# CertiPath Key Recovery Policy

**Version 1.5**

**December 16, 2013**

# Signature Page

Judith A Spencer

**DECEMBER 16, 2013**

CertiPath Policy Management Authority DATE

# Table of Contents

# 1 INTRODUCTION

One aspect of the CertiPath is the ability to escrow and recover private keys from key encipherment (or key exchange) public/private key pairs.  The Key Recovery System (KRS) provides the computer system hardware, software, staff and procedures to store the private keys securely and recover them when appropriate.  Section 1.3.2 describes the KRS and its components.

Since the KRS has a significant impact on the confidentiality services provided by a PKI, its design and operation must engender a high degree of trust.  One way to manage risk and provide trust is to develop and implement an operational policy.  This document describes the procedural and technical security controls that should be in place in order to operate the KRS securely.

In this Policy, the term "Entity" refers to the organization that operates a PKI and/or Key Escrow Database portion of the KRS.

In this Policy, the term "Enterprise" refers to the organization whose subscriber keys are escrowed and recovered.

"Entity" and "Enterprise" could be the same when an organization runs its own PKI and key escrow and recovery.  An "Entity" could be a pure service, offering the services to various "Enterprises".  An "Entity" could support its own needs as well as the needs of other "Enterprises".

## 1.1 Overview

The key recovery capability is based on the principle that all encryption activities using the certificates are performed on behalf of the person or the organization that authorized the issuance of encryption certificates.  Therefore, the person or the business has the right to identify the persons authorized to recover the decryption private key in order to maintain the continuity of business operations.  In addition, there may be a need to access the information for investigative and law enforcement purposes.  Some Organizations require that the contents of incoming and/or outgoing e-mail be examined for compliance with the Organization Policy.  This Key Recovery Policy (KRP) provides guidance to ensure that encrypted data is recovered expeditiously when appropriate.

The purpose of this document is to describe the security and authentication requirements to implement key recovery operations.  The KRP requires the use of two Key Recovery Agents (KRAs) to recover the keys from the Key Escrow Database (KED) when an authorized party requests recovery of a subscriber's private key.  Subscribers may authenticate themselves to the KED and perform self-recovery without requiring anyone else's approval.  Section 1.3.1.1 describes the KRA.  Section 1.3.2.1 describes the KED.

The Entity offering key recovery services shall develop a Key Recovery Practice Statement (KRPS) describing the procedures and controls implemented to comply with this KRP.  The

CertiPath Policy Management Authority (CPMA) will determine the KRPS compliance with this KRP.

## 1.2 Identification

There is no stipulation of an object identifier for this KRP.

## 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)

A KRA is an individual who, using a two party control procedure with a second KRA, is authorized, as specified in the applicable KRPS to interact with the KED in order to extract an escrowed key. The KRAs have high level sensitive access to the KED. Because KRAs can recover large numbers of keys, the CPMA places a high level of trust in them. Therefore, the number and location of KRAs should be closely controlled. The KRAs that do not belong to the Entity shall only be able to recover keys of subscribers from the KRAs' Organization/Enterprise.

#### 1.3.1.2 Key Recovery Official (KRO)

An Entity may choose to use the services of a Key Recovery Official (KRO) in performing identity verification and authorization validation tasks. KROs may authenticate the requestor. The KROs that do not belong to the Entity shall only be able to participate in the recovery of keys of subscribers from the KROs' Organization/Enterprise.

If an Entity chooses not to use the services of KROs, then all requirements outlined in this KRP for KROs apply to KRAs.

#### 1.3.1.3 Requestor

A requestor is the person who requests the recovery of a decryption private key. A requestor is generally the subscriber itself (for self-recovery) 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. Any individual who can demonstrate a reasonably verifiable authority and a need to obtain a recovered key can be considered a requestor.

> **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/Enterprise. The intent of this KRP is not to change the policy and procedures of the Organization/Enterprise. The subscribers’ Organization/Enterprise shall appoint authorized requestors and the PKI shall implement the KRP so that the existing Organization/Enterprise Policy regarding access and release of sensitive information can be met.

