Symantec
External Certificate Authority Key Recovery Practice Statement (KRPS)

Version 2

24 April 2013

(Portions of this document have been redacted.)

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

Symantec External Certificate Authority Key Recovery Practice Statement

Revision date: April 2013

Important – Acquisition Notice

On August 9, 2010, Symantec Corporation completed the acquisition of VeriSign Inc's Authentication division. As a result Symantec is now the registered owner of this Certificate Practices Statement document and the PKI Services described within this document.

However a hybrid of references to both "VeriSign" and "Symantec" shall be evident within this document for a period of time until it is operationally practical to complete the re-branding of the Certification Authorities and services. Any references to VeriSign as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership.

Trademark Notices

Table of Contents

1. INTRODUCTION

Symantec is an approved External Certification Authority (ECA) providing PKI services in support of the United States (US) Government ECA program. As part of its ECA services, Symantec provides escrow and recovery of private encryption keys for Symantec ECA Subscribers.

The Symantec Key Recovery System (KRS) provides the computer system hardware, software, personnel and procedures to store the private encryption keys securely and recover them, when appropriate. This Key Recovery Practices Statement (KRPS) document describes the procedural and technical security controls in place to ensure that the KRS operates securely.

1.1 *OVERVIEW*

Symantec's policies and procedures for the issuance and management of ECA Subscriber certificates are defined in the Symantec ECA Certificate Practices Statement (CPS). Requirements for ECA key recovery services provided in support of ECA certificate services are defined in the Key Recovery Policy (KRP) for External Certification Authorities.

This Key Recovery Practice Statement (KRPS) describes the security and authentication controls for the Symantec KRS, and the procedures in place to ensure that encrypted data can be recovered expeditiously, when appropriate. The Symantec KRS is based on the principle that all encryption activities using ECA certificates are performed on behalf of the person or the organization that authorized the issuance of encryption certificates. Therefore, the person or the organization has the right to identify the persons authorized to recover the private key needed to decrypt information. In addition, there may be need to access encrypted information for investigative and law enforcement purposes.

For the Symantec KRS implemented in support of the Symantec ECA service, Symantec will host and manage all of the components of the KRS. Only authorized Symantec employees and contractors shall perform the role of Key Recovery Agent.

1.2 *IDENTIFICATION*

No stipulation

1.3 *COMMUNITY AND APPLICABILITY*

This section describes some of the roles and systems involved in the key recovery process.

1.3.1 Key Recovery System Roles

1.3.1.1 Key Recovery Agent (KRA)

Symantec shall appoint trusted personnel as KRAs who, using a two party control procedure with a second KRA, are authorized, as specified in this Key Recovery Practices Statement (KRPS) to interact with the KRS in order to recover an escrowed key.

1.3.1.2 Trusted Agent (TA)

Symantec shall appoint TAs who will perform identity verification and authorization of a Requestor. The TA may act as an intermediary between the Requestor and the KRA providing the encrypted recovered keys to the Requestor.

1.3.1.3 Requestor

A Requestor is the person who requests the recovery of a private encryption key. A Requestor is the Subscriber of the certificate or a third party (e.g., supervisor, corporate officer or law enforcement officer) who is authorized to request recovery of a Subscriber's escrowed key.

Internal Requestor: An Internal Requestor is any Requestor who is in the Subscriber's supervisory chain or otherwise authorized to obtain the Subscriber's key for the organization. The intent of this KRPS is not to change the policy and procedures of the organization. The Subscribers' organization shall appoint authorized Requestors to Symantec to ensure that its existing organization policy regarding access and release of sensitive information can be met. The Subscriber organization shall provide Symantec with pre-established point of contact information for the organization's Legal and Human Resources department.

External Requestor: An External Requestor is an investigator or someone outside the Subscribers' organization with authorized court order to obtain the private encryption key of the Subscriber. An external Requestor must work with an internal Requestor unless the law requires Symantec to release the Subscriber's private key without approval of the Subscriber and Subscriber's organization. The intent of this KRPS is not to change the current procedures for obtaining information about individuals in connection with such requests. Symantec and Subscribers' organizations shall appoint authorized personnel and implement the KRPS so that the existing organization policy can be met while releasing the escrowed private key.

A KRA shall validate the authorization of the Requestor in consultation with management and legal counsel, as appropriate.

1.3.1.4 Subscriber

The Subscriber is the person or device that holds a private key that corresponds to a public key listed in their certificate.

1.3.2 Key Recovery System (KRS)

The Key Recovery System (KRS) includes all the information systems used to provide key escrow and key recovery services for Symantec ECA Customers. It is comprised of the Key Recovery System Infrastructure (KRSI) components and the Key Recovery Agent (KRA) and Trusted Agent (TA) Workstations. The KRSI only responds to key recovery requests from two or more Key Recovery Agents (KRAs) operating a KRA Workstation. Section 5.2.1 contains the description of the trusted roles required to operate the KRS.

The KRSI components include: a Key Manager Database (KMD), a Key Manager Server (KMS), the Symantec Certificate Server (SCS), and the Symantec Certificate Database (SCD).

1.3.2.1 KRA Workstation

KRAs perform the recovery process using a KRA Workstation that securely communicates with the KRSI.

1.3.2.2 Key Manager Server (KMS)

The Key Manager Server (KMS) generates and encrypts the Subscriber's private encryption key. It also stores and retrieves the encrypted key in the Key Manager Database.

1.3.2.3 Key Manager Database (KMD)

The Key Manager Database (KMD) is the repository that stores Subscribers' encrypted private keys.

1.3.3 Applicability

This KRPS applies to Symantec's ECA, and Subscribers and Subscribers' organizations using Symantec ECA Certificates.

1.4 *CONTACT DETAILS*

1.4.1 Key Recovery Policy Administration Organization

The organization administering this KRPS is the Symantec Practices Development group.

1.4.2 Contact Office

The contact office for the KRPS is:

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000 (voice)
+1 (650) 527-8050 (fax)
practices@symantec.com

1.4.3 Person Performing Policy / Practice Compatibility Analysis

A compatibility analysis will be performed by the ECA Policy Management Authority (EPMA), who will ensure that Symantec's KRPS is in compliance with the ECA KRP.

