Network Operator, Symantec returns the VIP Credential(s) for each Device in encrypted form and stores a copy of the VIP Credentials in encrypted form.

2. The Device manufacturer generates the VIP Credential, encrypts it, and securely transmits it to Symantec. As the Network Operator, Symantec stores a copy of the VIP Credentials in encrypted form.

These VIP Credentials are used to calculate the OTP values that are used to authenticate End Users.

To provision a Device using the dynamic post-production provisioning process, the End User must first obtain a provisioning code from a Credential Issuer. The End User will enter the provisioning code into the Device's OTP

application. A provisioning request will be sent securely to the dynamic provisioning service of the Network Operator, and the VIP Credential will be sent back securely to the Device.

3.3.2 VIP Credential Protection

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.

3.4 Credential Status

VIP Credentials have both Local and Global Status.

Table 1 below describes the different local statuses that may be associated with a VIP Credential on the VIP Network for a particular Relying Party, and how a particular status affects the operation of that VIP Credential for that Relying Party.

Status	Description
New	VIP Credential has been issued but not yet Activated or Bound
Enabled (Active)	VIP Credential has been Activated and Bound by a Relying Party at the request of an End User and is valid for use by that Relying Party.
Inactive	VIP Credential has been Deactivated by a Relying Party. The VIP Credential must be re-Activated and re-Bound in accordance with this Policy for future use by that Relying Party
Locked	VIP Credential has been Locked after too many consecutive failed validation attempts by a particular Relying Party and is not valid for use by that Relying Party. The VIP Credential must be unlocked by that Relying Party in accordance with this Policy for future use by that Relying Party.
Disabled	VIP Credential has been temporarily Disabled by a Relying Party, and is not valid for use by that Relying Party. The VIP Credential must be re-enabled in accordance with this Policy for future use by that Relying Party. While the VIP Credential is Disabled, the Relying Party can set a temporary passcode to be used for authentication.

Table 1: Local Credential Status Descriptions

The Local Credential Statuses and how they transition can be represented graphically as follows:

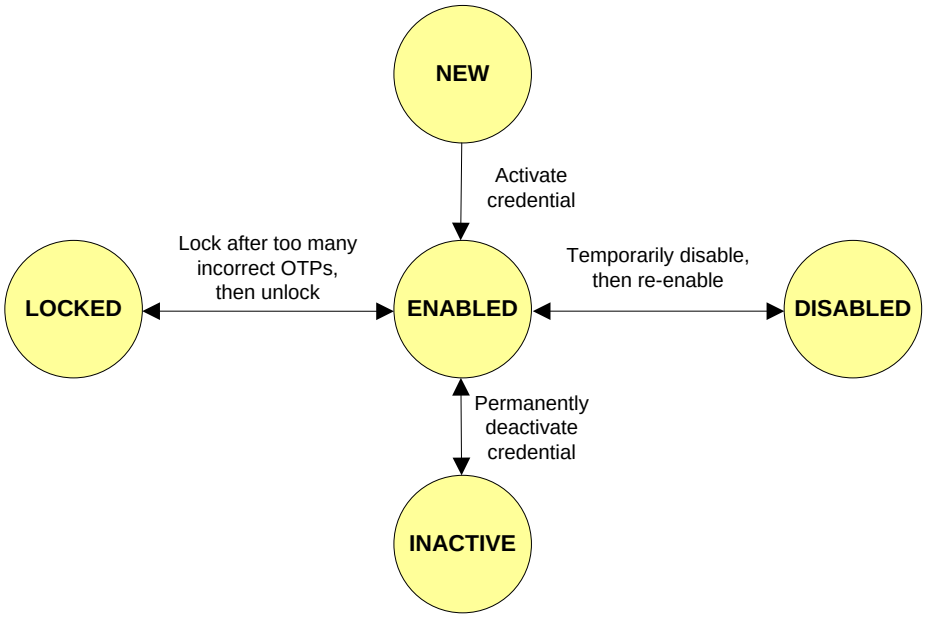


Figure 2: Local Credential Status Transitions

Table 2 below describes the different global statuses that may be associated with a VIP Credential on the VIP Network, and how a particular status affects the validity of that VIP Credential on the VIP Network for all Participants.