**External Requestor:** An External Requestor is an investigator or someone outside the subscribers' Organization/Enterprise with authorized court order to obtain the decryption private key of the subscriber. An external requestor must work with an internal requestor unless the law requires the Entity to release the subscriber's private key without approval of the subscriber and subscriber's Organization/Enterprise. Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests. The Entity and subscribers' Organizations/Enterprises shall appoint authorized personnel and implement the KRP so that the existing Organization/Enterprise policies regarding release of sensitive information can be met.

#### 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 that certificate.

### 1.3.2 Key Recovery System (KRS) Components

The KRS consists of all the information system (or systems), KRP, KRPS, and operations personnel used to provide key escrow and key recovery services.

The KRS information systems consist of the KED, KRA workstation(s), and optionally KRO workstation(s) and Key Server(s).

#### 1.3.2.1 Key Escrow Database (KED)

The KED is defined as the function, system, or subsystem that maintains the key escrow repository and responds to key registration requests. The KED also responds to key recovery requests from two or more KRAs or a current subscriber.

Section 5.2.1.3 contains the description of trusted roles required to operate the KED.

#### 1.3.2.2 KRA Workstation

KRAs perform key recovery by directly accessing the KED or from KRA workstations that securely communicate with the KED. The KRAs send the recovered keys to the requestors or to KRO.

#### 1.3.2.3 KRO Workstation

A KRO performs his/her function from a desktop computer that securely communicates with .the KRA. A KRO performs the following functions:

- Authentication of the requestor;
- Validation of the requestor's authorization;
- Sending key recovery requests to a KRA;
- Receiving encrypted recovered key from a KRA; and

- Providing encrypted recovered key to requestor

#### 1.3.2.4 Key Server

A Key Server is a automated system that has the capability to obtain subscriber private keys or session keys from the KED or another Key Server. A Key Server is a type of requester and must adhere to physical, personnel, procedural and technical security requirements of the KED.

### 1.3.3 Applicability

This KRP applies to the Entity KEDs, Key Servers, and subscribers whose decryption private keys are escrowed, and to the Organizations/Enterprises serviced by the Entities.

## 1.4 Contact Details

### 1.4.1 Key Recovery Policy Administration Organization

The CPMA is responsible for the definition, revision and promulgation of this KRP.

### 1.4.2 Contact Office

Questions regarding this KRP shall be directed to the Chair of the CPMA.

### 1.4.3 Person Performing Policy/Practice Compatibility Analysis

CPMA will determine if Entity KRPS conforms to this KRP. Entities will be required to obtain independent compliance auditor assessment of such compliance periodically as established by the CPMA. Further, the CPMA reserves the right to audit Entity compliance as set forth in this KRP and in the MOA between it and the Entity.

# 2 GENERAL PROVISIONS

## 2.1 Obligations

As part of the key escrow process, subscribers shall be notified that the private keys associated with their encryption certificates will be escrowed.

During delivery, escrowed keys shall be protected against disclosure to any party except the requestor.

The KRPS shall describe the method for ensuring that each individual understands and complies with the obligations for any Key Recovery role they execute.

### 2.1.1 Entity Obligations

An Entity who provides escrowed keys to requestors under the Policy defined in this document shall conform to the stipulations of this document. In particular, the following stipulations apply:

- The CPMA shall approve the Entity KRPS prior to key escrow.
- The Entity shall provide the KRPS to the KRAs.
- The Entity shall provide the KRPS to the KROs.
- The Entity shall operate the KED in accordance with the stipulations of the KRPS and this KRP.
- The Entity shall automatically notify the subscribers when their private keys have been escrowed with the KED (e.g., a dialog box may appear on a subscriber's screen during the certificate request process). Practice Note: This notification can be part of the subscriber agreement provided during the subscriber registration process.
- The Entity shall monitor KRA and KRO activity for patterns of potentially anomalous activity as indicators of possible problems in the infrastructure, and initiate inquiries or investigations as appropriate.

### 2.1.2 KRA Obligations

A KRA who submits requests as described in this KRP shall comply with the stipulations of this KRP and comply with the applicable KRPS. In particular, the following stipulations apply:

- KRAs shall keep a copy of this KRP and their KRPS.
- KRAs shall operate in accordance with the stipulations of this KRP and their KRPS.
- KRAs shall protect subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.