2. GENERAL PROVISIONS

2.1 *OBLIGATIONS*

2.1.1 Symantec Obligations

Symantec shall:

- Obtain the EPMA approval for the KRPS.
- Provide a copy of the ECA CP, ECA KRP, approved, redacted Symantec ECA CPS and the approved, redacted Symantec ECA KRPS to the KRAs and TAs.
- Operate the KRS in accordance with the provisions of the approved KRPS.
- Notify the Subscribers when their private keys have been escrowed with the KRS (e.g., a dialog box may appear on a Subscriber's screen during the certificate request process).
- Monitor Internet traffic into and out of Symantec and review the audit logs for patterns of potentially anomalous KRA or TA activity (e.g., repeated login failures) as indicators of possible problems in the infrastructure, and initiate inquiries or investigations as appropriate.
- Protect escrowed keys, during delivery, against disclosure to any party except the Requestor.
- Make commercially reasonable efforts to ensure that each individual understands and complies with the obligations for any Key Recovery role they execute and is trained to perform their duties in accordance with this KRPS.

2.1.2 KRA Obligations

KRAs shall:

- Acknowledge receipt of the KRPS and their responsibility to operate in accordance with the provisions of this KRPS.
- Protect Subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated PKCS#12 passwords.
- Protect Subscribers' recovered keys from compromise. After providing the Requestor with the encrypted key, the KRA shall destroy the copy of the encrypted key and associated PKCS #12 password in his/her system.
- Protect all information, including the KRA key(s) that could be used to recover Subscribers' escrowed keys.
- Initiate the process to recover a Subscriber's escrowed key only upon receipt of a request from an authorized Requestor. The KRA shall authenticate the identity of the Requestor using the same process as the one used for user registration as defined in section 3.2.3 of the Symantec ECA CPS. If the Requestor makes an electronic request, the KRA shall validate that the request is digitally signed as defined in section 3.2.3.2 of the Symantec ECA CPS.
- Validate the authorization for key recovery requests, to include consultation with legal counsel when appropriate.
- Release Subscribers' escrowed keys only for properly authenticated and authorized requests from Requestors.
- Protect all information regarding all occurrences of key recovery. KRAs shall communicate knowledge of a recovery process only to the Requestor involved in the key recovery. KRAs shall not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the Requestor.
- Keep records of all key recovery requests and dispositions, including acknowledgement of receipt by the Requestor. The audit records shall not contain Subscribers' keys in any form: plaintext, split, encrypted, etc.

2.1.3 TA Obligations

Trusted Agents shall:

- Request key recovery only upon receipt of a request from an authorized requestor. The TA, as an intermediary for the KRA, shall validate the identity and authorization of the requester seeking a key recovery using the process of identification and authorization established in this KRPS;
- If the Requestor is a third party, destroy the copy of the key in his/her system after delivering the key to the Requestor;

- Protect all information that could be used to obtain a recovered key;
- Protect all information regarding all requests and occurrences of key recovery. The TA shall communicate knowledge of any recovery process with only the specific Requestor. The TA shall communicate any information regarding a key recovery request with a Subscriber only when the Subscriber is the Requester;
- Accurately represent themselves to all entities when requesting key recovery services; and,
- Maintain records of all recovery requests and disposition. Audit records shall not contain Subscribers' keys in any form: plaintext, split, encrypted, etc.

2.1.4 Requestor Obligations

Prior to receiving a recovered key, the Requestor must formally acknowledge and agree to the following obligations:

- Requestors shall protect Subscribers' recovered key(s) from compromise. Requestors shall use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their keys and recovered Subscribers' keys. When the Requestor is not the Subscriber, the Requestor shall destroy Subscribers' keys when no longer required (i.e., when the authorized data has been recovered).
- Requestors shall request the Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- Requestors shall use the Subscriber's recovered keys only to recover Subscriber's data they are authorized to access.
- Requestors shall accurately represent themselves to all entities during any key recovery service. If the Requestor sends a digitally signed e-mail, the signature must be verified using a Symantec ECA issued credential of the same or higher assurance level as the key being recovered.
- A Requestor who is not a Subscriber shall protect information concerning each key recovery operation. The Requestor shall communicate information concerning the recovery to the Subscriber when appropriate as determined by the reason for the recovery. A determination whether or not to notify the Subscriber shall be based on the law, and Subscriber organization's policies and procedures for third party information access. In the event that the Requestor notifies the Subscriber of a key recovery, the Requestor shall advise the Subscriber to determine whether or not the recovery circumstances warrant revoking the associated public key certificate.
- As a condition of requesting a recovered key, a Requestor who is not a Subscriber shall sign a Key Recovery Acknowledgment Form which includes an agreement to follow the law and the Subscriber' s organization policies relating to protection and release of the recovered key.

The Key Recovery Acknowledgment Form shall include the following statement: *"I hereby state that I have legitimate and official need to recover this key in order to obtain (recover) the encrypted data that I have authorization to access. I acknowledge receipt of a recovered ECA encryption key associated with the Subscriber identified here. I certify that I have accurately identified myself to Symantec, and truthfully described all reasons that I require access to data protected by the recovered key. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to Symantec when no longer needed. I understand that I am bound by Subscriber' s organization policies, applicable laws and Federal regulations concerning the protection of the recovered key and any data recovered using the key."*

2.1.5 Subscriber Obligations

Subscribers shall comply with the following provisions:

- Subscribers shall provide accurate identification and authentication information during initial registration and subsequent key recovery requests.
- When the Subscriber is notified that his or her escrowed key has been recovered, the Subscriber shall determine whether revocation of the public key certificate associated with the recovered key is necessary. The Subscriber shall request the revocation, if necessary.

2.2 *LIABILITY*

2.2.1 Warranties and Limitations on Warranties

Symantec's key recovery procedures are implemented in accordance with the Key Recovery Policy (KRP) for External Certification Authorities (ECA), the Symantec's ECA CPS and this KRPS. All key escrow and recovery is done in accordance with the provisions of these documents.

Symantec warrants that its KRAs operate in accordance with the Key Recovery Policy for ECAs and this KRPS.

The TA representations described in section 9.6.5 of the ECA CPS similarly apply to this KRPS.

2.2.2 Damages Covered and Disclaimers

Other than the warranties included in Section 2.2.1, and to the extent permitted by applicable law, Symantec disclaims all possible warranties, including any warranty of merchantability or fitness for a particular purpose.