Status	Description
Valid	VIP Credential is valid for use by any VIP Participant. How that Credential can be used by a VIP Participant depends on the local status described above.
Revoked	VIP Credential has been Revoked by the Network Operator, and is not valid for use on the VIP Network by any VIP Participant.

Table 2: Global Credential Status Descriptions

3.5 Credential Validation Process

Once an End User has completed the Activation process for their VIP Credential and Bound it to a Relying Party website for use, the Relying Party website may prompt the End User to supply a one time password value from the VIP Credential for second factor authentication. Once the end User has supplied the one time password value the Relying Party then retrieves the VIP Credential ID associated with that End User from its local user store and forwards both the VIP Credential ID and the one time password value to the Network Operator for validation. The Network Operator then returns a valid or invalid message to the Relying Party website.

3.6 Credential Lifecycle Management

Once a VIP Credential is provisioned and issued to an End User, such VIP Credential is available for Activation and Binding by any Relying Party. Each Relying Party is responsible for managing the Credential Lifecycle Functions of any VIP Credential that it coordinates the Activation of and Binds.

The following section describes the primary Credential Lifecycle Functions relating to all VIP Credentials. On the VIP Network, Relying Parties shall be responsible for ensuring the correct status of the VIP Credentials on the VIP Network for that Relying Party is always reflected. However, Relying Parties shall not be responsible for managing the Credential Lifecycle Functions of VIP Credentials for use at other Relying Parties' sites. The Network Operator shall have the right to exercise all Credential Lifecycle Functions of any and all VIP Credentials on the VIP Network.

The following are Credential Lifecycle Functions.

3.6.1 Activation

Activation is the process of enabling the VIP Credential for use on the VIP Network for a particular Relying Party. For the avoidance of doubt, Activation does not link an End User's identity to the VIP Credential. When a VIP Credential is *Activated* for a Relying Party, that Credential can then be subsequently Bound by that Relying Party.

3.6.1.1 Who can Request Activation?

Each Relying Party must send an Activation request to the Network Operator to validate and *Activate* a VIP Credential for that Relying Party. Credential Issuers who are also Relying Parties may pre-*Activate* the VIP Credentials they issue and may also pre-*Bind* VIP Credentials to an End User's identity at its Relying Party website.

3.6.1.2 Who is Responsible for Activating a VIP Credential

The Network Operator is the only VIP Participant who can *Activate* a VIP Credential on the VIP Network.

3.6.1.3 Requirements for Activation

In order for a VIP Credential to get *Activated* on the VIP Network, the End User must prove possession of the VIP Credential to the Relying Party. For VIP Credentials that are pre-Activated by a Credential Issuer, this requirement is not applicable.

3.6.2 Locking/unLocking

Locking a VIP Credential is the process of changing the status of a VIP Credential from 'Enabled' to '*Locked'* for a particular Relying Party. A *Locked* VIP Credential cannot be used by that Relying Party until it has been *unLocked*. *Locking* a VIP Credential for a particular Relying Party does not affect the use of that VIP Credential at any other Relying Parties' websites.

3.6.2.1 Circumstances Requiring VIP Credential Locking

A VIP Credential is *Locked* for a Relying Party when too many consecutive failed attempts have been made to validate the VIP Credential by a particular Relying Party.

For example, in the case of a VIP Credential on an OTP token, if a series of wrong OTPs are entered against a given VIP Credential by a particular Relying Party, the VIP Credential will be *Locked* for further use by that Relying Party. Although the threshold number of failed OTP attempts is configurable by the Relying Party accepting the OTP value, the recommended number of failed authentications resulting in a *Locked* VIP Credential should not exceed ten (10).

3.6.2.2 Who can Lock a VIP Credential?

Only the Network Operator can *Lock* a VIP Credential for a particular Relying Party after receiving too many consecutive failed validation attempts for that VIP Credential from such Relying Party.

3.6.2.3 Who can Request unLocking of a VIP Credential?

Only the End User who owns the account where the VIP Credential is bound can request a Relying Party to send a request to the Network Operator to *unLock* a *Locked* VIP Credential.