- KRAs shall protect all information, including the KRA's own key(s) that could be used to recover subscribers' escrowed keys.
- KRAs may rely upon the KROs for authentication and verification of the identity and authority of the requestor. However, KRAs shall also authenticate the identity of the requestor when the requestor digital signature is available; i.e., when the requestor makes an electronic request that is digitally signed. This will require the KRO to forward the requestor digital signature in a form verifiable by the KRA. For example, S/MIME signed e-mail from the requester must not be simply forwarded by the KRO to KRA, but must be sent as an attachment. In addition, KRAs may request additional information or verification from the KROs if deemed necessary.
- KRAs shall release subscribers' escrowed keys only for properly authenticated and authorized requests from requestors. The requestor authentication and authorization verification may be delegated to the KROs. KRAs shall authenticate the KROs using strong (e.g., cryptographically-based, using Medium Hardware Assurance certificate issued by the Entity PKI) authentication techniques.
- KRAs shall validate the authorization of the KRO by ensuring that the KRO is an authorized KRO for the subscriber whose key has been requested to be recovered.
- KRAs shall protect all information regarding all occurrences of key recovery. KRAs shall communicate knowledge of a recovery process only to the KRO and 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.
- KRAs shall monitor KRO activity for patterns of potentially anomalous activity as indicators of possible problems in the infrastructure, and initiate inquiries or investigations as appropriate.

### 2.1.3 KRO Obligations

A KRO initiates a key recovery request for a Requestor. The requestor is generally a third party, but this KRP does not preclude the subscriber from seeking the assistance of a KRO to recover the subscriber's private key.

- The KRO shall protect subscribers' recovered keys from compromise. The KROs receive the recovered keys in encrypted form not usable by the KRO (i.e., KRO shall not be able to decrypt or use the key). After providing the requestor with the encrypted key, the KRO shall destroy the copy of the key in his/her system.
- The KRO shall request the subscriber's keys only upon receipt of a request from an authorized requestor. The KRO, as an intermediary for the KRA, shall validate the identity of any requestor seeking a key recovery. The process for validating the identity shall be the same as the one used for user registration as defined in the Entity CPS. Alternatively, the KRO can authenticate the requestor provided the requestor certificate is issued by the Entity PKI, the certificate is current, is not revoked, and is for the same or greater assurance level than the certificate associated with the key being requested.

- When the requestor is authenticated on the basis of digital signature, the KRO shall forward the requestor digital signature in a form verifiable by the KRA. For example, S/MIME signed e-mail from the requester must not be simply forwarded by the KRO to KRA, but must be sent as an attachment.
- In the case of persons other than the subscriber seeking a key recovery, the KRO shall ensure that the requestor has the authority to request the subscriber's key.
- The KRO, as an intermediary for the KRA, shall validate the authorization for the request, to include consultation with legal counsel when appropriate.
- The KRO shall protect all information, including the KRO's own key(s) that could be used to obtain the subscriber's recovered key(s).
- The KRO shall protect all information regarding all occurrences of key recovery. The KRO shall communicate knowledge of any recovery process only to the requestor, except as permitted by Section 3.2.2. The KRO shall not communicate any information concerning a key recovery to the subscriber except when the subscriber is the requestor.
- The KRO shall accurately represent themselves to all entities when requesting key recovery services.
- The KRO shall keep records of all recovery requests and disposition, including acknowledgement of receipt by the requestor. The 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 obligations described here.

- 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 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. When the request is made to a KRO, the Requestor shall provide accurate identification and authentication information at least to the same level required for issuing new PKI certificates at the level of the key being requested. If the Requestor can send a digitally signed request using the credential issued by the Entity PKI and of the same or higher assurance level as the key being recovered, that will suffice.

- The 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. Whether to notify the subscriber or not, shall be based on the law, and subscriber Organization's/Enterprise'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 receiving a recovered key, a requestor shall sign an acknowledgement of agreement to follow the law and the subscriber's Organization/Enterprise policies relating to protection and release of the recovered key.
- Upon receipt of the recovered key(s), the requestor (if not the subscriber) shall sign[1] a form prepared by the requestor, which includes 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 encryption key associated with the subscriber identified here. I certify that I have accurately identified myself to the KRO, 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 KRO when no longer needed. I understand that I am bound by subscriber's Organization/Enterprise policies, applicable laws and Federal regulations concerning the protection of the recovered key and any data recovered using the key."