2.2.3 Loss Limitations

The limits for losses due to actions by Symantec in variance to this KRPS are set out in the Symantec ECA CPS Section 9.8.

Symantec disclaims any liability for loss due to improper use of a recovered key, if the key was recovered in accordance with this KRPS.

2.2.4 Other Exclusions

No Stipulation.

2.2.5 US Federal Government Liability

Subscribers and Requestors shall have no claim against the US Federal Government arising from use of the Subscriber' s recovered private key or for the ECA' s inability to recover a private key. In no event will the Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any key escrow or recovery operation, or non-performance of a key escrow or recovery operation.

Subscribers and Requestors shall have no claim against the US Federal Government arising from erroneous key escrow and key recovery operations by Symantec.

Symantec shall have no claim for loss against the EPMA.

2.3 *FINANCIAL RESPONSIBILITY*

2.3.1 Indemnification by Relying Parties and Subscribers

Neither Symantec nor its agents shall assume financial responsibility to Relying Parties and Subscribers for improper use of a recovered key by a Requestor.

2.3.2 Fiduciary Relationships

Symantec is not an agent, fiduciary, trustee, or other representative of Subscribers or Requestors, and escrow and recovery of private keys in accordance with this KRPS does not make Symantec an agent, fiduciary, trustee, or other representative of Subscribers or Requestors.

2.4 *INTERPRETATION AND ENFORCEMENT*

2.4.1 Governing Law

Governing law shall be in accordance with section 9.14 of the Symantec ECA CPS.

This governing law provision applies only to this KRPS. Agreements incorporating the KRPS by reference may have their own governing law provisions, provided that this KRPS § 2.4.1 governs the enforceability, construction, interpretation, and validity of the terms of the KRPS separate and apart from the remaining provision of such agreements, subject to any limitation appearing in applicable law.

This KRPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

2.4.2 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this KRPS is incorrect or invalid, the other sections of this KRPS shall remain in effect until the KRPS is updated.

2.4.3 Conflict Provision

In the event of a conflict between this KRPS or the cited provisions of the CPS, and the KRP or CP, the KRP and CP shall take precedence. Any conflict will be brought to the immediate attention of the EPMA.

2.4.4 Dispute Resolution Procedures

The EPMA shall be the sole arbiter of disputes arising over the interpretation or applicability of the KRP.

2.4.4.1 Notification among Parties to a Dispute

Before invoking any dispute resolution mechanism (including litigation or arbitration), with respect to a dispute involving any aspect of this KRPS, aggrieved persons shall notify Symantec and any other party to a dispute for the purpose of seeking dispute resolution among themselves.

2.4.4.2 Disputes with Subscriber or Relying Parties

Resolution of disputes with Subscribers or Relying parties shall be in accordance with section 9.13 of the Symantec ECA CPS.

2.5 *FEES*

Symantec is entitled to charge ECA customers for the provision of key recovery services.

2.6 *PUBLICATION AND REPOSITORY*

Not Applicable.

2.7 *COMPLIANCE AUDIT*

2.7.1 Frequency of Entity Compliance Audit

An audit of the KRS shall be conducted annually in conjunction with Symantec's Certification Authority (CA) audit. The scope of the audit shall include all the KRAs and TAs in accordance with the ECA CPS Compliance Audit.

In the event a KRA or TA is relieved of responsibility due to a failure to comply with this KRPS, Symantec shall direct a special compliance audit. The purpose of the audit will be to determine whether any key recovery activities of the removed KRA or TA may have been improper or may have affected the integrity of the KRS.

2.7.2 Identity/Qualifications of Compliance Auditor

The auditor shall demonstrate competence in the field of security compliance audits of Information Technology (IT) systems, and shall be thoroughly familiar with Symantec's KRPS and cited provisions of the Symantec ECA CPS. The compliance auditor shall perform PKI or IT system compliance audits as a primary responsibility. In addition, the compliance auditor shall have expertise in information security, cryptography and PKI in accordance with section 8.2 of the ECA CPS.

2.7.3 Compliance Auditor's Relationship to Audited Party

The compliance auditor shall be an independent contractor (e.g., a third party auditing firm such as KPMG) that has a contractual relationship for the performance of the compliance audit.

2.7.4 Topics Covered by Compliance Audit

All the topics identified in this KRPS document and the cited ECA CPS provisions will be covered by the compliance audit. The purpose of a compliance audit shall be to verify that the KRS operates in accordance with this KRPS and the cited provisions of the Symantec ECA CPS and has requisite procedures and control in place to operate securely. The compliance auditor will examine the computer security audit and other records of the KRS, including the various KRSI components and the KRA and TA Workstation to ensure that they are consistent with respect to the key recovery activities.

2.7.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy with the provisions of the KRPS, the following actions must occur:

- The compliance auditor shall note the discrepancy in an audit report; and
- The audited entity shall propose a remedy, including expected time for inclusion in the audit report.

2.7.6 Communication of Results

The compliance auditor will submit a report of the compliance audit to the EPMA and to Symantec.

2.8 *CONFIDENTIALITY*

2.8.1 Type of Information to be Protected

Symantec and the company TA protect personal or sensitive information used to identify and authenticate participants in the recovery process. Such information may include: Social Security Number (SSN), identification credential serial numbers, and affiliation with investigative agencies, when specified by the Requestor as sensitive. All such sensitive information is maintained and stored in cabinets in a Tier 4 area accessible only by authorized, trusted personnel.

When key recovery is requested as part of an investigation or court order, information concerning the request shall also be protected.

2.8.2 Information Release Circumstances

The identity of the Requestor of escrowed keys shall be authenticated per Section 3. Symantec shall not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless:

- Authorized by this KRPS; or
- Required by the law or government rule or regulation; or
- Required by the Subscriber' s organization policy; or
- Required by order of a court of competent jurisdiction.

3. IDENTIFICATION AND AUTHENTICATION

Symantec shall verify the Requestor's identity and authorization to access the requested escrowed key. The Requestor's authenticated identity shall be used as the basis for determining access permissions and providing Requestor accountability.

3.1 *IDENTITY AUTHENTICATION*

Identity authentication shall be based on the activities specified in section 3.2 of the Symantec ECA CPS for authentication of individual identity during initial certificate enrollment or shall be based on digital signatures that can be verified using Symantec ECA public key certificates. A Requestor may appear before a KRA, Trusted Agent, or Notary Public for in-person identity proofing in accordance with the ECA CPS[1]. If identity authentication is based on digital signatures, the assurance level of a certificate used for identity authentication of a Requestor shall be commensurate with the assurance level of the ECA certificate associated with the key being recovered.