3.6.2.4 Who can unLock a VIP Credential

Upon receipt of a request from the Relying Party with respect to a VIP Credential, only the Network Operator can *unLock* such VIP Credential.

3.6.2.5 Requirements for UnLocking a VIP Credential

A VIP Credential shall only be *unLocked* for a Relying Party by the Network Operator only after receiving a request to do so from the Relying Party. The Relying Party shall only send such a request once it has sufficiently identified the End User and confirmed that the End User is in possession of such VIP Credential in accordance with Section 3.2 above.

3.6.3 Disabling/Enabling

Disabling a VIP Credential is the process of temporarily changing the status of the VIP Credential from *Enabled* to *Disabled* for a particular Relying Party. A *Disabled* VIP Credential cannot be used by that Relying Party until it has been re-enabled. A temporary passcode can be set by the Relying Party for a *Disabled* VIP Credential, to use in place of an OTP while such VIP Credential itself is *Disabled*.

3.6.3.1 Circumstances Requiring VIP Credential Disabling

Examples of situations where a VIP Credential may be *Disabled* for a particular Relying Party:

- The End User is temporarily without his/her VIP Credential and needs access to the Relying Party's site
- The VIP Credential is no longer operational and the End User needs access to the Relying Party's site while waiting for a replacement VIP Credential
- The End User reports that it suspects that the VIP Credential has been compromised and the End User needs access to the Relying Party's site while waiting for a replacement VIP Credential

3.6.3.2 Who can Request Disabling of a Credential?

An End User of a VIP Credential may request a Relying Party to send a request to the Network Operator to *Disable* the VIP Credential for that Relying Party.

A Relying Party may request the Network Operator directly to *Disable* a VIP Credential for that Relying Party if in its sole discretion such action is warranted in terms of this Policy.

The Network Operator shall also have the ability to *Disable* a VIP Credential for a particular Relying Party, if in its sole discretion such action is warranted in terms of this Policy.

3.6.3.3 Who can Disable a VIP Credential

Only the Network Operator can *Disable* a VIP Credential for a particular Relying Party. Each Relying Party has an obligation to report any misuse of any VIP Credential in accordance with Section 4.2.2.5 of this Policy.

3.6.3.4 Who can Re-enable a Credential?

Only an End User can request a Relying Party to send a request to the Network Operator to re-enable its *Disabled* VIP Credential. A VIP Credential may only be re-enabled for that Relying party by the Network Operator upon the Network Operator's receipt of a request from the Relying Party to re-enable such VIP Credential. The Relying Party shall only send such a request once it has (i) identified the End User with sufficient second factor authentication, (ii) confirmed that the End User is in possession of such VIP Credential in accordance with Section 3.2 above and (iii) confirmed that the VIP Credential was not *Disabled* for a reason that is potentially harmful to the VIP Network.

3.6.4 Synchronization of OTP-Only VIP Credentials

Synchronization will allow for the synchronization or re-synchronization of an OTP-only VIP Credential on the VIP Network.

3.6.4.1 Circumstances Requiring Synchronization

It is possible for a VIP Credential to get out of sync with the Network Operator if OTPs are generated on an event-based VIP Credential without being validated on the VIP Network or, if the time-based VIP Credential has not been validated on the VIP Network for an extended period of time.

3.6.4.2 Who can Synchronize a VIP Credential

Upon receipt of a request for re-synchronization by an End User, the applicable Relying Party shall request that the Network Operator re-synchronize such End User's VIP Credential. The Relying Party shall request that the Network Operator resynchronize the VIP Credential only after it has (i) identified the End User with sufficient second factor authentication and (ii) confirmed that the End User is in possession of such VIP Credential in accordance with Section 3.2 above.

3.6.5 Deactivation of VIP Credentials

Deactivating a VIP Credential is the process of changing the status of the VIP Credential from *Enabled*, *Locked* or *Disabled* to *Inactive* for a particular Relying Party. An *Inactive* VIP Credential cannot be used by that Relying Party until it has been re-*Activated*.