### 2.1.5 Key Server Obligations

Prior to the beginning of the operation of a Key Server, the Enterprise shall formally acknowledge and agree to the obligations described here by signing an appropriate form

- The Key Server shall protect subscribers' recovered key(s) from compromise. Key Server 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. The Key Server shall destroy subscribers' keys when no longer required (i.e., when the data has been recovered).
- The Key Server shall request the subscriber's escrowed key(s) only upon receiving request to decrypt subscriber data from an authenticated authorized Enterprise system (e.g., an e-mail Server)

[1] Acceptable examples include a signed paper or a document digitally signed using the credential issued by the Entity PKI.

- The Key Server shall use the subscriber's recovered keys only to recover subscriber's data requested from an authenticated authorized Enterprise system (e.g., an e-mail Server)
- The Key Server shall provide accurate identification and authentication information at least at the same assurance level required for issuing new PKI certificates for the assurance level of the key being requested.

### 2.1.6 Subscriber Obligations

Subscribers shall comply with the following stipulations.

- 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 pubic 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

The Entity shall warrant that their procedures are implemented in accordance with this KRP and their KRPS, and that all key escrow and recovery are done in accordance with this KRP and the Entity KRPS.

The Entity and Enterprises shall warrant that their respective Key Servers, KRAs and KROs will operate in accordance with the applicable sections of this KRP and the Entity KRPS.

### 2.2.2 Damages Covered and Disclaimers

Other than the warranties included in Section 2.2.1, Entity may disclaim any warranties or obligations of any type concerning the accuracy of information provided by a Subscriber or Requestor, provided the procedures stated in the Entity KRPS were followed and the procedures were in compliance with the CertiPath CP, Entity CP, and this KRP. Furthermore, Entity may disclaim any and all liability solely arising due to negligence and/or lack of reasonable care on the parts of Subscribers and Requestors.

### 2.2.3 Loss Limitations

The Entity shall identify in its CPS limits of losses due to operations in variance with its procedures defined in its CPS. The Entity may disclaim any liability for loss due to improper use of a recovered key, if the key was recovered in accordance with this KRP and the Entity KRPS.

### 2.2.4 Other Exclusions

An Entity may state, in its KRPS, other exclusions that do not conflict with this KRP.

## 2.3 Financial Responsibility

### 2.3.1 Indemnification by Relying Parties and Subscribers

Neither the Entity nor its agents (e.g., KRA, KRO, etc.) assume financial responsibility for improper use of a recovered key by subscriber or by requestor.

### 2.3.2 Fiduciary Relationships

Escrow and recovery of private keys in accordance with this KRP and the Entity KRPS does not make an Entity, or any KRA or KRO, an agent, fiduciary, trustee, or other representative of Subscribers or Requestors.

## 2.4 Interpretation and Enforcement

### 2.4.1 Governing Law

This KRP shall be governed by the laws of the State of New York in the United States of America.

### 2.4.2 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this KRP is incorrect or invalid, the other sections shall remain in effect until the KRP is updated. Requirements for updating this KRP are described in Section 7. Responsibilities, requirements, and privileges of this document are merged to the newer edition upon release of that newer edition.

### 2.4.3 Conflict Provision

In the event of any conflict between this KRP and the Entity KRPS, this KRP shall take precedence over the Entity KRPS.

### 2.4.4 Dispute Resolution Procedures

The CPMA shall be the sole arbiter of disputes over the interpretation or applicability of this KRP.

## 2.5 Fees

Fees for performing key recovery services may be published or established contractually by the Entities.

## 2.6 Publication and Repository

Not Applicable.

## 2.7 Compliance audit

### 2.7.1 Frequency of Entity Compliance Audit

Audits of KRS components shall be conducted with the following minimum audit frequencies:

- KED - Annual;
- Key Server – Annual;
- KRA – Annual; and
- KRO – Annual.

An audit of the KRS may be conducted in conjunction with the audit of the other elements of the PKI.  The KED and the Key Server may be audited in conjunction with the Certification Authority (CA) audit.  The KRA and KRO may be audited in conjunction with the Registration Authority (RA) audit.

In the event that a KRO or KRA is relieved of that responsibility due to a failure to comply with this KRP, the Entity PMA[2] shall direct a special compliance audit.  The purpose of that audit will be to determine whether any key recovery activities of the removed KRO or KRA 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 the Entity KRPS. 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.