3.2 *THIRD PARTY REQUESTOR*

A third party Requestor is an individual other than the Subscriber and may be a representative of the Subscriber's organization (ie, an internal requestor), or a representative of a law enforcement agency (ie, an external requestor).

The following subsections identify the requirements for authentication and authorization of a third party Requestor. The requirements for authentication and authorization of a Requestor that is the Subscribers, are addressed in Section 3.3.

3.2.1 Requestor Authentication

Organization Representative

All organization representatives must complete a Key Recovery Request Form to request recovery of a private key belonging to a Subscriber in their organization. All organization representatives must appear before a KRA, Trusted Agent or Notary Public for identity authentication and completion of the Key Recovery Request Form. The Symantec KRA, Trusted Agent or Notary Public shall personally verify the identity of the Requestor using the procedures defined in the Symantec ECA CPS for initial Subscriber enrollment.

If the Requestor appears before a KRA, the KRA authenticates the Requestor's identity and signs and archives the Key Recovery Request Form.

If the Requestor appears before a Trusted Agent, the Trusted Agent authenticates the Requestor's identity, signs and retains a copy of the Key Recovery Request Form, and sends a digitally signed and encrypted message (using a Symantec ECA digital certificate) to a Symantec KRA requesting recovery of the Subscriber's key.

If the Requestor appears before a Notary Public, the notary authenticates the Requestor's identity, signs and notarizes the Key Recovery Request Form and returns the form to the Requestor. The Requestor shall mail the notarized Key Recovery Request Form to a Symantec KRA by first class postal mail, Federal Express or any similar method. The KRA shall examine the form to verify that it has been properly completed and notarized and shall archive the form.

Law Enforcement Representative

If the Requestor is a representative of a law enforcement agency, the Requestor must complete a Key Recovery Request Form and establish his or her identity to a Symantec KRA or Notary Public who shall personally verify the identity of the Requestor using the procedures defined in the Symantec ECA CPS for initial Subscriber enrollment.

[1] All stipulations within the KRPS referring to the choice of using either a KRA, Trusted Agent or Notary Public shall be enforced in accordance with details described in the ECA CPS.

If the Requestor appears before a KRA, the KRA authenticates the Requestor's identity and signs and archives the Key Recovery Request Form.

If the Requestor appears before a Notary Public, the notary authenticates the Requestor's identity, signs and notarizes the Key Recovery Request Form and returns the form to the Requestor. The Requestor shall mail the Key Recovery Request Form to a KRA by first class postal mail, Federal Express or any similar method. The KRA examines the form to verify that it has been properly completed and notarized and archives the form.

3.2.2 Requestor Authorization Verification

The Symantec KRA that performs identity authentication of a Requestor shall also verify the authorization of the Requestor. A Trusted Agent that performs identity authentication of Requestor who is an authorized representative of the Subscriber's organization shall also verify the authorization of the Requestor.

Authorization Verification by Trusted Agent

After personally authenticating the identity of an authorized representative of the Subscriber's organization or after receiving a notarized Key Recovery Request form from an authorized representative of the Subscriber's organization, the Trusted Agent for the organization shall verify the Requestor's authorization by consulting with the Legal or Human Resources department of the organization to verify that the requestor is authorized to request recovery of the Subscriber's key. The mechanism to validate the authorization shall be via telephone, postal mail, or a comparable procedure.

The Trusted Agent shall sign the form confirming that the Requestor is authorized to request recovery, archive the form, and shall send a digitally signed and encrypted message (using a Symantec ECA digital certificate) to a Symantec KRA requesting recovery of the Subscriber's key.

Authorization Verification by KRA

If the Requestor is an authorized representative of the Subscriber's organization, the Symantec KRA shall validate the authorization by consulting with the Legal or Human Resources department of the Subscriber's organization to verify that the Requestor is authorized to request recovery of the Subscriber's key. The mechanism to validate the authorization shall be via telephone, postal mail, or a comparable procedure.

If the Requestor is not an authorized representative of the Subscriber's organization, the Symantec KRA shall review the Requestor-submitted court-issued subpoena or order, and shall validate the authorization of the Requestor in consultation with Symantec management and legal counsel, as appropriate. Any consultation with the Legal or Human Resources department of the Subscriber's organization is subject to applicable law.

3.3 *SUBSCRIBER*

3.3.1 Subscriber Authentication

If the Subscriber has a current, valid Symantec ECA certificate, he/she may authenticate by sending a digitally signed message directly to a KRA. The assurance level of the Symantec ECA authentication certificate used shall be equal to or greater than that of the certificate whose corresponding private key is being recovered. A KRA shall authenticate the identity of the Subscriber by validating the digital signature on the message.

If the Subscriber does not have a current or valid Symantec ECA certificate or chooses not to authenticate by sending a digitally signed message, the Subscriber must establish his or her identity by personally appearing before a Symantec KRA, a Trusted Agent or a Notary Public for personal presence identity proofing using the procedures defined in the ECA CPS for initial Subscriber enrollment.

If the Subscriber appears before a notary public, the notary authenticates the Subscriber's identity, signs and notarizes the Key Recovery Request Form and returns the form to the Subscriber. The Subscriber shall mail the notarized Key Recovery Request Form to the Symantec KRA via first class postal mail, Federal Express or any

other similar method. The KRA shall examine the form to verify that it has been properly completed and notarized and shall archive the form.

If the Subscriber appears before a Trusted Agent for the Subscriber's organization, the Trusted Agent authenticates the Subscriber's identity, signs the Key Recovery Request Form, archives the form and shall send a digitally signed and encrypted message (using a Symantec ECA digital certificate) to a Symantec KRA requesting recovery of the Subscriber's key.

3.3.2 Subscriber Authorization Verification

If the Subscriber is authenticated by a KRA by validating the digital signature on a signed message received from the Subscriber and signed using a current, valid ECA certificate, or if the Subscriber submits a notarized Key Recovery Request Form no further authorization checks are required.