3.6.5.1 Circumstances Requiring Deactivation

Examples of situations where a VIP Credential may be deactivated on the VIP Network for a particular Relying Party:

- It is being used in a manner contrary to this Policy
- The End User has reported the VIP Credential is lost, stolen or destroyed
- The End User has terminated his/her relationship with the Relying Party
- The End User no longer wishes to use his/her VIP Credential with the Relying Party
- The VIP Credential is no longer operational
- The End User reports that it suspects that the VIP Credential has been compromised
- The VIP Credential's continued use on the VIP Network is considered potentially harmful to the VIP Network

3.6.5.2 Who can Request Deactivation?

An End User of a VIP Credential may request a Relying Party to send a request to the Network Operator to *Deactivate* the VIP Credential for that Relying Party on the VIP Network.

A Relying Party may request the Network Operator directly to *Deactivate* a VIP Credential for that Relying Party on the VIP Network if in its sole discretion such action is warranted in terms of this Policy.

The Network Operator shall also have the ability to *Deactivate* a VIP Credential on the VIP Network, if in its sole discretion such action is warranted in terms of this Policy.

3.6.5.3 Who can Deactivate a VIP Credential

Relying Parties who have coordinated the *Activation* of a particular VIP Credential can request that the Network Operator *Deactivate* such VIP Credential for that Relying Party's use on the VIP Network. The Network Operator can *Deactivate* any VIP Credential for any VIP Network Participant. Each Relying Party has an obligation to report any misuse of any VIP Credential in accordance with Section 4.2.2.5 of this Policy.

3.6.6 Revoking of VIP Credentials

Revoking a VIP Credential is the process of changing the global status of the VIP Credential from *Valid* to *Revoked* on the VIP Network. A *Revoked* VIP Credential cannot be used on the VIP Network by any Relying Party.

3.6.6.1 Circumstances Requiring Revocation

Examples of situations where a VIP Credential may be *Revoked* on the VIP Network:

- It is being used in a manner contrary to this Policy
- The End User has reported the VIP Credential is lost, stolen or destroyed, and the Network Operator can reasonably confirm this
- The Credential Issuer has reported the VIP Credential is lost, stolen or destroyed, and the Network Operator can reasonably confirm this
- The VIP Credential is no longer operational
- The VIP Credential has been compromised
- The VIP Credential's continued use on the VIP Network is considered potentially harmful to the VIP Network, in the sole discretion of the Network Operator

3.6.6.2 Who can Request Revocation?

An End User of a VIP Credential may request the Credential Issuer which issued such VIP Credential or a Relying Party which has *Bound* such VIP Credential to an End User identity to send a request to the Network Operator to *Revoke* the VIP Credential on the VIP Network.

A Credential Issuer which issued a VIP Credential or a Relying Party which has *Bound* a VIP Credential to an End User identity may request the Network Operator directly to Revoke such VIP Credential on the VIP Network if in its sole discretion such action is warranted in terms of this Policy.

The Network Operator shall also have the ability to *Revoke* a VIP Credential on the VIP Network, if in its sole discretion such action is warranted in terms of this Policy.

3.6.6.3 Who can Revoke a VIP Credential

Only the Network Operator can *Revoke* a VIP Credential on the VIP Network.

Each Relying Party has an obligation to report any misuse of any VIP Credential in accordance with Section 4.2.2.5 of this Policy.

4 Roles and Responsibilities

4.1 Network Operator

The Network Operator operates the secure infrastructure supporting the use of IPT Credentials across the IPT Network and shall comply with the requirements described in this Section. For purposes of the IPT Network and this Policy, Symantec is the Network Operator.

4.1.1 Security Requirements

The Network Operator is responsible for establishing policies and procedures for the secure operation of the VIP Network and may take any action that, in its sole discretion, it deems necessary to protect the integrity of the VIP Network. This includes the right to shut down any VIP Participant or to *Revoke* a VIP Credential if misuse of the VIP Network by a VIP Participant or a VIP Credential is detected or suspected.

The Network Operator shall use commercially reasonable efforts to secure the systems maintaining VIP Network software and data files from unauthorized access. Symantec undergoes an annual AICPA Service Organizations Control (SOC) audit of its datacenter. The most current SOC audit report will be made available to any Credential Issuer or any Relying Party upon request by such party.