If a Subscriber is authenticated by personally appearing before a Trusted Agent or by appearing before a Notary Public and submitting a notarized Key Recovery Request Form to the Trusted Agent, the Trusted Agent shall consult with the Legal or Human Resources department of the Subscriber's organization to verify that the Subscriber is authorized to recover the key and shall verify that the recovered key is being sent to the Subscriber's authenticated e-mail address included in the original certificate.

3.4 *KRA AND KRO AUTHENTICATION*

3.4.1 KRA Authentication

KRAs shall be trusted Symantec personnel. The KRA shall authenticate to the SCS using a Symantec Trust Network (STN) Class 3 Administrator certificate with the KRA key pair generated and stored on FIPS 140-1 Level 2 hardware token. Identity proofing for a STN Class 3 Administrator certificate is performed by a Symantec CMA as defined in Symantec ECA CPS section 1.3.3.

The KRA authentication is performed via client-authenticated SSL by using the STN Class 3 Administrator certificate to create the SSL session. Additionally this STN Class 3 Administrator certificate is used for KRA authentication and authorization to perform KRA functions as follows:

- The certificate is confirmed to be valid through full path validation including CRL and certificate expiration checks and signed by the trusted Class 3 Onsite Enterprise Administrator CA. Only the Symantec Class 3 Onsite Enterprise Administrator CA issues certificates to only account PKI Administrators (i.e., RA and KRA).
- The O and OU attribute values within the Subject DN are used to identify the KRA's jurisdiction; the KRA may perform KRA functions for only recovery requests with the identical O and OU values. Only individuals that have been authorized to perform the ECA KRA role are issued a STN Class 3 Administrator certificate with the O and OU values corresponding to the ECA jurisdiction. A fraudulent request for a Class 3 Admin Certificate Request with an O and OU corresponding to the ECA jurisdiction will be rejected for failing the strict authentication requirements.[2]
- The O, OU, CN and email address within the Subject DN and are used in a lookup of authorized KRA permissions pre-established within the CA system by individuals in the role of Master PKI Administrator. If the lookup succeeds, the KRA is provided with options and data corresponding to the privileges retrieved in the lookup. If the lookup fails, the KRA authentication is rejected.

The KRA does not have more than one identity on the CA or KMS and shall not have more than one Class 3 Administrator certificate in accordance with the ECA CPS, section 5.2.4. The Administrator certificate issued to the KRA shall be restricted for use in key recovery and RA functions only; using the certificate for any other purposes shall not be permitted.

[2] The STN Class 3 Administrator certificates are issued under the High Assurance level which includes authentication of the organization name (O) contained within the certificate and a confirmation from the organization of the authorization of the person to act as Administrator.

The KRA individual is issued a Class 3 Administrator Certificate containing the individual's email address within the Subject DN. During the Class 3 certificate enrollment processes, the email address is validated to be unique within the Class 3 CA domain and is reasonably associated with that specific applicant by manual review. The email address value is signed by the Class 3 CA at certificate issuance and ad-hoc changes are not permitted.

Identity proofing of the KRA for a Class 3 Administrator certificate shall be done in person by a Symantec CMA as defined in Symantec ECA CPS section 1.3.3.

3.4.2 TA Authentication

The KRA authenticates the TA by verifying the validity of the digital signature on the signed email message. The subject name of the digital signature is verified against a valid TA List. The TA certificate enrollment is described in the ECA CPS, section 1.3.6.3.

4. OPERATIONAL REQUIREMENTS

4.1 *ESCROWED KEY RECOVERY REQUESTS*

4.1.1 Who Can Request Recovery of Escrowed Keys

Subscribers may request recovery of their own escrowed keys. Key recovery may also be requested by the personnel permitted by the Subscriber's organization policy, as verified by the organization, and by authorized law enforcement personnel with court order from a competent court.

4.1.2 Requirements for Requesting Escrowed Key Recovery

Persons requesting recovery of escrowed keys are required to provide sufficient information that can be used by Symantec to verify their identity and authorization according to section 3 of this KRPS.

Subscribers may use electronic or manual means to request their own escrowed keys from the KRS. If the request is made electronically, the Subscriber shall digitally sign the request using a Symantec issued ECA authentication certificate of assurance level equal to or greater than that of the escrowed key. Manual requests shall be in writing and shall be signed by hand.

Third party Requestors may use electronic or manual means to request recovery of a Subscribers' escrowed key. The Requestor shall submit the request to a Symantec KRA. If the request is made electronically, the Requestor shall digitally sign the request using a Symantec issued ECA Certificate of assurance level equal to or greater than that of the escrowed key. Manual requests shall be in writing and shall be signed by hand.

Requests from law enforcement must be under cover of a court-issued subpoena or order authorizing a particular law enforcement official or department to recover a Subscriber's encryption key.

4.2 *PROTECTION OF ESCROWED KEYS*

Escrowed keys are encrypted and stored within the protected KMD. For enhanced security the information required to decrypt the escrowed keys is stored in separate components of the KRS system (see section 4.2.1.1 for more details). Escrowed keys are protected during delivery to the Requestor by a combination of electronic transmission of a PKCS #12 encrypted file to the authenticated requestor and the delivery of the password to access the PKCS#12 file using a separate communication method.

4.2.1 Key Escrow and Recovery through Symantec

Symantec shall provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access shall require the actions of at least two trusted KRAs. (Note: The KRS enforces two person control. A key recovery request cannot be initiated by only one KRA).

All copies of escrowed keys are protected continuously using two person control procedures during recovery. The protection mechanisms include separation of the recovered key and the password for that key.

4.2.1.1 Key Escrow Procedure

The key escrow process flow is described as follows:

1. The Subscriber enrollment request for an ECA Encryption certificate is received by the Certificate Enrollment Web Server.

2. The request is forwarded to the KMS

12. The Subscriber Encryption certificate is then sent to the Certificate Enrollment Web Server for forwarding to the Subscriber.

4.2.1.2 Key Recovery Procedure

For each Key Recovery Request, once the process is initiated, the individual performing either the KRA1 or KRA2 role strictly perform only the functions of that single role from start to end. No substitute KRA shall be allowed in mid-process. The process flow is described as follows:

1. Using a dedicated KRA1 Workstation, KRA1 authenticates by inserting his/her FIPS 140-1 level 2 hardware cryptographic token, logging on and presenting the KRA digital certificate stored on the token.