4.1.2 Operational Requirements

4.1.2.1 Accreditation of Participants and Devices

The Network Operator is responsible for

- Accrediting different Devices for use with VIP Credentials on the VIP Network
- Accrediting Credential Issuers and Relying Parties on the VIP Network

4.1.2.2 Network Operation

The Network Operator shall:

- Activate VIP Credentials on the VIP Network
- Respond to all requests from VIP Participants (other than End Users) for current VIP Credential status (enabled, disabled, locked etc.)
- Maintain and communicate up to date VIP Credential status on the VIP Network

- Validate OTP values
- Perform all Credential Lifecycle Functions on behalf of Relying Parties

4.1.3 Privacy Requirements

4.1.3.1 Privacy Policy

The Network Operator shall maintain a privacy policy that conforms to applicable privacy laws.

Symantec participates in the VIP Network as the Network Operator as well as a Credential Issuer through the Symantec Validation and ID Protection Center. As a Credential Issuer, Symantec will obtain private, End User information. Any private End User information received by Symantec, as a Credential Issuer, shall by subject to Symantec's privacy policy and applicable privacy laws.

4.1.3.2 Information Treated as Private

The Network Operator shall not obtain any private End User information associated with any VIP Credentials. With respect to each VIP Credential, the Network Operator only maintains the shared secret and VIP Credential identifier that are anonymous and do not include any personal information of any End User. This VIP Credential identification information used by the Network Operator to validate VIP Credentials on the VIP Network will be treated as private by the Network Operator and shall be subject to the Network Operator's privacy policy.

VIP Credential status information (enabled versus inactive) is not regarded as private Information.

4.1.4 Liability

When validating a VIP Credential on the VIP Network, the Network Operator determines that the VIP Credential is Valid on the VIP Network, Enabled for the requesting Relying Party, and that the OTP value generated from the VIP Credential is associated with the VIP Credential ID. Symantec makes no representations about VIP Credentials and shall not be held liable for damages relating to the use of any VIP Credential outside its control.

4.2 Relying Parties

A Relying Party is any entity that accepts any VIP Credential pursuant to the terms of this Policy. Relying Parties are required to adhere to the requirements of this Section.

4.2.1 Security Requirements

Relying Parties shall be able to properly identify users with appropriate authentication means such as secret questions/answers or out of band authentication.

Relying Parties shall secure End User information by:

- Protecting all login information using a secure channel such as Secure Socket Layer (SSL) technology
- Protecting the security of its network containing the Binding of a VIP Credential to an End User identity. At a minimum Relying Parties shall use firewalls to protect their networks from internal and external intrusion and limit the nature and source of network activities that may access production systems.

4.2.2 Operational Requirements

4.2.2.1 Network Participation

A Relying Party is responsible for representing itself as an accredited Relying Party on the VIP Network by prominently displaying the VIP logo at all places that VIP Credentials are requested from End Users. Additionally, a Relying Party agrees to be included on any list of Accredited VIP Participants maintained and published by the Network Operator.

4.2.2.2 Activating a Credential

When Activating a VIP Credential for its use on the VIP Network, a Relying Party shall:

- Obtain all the necessary End User identification information
- Obtain all the necessary VIP Credential identification information
- Require the End User to agree to terms and conditions of VIP Credential usage in a form substantially similar to the form provided by the Network Operator
- Securely transmit requests to Symantec to validate the VIP Credential identification information and coordinate the Activation of the VIP Credential for the Relying Party on the VIP Network.

4.2.2.3 Credential Management

Relying Parties are responsible for proper management of VIP Credentials they have Activated and Bound for their use on the VIP Network. These responsibilities include:

- Promptly Disabling or Deactivating VIP Credentials for fraudulent or suspected fraudulent use, or, upon notification, that the VIP Credential has been lost or stolen, or, upon request, from the End User.
- Providing first level support to End Users of VIP Credentials that it has coordinated the Activation of and Bound.
- Providing a means for End Users to manage their VIP Credentials
- Providing all Credential Lifecycle Functions described in Section 3.6

4.2.2.4 Relying on Credentials

A Relying Party shall accept all Valid VIP Credentials. Before relying on a VIP Credential, the Relying Party shall first coordinate the Activation of the VIP Credential with the Network Operator for its use on the VIP Network. The Relying Party will then *Bind* the VIP Credential to the End User identity within its own system.

When relying on a VIP Credential, the Relying Party shall use a primary authentication method that is separate from the VIP Credential.

4.2.2.5 Reporting Misuse

Relying Parties shall inform the Network Operator of fraudulent or suspected fraudulent use of a VIP Credential, or upon notification, that the VIP Credential has been lost or stolen.

4.2.2.6 Alternative Authentication Methods

In the event an End User is unable to use a VIP Credential through loss, damage or any other reason, the Relying Party must provide an alternative means to authenticate the End User. The Relying Party shall provide a secure mechanism to verify the identity of the End User and allow access to the Relying Party site, until a new VIP Credential has been *Activated* for the End User or the original VIP Credential is again usable.

The End User's identity may be verified in a variety of ways based on that entity's security policies, including:

- An answer to a predefined secret question(s)
- An out of band authentication on that End User
- In-person proofing (in a bank branch, for example)

A temporary password issued in this manner shall not be valid for longer than 7 days, after which time a new temporary password must be issued.

4.2.3 Privacy

4.2.3.1 Privacy Policy

A Relying Party shall maintain a privacy policy that conforms to applicable privacy laws.

4.2.3.2 Information Treated as Private

All information supplied by an End User to a Relying Party in the process of Activating and Binding a VIP Credential to that End User shall be treated as private information and shall be subject to Relying Party's privacy policy.

VIP Credential status information is not regarded as private information.

4.2.4 Liability

Relying Parties bear the risk of relying on a valid VIP Credential that they have Activated and Bound to the identity of an End User.

4.3 Credential Issuer

A Credential Issuer is an entity that issues VIP Credentials for use on the VIP Network. Credential Issuers shall comply with the requirements described in this Section.

4.3.1 Security Requirements

Credential Issuers shall ensure the security of End User information by:

- Protecting all data supplied by an End User for the purposes of credential issuance using a secure channel such as Secure Socket Layer (SSL) technology.
- Protecting the security of its network. At a minimum, Credential Issuers shall use firewalls to protect their network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

4.3.2 Operational Requirements

4.3.2.1 Network Participation

Credential Issuers are responsible for representing themselves as accredited Credential Issuers on the VIP Network by prominently displaying the VIP logo:

- At all places they provide VIP services to End Users
- On Devices with VIP Credentials issued by the Credential Issuer.

Additionally Credential Issuers agree to be included on any lists of accredited VIP Participants maintained and published by the Network Operator.

4.3.2.2 Issuing a Credential

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

- Obtain all the necessary End User identification information
- Obtain all the necessary VIP Credential identification information
- Require the End User to agree to terms and conditions of VIP Credential usage in a form substantially similar to the form provided by the Network Operator

4.3.3 Privacy Requirements

4.3.3.1 Privacy Policy

Credential Issuers shall maintain a privacy policy that conforms to applicable privacy laws.

4.3.3.2 Information Treated as Private

All information supplied by an End User to a Credential Issuer in the process of obtaining a VIP Credential shall be treated as private information and shall be subject to Credential Issuer's privacy policy.

4.3.4 Liability

A Credential Issuer is responsible for providing a Valid VIP Credential to an End User. A Credential Issuer makes no other representations about a VIP Credential and shall not be liable for damages relating to the use of a valid VIP Credential if it has acted in accordance with this Policy in providing issuing services.

4.4 End User

The End User of a VIP Credential is the person to whom a valid VIP Credential has been issued.

4.4.1 Security Requirements

End Users are responsible for the security of their VIP Credentials. At a minimum, End Users shall:

- Ensure the VIP Credential is kept separate from any primary authentication data.
- Notify the Credential Issuer or a Relying Party in the event a VIP Credential has been lost, stolen or otherwise compromised.