2. KRA1 is then presented with a query page which enables searching for any Subscriber's certificate based on Subscriber name, e-mail address or certificate serial number. After submitting the search query, the KRA can examine each of the certificates listed if necessary, to determine the correct certificate whose corresponding private key is to be recovered. After selecting the desired certificate, the KRA submits an *Authorization* for the recovery of the key selected. KRA1 then logs off the SCS.
3. Using a dedicated KRA2 Workstation, the KRA2 logs on and repeats the same steps as KRA1, including identifying the specific Subscriber's certificate whose corresponding private key is to be recovered.
   KRA2 then immediately initiates the key recovery operation without interruption or delay for subsequent retrieval of the key as described in the steps following.

4. KRA2 authenticates to the Key Recovery Web Server using the same digital certificate used to login and transmits the Key Recovery Request identifying the unique key selected from the KRA Workstation to the Key Recovery Web Server which transmits it to the KMS.

14. The PKCS #12 is sent via the Key Recovery Web Server to the KRA2 Workstation and downloaded as set forth in section 6.1 by KRA2 using the current active SSL session. Upon receipt of the PKCS #12, KRA2 logs off and closes the browser to remove all residual information held in memory.

    The KMS sends a password notification e-mail to KRA1's corporate mailbox.

16. Using the dedicated KRA1 Workstation, KRA1 authenticates to the *Password Retriever Web Server*[3] by inserting his/her FIPS 140-1 level 2 hardware cryptographic token, logging on and presenting his/her KRA digital certificate stored on the token. The *Password Retriever Web Server* authenticates that the holder of the presented certificate is on the list of approved Key Recovery Agents.
    Once the password is retrieved, it is removed from the database table. If the password is not retrieved within an established time window (configurable setting), it is marked as expired and removed from the database table, and the Key Recovery Procedure must be repeated from the beginning.

    Note that when a TA acts as an intermediary between the KRA and the Requestor in the distribution of the escrowed keys, the PKCS#12 and the associated password shall not both be delivered through the single TA. The password is distributed directly to the Requestor without a TA intermediary.

17. KRA2 decrypts and delivers the PKCS #12 to the Requestor as described in section 6.1.

4.2.2 Automated Self-Recovery

The Symantec KRS does not support automated self-recovery.

[3] The Password Retriever Web Application resides on the same physical machine as the Key Recovery Web Server and is referred to as the Password Retriever Web Server.

4.3 *CERTIFICATE ISSUANCE*

KRAs must enroll for an ECA certificate pair using the procedures defined in the Symantec ECA CPS.

4.4 *CERTIFICATE ACCEPTANCE*

KRAs must accept ECA certificates using the procedures defined in the Symantec ECA CPS.

4.5 *SECURITY AUDIT PROCEDURES*

The security auditing capabilities of the KRS are enabled upon installation and remain enabled during operation.

4.5.1 Vulnerability Assessments

A networking intrusion detection system (IDS) continuously monitors the KRSI components and KRA Workstation to detect potentially malicious activity.

4.6 *RECORDS ARCHIVAL*

Symantec maintains a trusted archive of information stored and transactions carried out.

4.7 *KRS KEY CHANGEOVER*

A list of the KRS keys and their re-key frequency is shown in Table 1 below.

Key Type	Rekey Frequency
All SSL keys	Every year
KRA keys*	Every year
KMS Admin key	Every year
KMS Master 3DES key	Never re-keyed

Table 1: KRS Re-key Table

* KRAs are issued Symantec Class 3 Administrator certificates. TAs are issued standard Symantec ECA certificates.

4.8 *KRS COMPROMISE AND DISASTER RECOVERY*

Compromise or disaster notification and recovery procedures are necessary to ensure the KRS remains in a secure state.

4.8.1 KRS Compromise

In the event that the KRS is compromised or is suspected of compromise, the EPMA shall be notified. The EPMA shall be granted sufficient access to information to determine the extent of the compromise. The EPMA shall direct the appropriate action. This may include revocation of certificates associated with the compromised private keys stored in the KRS. The audit logs shall be examined to ascertain the scope of the compromise. Those key recoveries authorized by a KRA certificate during the period that the KRA certificate was deemed compromised shall be identified and also deemed compromised. Certificate revocation is performed in accordance with the ECA CPS, section 5.7.3.

4.8.2 Disaster Recovery

Symantec has implemented a disaster recovery site at a Symantec-owned facility. Symantec has developed, implemented and tested a Disaster Recovery Plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Symantec has the capability to restore or recover operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:

- · Certificate issuance;
- · Certificate revocation;
- · Publication of revocation information; and
- · Key recovery for ECA certificates

4.9 *KRA TERMINATION*

Upon a KRA termination, Symantec shall retain possession of all KRA archive records.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 *PHYSICAL CONTROLS*

The KMS and KMD are protected as specified in the ECA CPS Section 5.1 for CA and CMA equipment. KRA workstations are protected with physical controls as specified in the Symantec ECA CPS Section 5.1 for Registration Authority (RA) and CMA equipment.

5.2 *PROCEDURAL CONTROLS*

5.2.1 Trusted Roles

The primary trusted roles defined by this KRP are the following:

5.2.1.1 Key Recovery Agent

KRAs are subject to the provisions in this KRPS.

5.2.1.2 Trusted Agent

Trusted Agents are subject to the provisions in this KRPS.

5.3 *PERSONNEL CONTROLS*

5.3.1 Background, qualifications, experience, and clearance requirements

Persons selected for KRA roles shall be US citizens and shall meet the requirements specified in the Symantec's ECA CPS Section 5.3.1 for RAs. Persons selected for other trusted roles for KRS shall meet the requirements specified for other trusted roles in Symantec's ECA CPS Section 5.3.1.

5.3.2 Background check procedures

Background check procedures are described in Section 5.3.2 of Symantec's ECA CPS.

5.3.3 Training requirements

All personnel involved in ECA key recovery operation shall be appropriately trained on the procedures applicable to them and the KRS equipment they will use to perform their duties in terms of this KRPS and the cited portions of the Symantec ECA CPS.

5.3.4 Retraining Frequency and Requirements

Significant changes to KRS operations shall require implementation of a training plan that includes any retraining required for KRS operational staff. The execution of such plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Symantec shall commence appropriate administrative and disciplinary actions against personnel who violate this KRPS.

5.3.7 Contracting Personnel Requirements

Symantec shall ensure that any subcontractors perform their duties in accordance with this KRPS, the ECA KRP and relevant portions of the ECA CP and the Symantec ECA CPS. Subcontracts shall pursue appropriate administrative and disciplinary actions against subcontractor personnel in violation of these defined duties.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

6. TECHNICAL SECURITY CONTROLS

6.1 *PROTOCOL SECURITY*

6.1.1 Escrowed Key Distribution Security

Communication of distributed copies of escrowed keys between the KRA and Requestor shall be secure from protocol threats such as disclosure, modification, replay, and substitution.

Recovered escrowed keys are cryptographically protected at all time. Recovered escrowed keys are protected during delivery to the Requestor by separating the delivery of an encrypted PKCS #12 file and the delivery of the password needed to decrypt the PKCS#12 file through different KRAs and separate channels. Note: the encrypted PKCS#12 file can only be decrypted using the password which is sent to the Requestor by a separate communication method.

6.2 *KMS AND KRA PRIVATE KEY PROTECTION*

6.2.1 Standards for Cryptographic Modules

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [current version of FIPS 140]. The KMS and KRA shall use hardware cryptographic modules that meet at least the criteria specified for FIPS 140-1 Level 2.

For all assurance levels, Subscriber encryption key pairs are generated in FIPS 140 Level 2 hardware cryptographic tokens at the KMS and never leave the boundary of the tokens.

The KRA keys are generated and stored on a FIPS 140-1 Level 2 certified USB hardware token.

6.2.2 Private Key Control

The private components of the KRA signature key pairs and encryption key pairs are under single person control.

The KRA responsible for sending the password needed to decrypt the recovered key to the Requestor shall not have access to the encrypted PKCS#12 file.

6.2.3 KMS Key Backup

The process of restoring the backup KMS key shall maintain three-party control throughout, as described in Section 6.2.5.

6.2.4 Private Key Generation and Transport

Private components of the KMS Admin key, KRA encryption key pairs and 3DES Master key are generated in and stored in hardware cryptographic modules.

6.2.5 Method of Activating Private Key

Activation of the KRA and TA private key is by a password known only by the KRA and TA, respectively. All password entry is protected with no-echo.

Activation data for the recovered private key is distributed to the Requestor separately from the cryptographic module that they activate.

6.2.6 Method of Deactivating Private Key

The private component of the KRA encryption key pair is deactivated when the KRA logs out of the KRA Workstation or if the KRA removes the hardware token from the KRA Workstation.

When not in use, hardware modules are removed and stored in accordance with physical protections described in section 5.1.2 of the ECA CPS.

6.3 *PRIVATE KEY ACTIVATION DATA*

Generation, change, and management of private key activation data shall be in accordance with the FIPS 140-1 standard.

6.4 *COMPUTER SECURITY CONTROLS*

Tools and technologies used to restrict and monitor computer and network access are described in section 6.6 of this KRPS and section 6.7 of the Symantec ECA CPS.

6.5 *LIFE CYCLE TECHNICAL CONTROLS*

Individuals with trusted roles in the KRS facility (e.g., system administrators, crypto officers, audit administrators, operators, etc.), use security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements. These tools and procedures check the integrity of the system data, software, discretionary access controls, audit profile, firmware, and hardware to ensure secure operation. See Section 4.5.8 for details of the tools and procedures used to protect the security of the KRS.

6.6 *NETWORK SECURITY CONTROLS*

6.7 *Network access controls are specified in the Symantec ECA CPS section 6.7. CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS*

Requirements for cryptographic modules are stated in section 6.2.1.

7. POLICY ADMINISTRATION

7.1 *POLICY CHANGE PROCEDURES*

This KRPS is maintained under the specification change procedures identified in Symantec's ECA CPS Sections1.5 and 9.12.

7.2 *PUBLICATION AND NOTIFICATION POLICIES*

The approved KRPS shall be published as specified in Symantec's ECA CPS Section 2.1.

7.3 *POLICY APPROVAL PROCEDURES*

This KRPS is approved based on the procedures specified in Symantec's ECA CPS Section1.5.4.

APPENDIX A: ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CC	Common Criteria
CP	Certificate Policy
CPS	Certification Practices Statement
CMA	Certificate Management Authority
CRS	Certificate Request Syntax
DES	Data Encryption Standard
DN	Distinguished Name or Directory Name
EAL	Evaluation Assurance Level
ECA	External Certification Authority
EPMA	External Policy Management Authority
FIPS	Federal Information Processing Standard
I & A	Identification and Authentication
IT	Information Technology
KMD	Key Manager Database
KMS	Key Manager Server
KRA	Key Recovery Agent
KRO	Key Recovery Official
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
KRS	Key Recovery Service
KRSI	Key Recovery System Infrastructure
PKI	Public Key Infrastructure
RA	Registration Authority
SSN	Social Security Number
TA	Trusted Agent
US	United States
USD	United States Dollar

APPENDIX B: GLOSSARY

Dual-person control	For the purpose of this KRPS, dual person control is a process that requires two or more people in order to execute certain activities involving the Key Recovery System.
Encryption Certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing, protecting, and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
Key Escrow	The retention of the private component of the key pair associated with a Subscriber's Encryption Certificate to support key recovery.
Key Recovery	Production of a copy of an escrowed key and delivery of that key to an authorized Requestor.
Key Recovery Agent (KRA)	An individual authorized to interface with the Key Recovery System in conjunction with one or more other key recovery agents) to cause the key escrow database to carry out key recovery requests, as specified by the Key Recovery Policy.
KRA Workstation	The workstation from which the Key Recovery Agent interfaces with the Key Recovery System.
Key Recovery System	The function, system, or subsystem that maintains the key escrow repository and responds to key registration and key recovery requests from one or more Key Recovery Agents, as specified by the Key Recovery Policy.
Key Recovery Official (KRO)	An individual authorized to authenticate and submit key recovery requests to the Key Recovery Agent on behalf of Requestors, as specified by the Key Recovery Policy.
Key Recovery Policy (KRP)	Specifies the conditions under which key recovery information must be created and conditions under which and to whom escrowed keys may be released; it also indicates who are allowable Key Recovery Agent(s) and Key Recovery Officials and how or where escrowed keys must be maintained.
Key Recovery Practice Statement (KRPS)	The Key Recovery Practice Statement is a statement of the practices, procedures, and mechanisms that a key escrow system employs in registering and recovering escrowed keys.
Requestor	An individual who is authorized, under the Key Recovery Policy, to request recovery of a Subscriber's escrowed key. Subscribers can always request recovery of their own keys.
Policy Management Authority	Body established to oversee the creation and update of Certificate and Key Recovery Policies, review Certification and Key Recovery Practice Statements, review the results of CA and Key Recovery audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate and Key Recovery policies.
Public Key Infrastructure	Framework established to issue, maintain, and revoke public key certificates.
Split Key Procedure	A mechanism whereby a key is cryptographically divided into some number of pieces so that when a specific-sized subset of the pieces is recombined the original key can be reconstructed.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in an entity, and (3) holds a private key that corresponds to a public key listed in that certificate. Current Subscribers possess valid ECA-issued certificates.
Third Party	A person other than the Subscriber who requests escrowed keys (e.g., law enforcement, supervisor).