4.4.2 End User Obligations

End Users shall at a minimum:

- Provide accurate information to a Credential Issuer when obtaining a VIP Credential
- Provide accurate information to a Relying Party when Activating a VIP Credential
- Use the VIP Credential for legal purposes only.
- Use the VIP Credential only at accredited VIP Relying Party websites

4.4.3 Liability

End Users may be liable to any party for any damages caused by a failure of the End User to perform in terms of this Policy.

5 Policy Administration

5.1 Organization Administering the Document

Symantec Corporation
350 Ellis Street
Mountain View CA 94043
USA

5.2 Contact Information

Symantec Validation and ID Protection (VIP) Network Product Manager
c/o Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000 (voice)
+1 (650) 527-8050 (fax)
vip-practices@symantec.com

5.3 Policy Amendment Procedure

Symantec reserves the right to revise this VIP Policy 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 shall solicit feedback and comments to proposed revisions of a material nature (e.g., without limitation, substantive revisions that would have material affect on VIP Participants) from Credential Issuers and Relying Parties by posting proposed revisions to the Practices Updates and Notices section of the Symantec Repository, *www.symauth.com/repository*. The comment period for any material revisions to the Policy shall be fifteen (15) calendar days, starting on the date on which the proposed revisions are posted. 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 Policy.

Glossary of Terms

Term	Definition
Activation	The process of enabling a VIP Credential for use by a particular Relying Party.
Bind	The process whereby a Relying Party ties an Activated VIP Credential to the identity of an End User on such Relying Party's website.
Credential Issuer	An entity that has the authority under the VIP Network to issue a VIP Credential.
Credential Lifecycle Functions	The primary management functions related to the lifecycle of any VIP Credential, including, Activation/Deactivation, Locking/Unlocking, Disabling/Enabling and Synchronization of OTP Only VIP Credentials
Device	The hardware or software device which protects a VIP Credential, or in which a VIP Credential is embedded, and which is accredited for use on the VIP Network by the Network Operator
Disable	Changing the status of a VIP Credential temporarily from Enabled so that it is not usable by a particular Relying Party
Enable	Changing the status of a Disabled VIP Credential to render it is Enabled and usable by the Relying Party who disabled it
End User	An individual end user of a VIP Credential, who is in possession of such VIP Credential.
Deactivate	Changing the status of an Enabled VIP Credential to Inactive so that it is not usable by a particular Relying Party
Lock	Changing the status of a VIP Credential from Enabled so that it is not usable by a particular Relying Party
Network Operator	The operator of the VIP Network.
One Time Password (OTP)	A short-lived password generated by a cryptographic algorithm used to validate a VIP Credential that is in the possession of an End User
Relying Party	Any entity that accepts any valid VIP Credential for second factor authentication.
Shared Secret	A randomly generated code associated with a VIP Credential known only to an End User and the Network Operator used to validate possession of a Credential.
Unlock	Updating the status of a Locked VIP Credential to render it Enabled and usable on the VIP Network by a particular Relying Party
Symantec Validation and ID Protection Center	The website through which Symantec offers Credential Issuing services, which can be found at: https://idprotect.verisign.com
VIP Credential	A shared secret or shared key
VIP Network	The second factor authentication based infrastructure governed by the Symantec Validation and ID Protection Authentication Network Policy, which enables the deployment and use of VIP Credentials by the Network Operator, Credential Issuers, Relying Parties and End Users.
VIP Participant	An individual or organization that is one or more of the following within the VIP Network: the Network Operator; a Credential Issuer; a Relying Party; or an End User.

Change History

History of changes: version 2.1

Description	Section & Changes made
Transition ownership & branding from VeriSign to Symantec including: name, URLs, contact info.	Throughout document, Naming: VeriSign Inc to Symantec Corporation VeriSign Identity Protection (VIP) to Symantec Validation and ID Protection (VIP) URLs: from verisign.com to symauth.com Address, phone & Email address: from verisign.com to symantec.com
Section 4.1.1 Reflect the AICPA change from SAS/70 to the SOC standard as documented in www.aicpa.org/soc.	Section 4.1.1 Symantec undergoes an annual AICPA Service Organizations Control (SOC) audit of its datacenter. The most current SOC audit report will be made available to any Credential Issuer or any Relying Party upon request by such party.