APPENDIX C: ECA Key Recovery Request Form

Instructions to Requestor:

1. Print out this form.
2. Complete Sections A & B of the form. ***Do not sign the form yet.***
3. This form can only be signed by the certificate Subscriber or the company representative (e.g. organization's legal officer, security officer, or human resources representative) in the presence of your corporate notary or other notary public. You are responsible for all fees (if any) charged by the notary.
4. Bring two forms of identification with you to the notary as follows:
   -One widely recognized, government-issued Photo ID such as a Driver's License or Passport;
   And
   -One other type of identification (photo not required) such as a valid national credit card, an employee ID, a utility or tax bill, or insurance card.
5. Instruct the notary to read the instructions below and complete the Acknowledgement.
6. Sign your name (section C) in the presence of the notary.
7. Make and retain a copy of this form and the Subscriber Agreement for your records.
8. Fee: The price of a key recovery is $125.00. In case the requestor is the subscriber, it is possible to request a replacement ECA certificate pair for no additional charge (as indicated in section A below).
9. Send the completed (original) notarized form along with a copy of the Photo ID presented to the notary by First Class Postal Mail, Federal Express or other equivalent means to:

ECA Key Recovery Processing & Fulfillment
Symantec Order Fulfillment
350 Ellis Street
Mountain View, CA 94043 USA

Please ensure that the entries in these fields are accurate and legible.
A. Requestor Information:

Check the appropriate box(es) below

☐ I am the subscriber of the ECA certificate associated with the encryption private key to be recovered
   ☐ I want to revoke my existing ECA certificate pair and get a new ECA certificate pair as part of the recovery process.
   ☐ I do not want a new ECA certificate pair as part of the recovery process.

OR

☐ I am **NOT** the subscriber of the ECA certificate associated with the encryption private key to be recovered
*[**Note**: Other than the Subscriber, only an organization's **legal officer**, **security officer**, or **human resources representative**, or a **law enforcement official** (with a Court authorized order) may request recovery]*

If this box is checked, the Requester **MUST** also complete the ***ECA Key Recovery Acknowledgment Form***.

B. Information about the ECA Certificate associated to the encryption key being recovered
(This must correspond to the information in the ECA subscriber certificate)
- *First Name _____
- *Last Name _____
- *E-mail Address _____

C. Declaration (to be signed in the presence of a Notary)
I do hereby make oath and/or affirm that all the information contained in this document is true and correct and that I am duly authorized to recover the encryption key for the certificate described in Section B. As a condition of

receiving the recovered key, I hereby agree to comply with all laws and the subscriber's organization policies relating to protection and release of the recovered key.

_____
Your signature, made in the presence of a notary
- First Name _____
- Last Name _____
- Organization _____
- Postal Address _____
- E-mail Address _____
- Phone Number _____
- Fax Number _____
- Job Title _____

Instructions to Notary:
The document you are notarizing is part of the Key Recovery Request process for a Symantec Digital ID used in conjunction with programs authorized by the U.S. Department of Defense (DOD). The DOD requires that the personal identity of the requestor be validated. If you would like more information about the ECA program, please visit Symantec a*thttps://www.symantec.com/theme.jsp?themeid=eca-certificates.*

1. Modify this form where necessary to assure compliance with the laws of your jurisdiction. Use the backside of this form if necessary.
2. Complete the Acknowledgement below.
3. Request and examine at least two pieces of Subscriber identification as follows:
   - One widely-recognized, government-issued Photo ID such as a Driver's License or Passport; and
   - One other type of identification (photo not required) such as a valid national credit card, employee ID, utility or tax bill, or insurance card.
4. Administer the prescribed oath.
5. You must check the Subscriber's forms of identification even if you are acquainted with the Subscriber.

D. – This section is to be completed by Notary Public

Acknowledgement
State/Commonwealth/Province of _____)
County of _____)
Country _____)
On (date) _____, before me, _____ (notary) personally appeared_____ (subscriber), and proved to me on the basis of the presentation of the two forms of identification listed below, to be the person whose name is subscribed to the instrument, and acknowledged to me that he/she executed the same, and that by his/her signature on the instrument the person executed the instrument in my presence and took the prescribed oath.

ID#	Type of ID	Identifying Number	Expiration Date
1*			
2			

* ID #1 must be accompanied by photo.

Witness my hand and official seal.
- Notary Signature _____
- Notary Name (print) _____
- Notary Address _____
_____ (Place Seal/Stamp Here)

- Notary Phone _____
- Notary E-mail Address (optional) _____
- My Commission Expires on: _____
(Place Seal/Stamp to the right where indicated)

APPENDIX D: ECA Key Recovery Acknowledgement Form

ECA Key Recovery Acknowledgment Form

I hereby state that I have legitimate and official need to recover the Symantec ECA key belonging to the following Subscriber:

First Name _____
Last Name _____
E-mail Address _____

in order to obtain (recover) the encrypted data that I have authorization to access. I acknowledge receipt of a recovered ECA encryption key associated with the Subscriber identified here. I certify that I have accurately identified myself to the Symantec Key Recovery Agent, and truthfully described all reasons that I require access to data protected by the recovered key. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to the Symantec Key Recovery Agent when no longer needed. I understand that I am bound by the Subscriber's organization policies, applicable laws and Federal regulations concerning the protection of the recovered key and any data recovered using the key.

_____
Signature

First Name _____
Last Name _____
Organization _____
Postal Address _____
E-mail Address _____
Phone Number _____