### 2.7.3 Compliance Auditor's Relationship to Audited Party

The compliance auditor and the Entity operating the KRS shall have a contractual relationship for the performance of the compliance audit, or be sufficiently organizationally separated from the audited KRS component to provide an unbiased, independent evaluation.

[2] See CertiPath X.509 Certificate Policy (CP) for the definition of PMA

### 2.7.4 Topics Covered by Compliance Audit

All the topics identified in this KRP document will be covered by the compliance audit. The purpose of a compliance audit shall be to verify that the KED, KRA Workstation, and KRO Workstation have requisite procedures and control in place.

### 2.7.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between a KED, Key Server, KRA or KRO operation and the stipulations of the applicable KRPS, the following actions must occur:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the parties identified in Section 2.7.6 of the discrepancy; and
- The audited component shall propose a remedy, including expected time for completion, to the Entity PMA.

The Entity PMA shall determine the appropriate remedy, up to and including revocation or non-recognition of the audited component's certificate. Upon correction of the deficiency, the Entity PMA may reinstate the audited component.

### 2.7.6 Communication of Results

For a KED and Key Server compliance audit, the compliance auditor shall submit a report of the compliance audit to the Entity PMA, and to the Entity. CPMA shall be provided the compliance auditor opinion letter and the management assertion.

For a KRA compliance audit, the compliance auditor shall submit a report to the Entity.

Results of KRO compliance audits shall be submitted to the Entity and to the designated representative of the subscribers' Organization/Enterprise.

## 2.8 Confidentiality

### 2.8.1 Type of Information to be Protected

The KED, KRA, KRO and requestor must protect personal or sensitive information used to identify and authenticate participants in the recovery process. Such information includes Social Security Number (SSN), identification credential serial numbers, affiliation with investigative agencies when specified by the requestor as sensitive. Protections are described in Sections 4, 5, and 6 of this KRP.

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

### 2.8.2 Information Release Circumstances

A KRA shall not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless authorized by this KRP; required by the law, government rule, or regulation; by the subscriber's Organization/Enterprise policy; or by order of a court of competent jurisdiction.  The identity of the requestor of escrowed keys shall be authenticated per Section 3.

# 3 IDENTIFICATION AND AUTHENTICATION

The purpose of Identification and Authentication is to verify that requestors are who they say they are and are authorized to access requested escrowed key.

The user’s authenticated identity shall be used as the basis for determining the user’s access permissions and providing user accountability.

## 3.1 Identity Authentication

Identity authentication shall be commensurate with the assurance level of the certificate associated with the key being recovered. It shall comprise the activities specified by the Entity CPS for authentication of individual identity during initial registration for at least the specified certificate policy assurance level or be based on digital signatures that can be verified using current, valid (i.e., un-revoked) public key certificates issued by the Entity PKI and for at least the specified certificate policy assurance level.

## 3.2 Requestor

This section addresses the requirements for authentication and authorization of a third party requestor, i.e., a requestor other than the subscriber itself. The requirements for authentication and authorization, when the requestor is the subscriber, are addressed in Section 3.3.

### 3.2.1 Requestor Authentication

The requestor shall establish his or her identity to the KRA or the KRO, as an intermediary for the KRA, as specified in Section 3.1. The KRA or KRO shall personally verify the identity of the requestor prior to initiating the key recovery request. The authentication mechanism shall be detailed in the KRPS.

### 3.2.2 Requestor Authorization Verification

The KRA or the KRO, as an intermediary for the KRA, shall validate the authorization of the requestor in consultation with Organization/Enterprise management and/or legal counsel, as appropriate. The mechanism to validate the authorization shall be detailed in the KRPS.

## 3.3 Subscriber

### 3.3.1 Subscriber Authentication

The subscriber shall establish his or her identity to the KED, KRA or the KRO, as an intermediary for the KRA, as specified in Section 3.1. If the authentication is not based on digital signatures that can be verified using the public key certificates issued by the Entity PKI and for at least the given certificate policy assurance level, the KRA or KRO shall personally verify the identity of the subscriber prior to initiating the key recovery request.

The authentication mechanism shall be detailed in the KRPS and shall be in compliance with that for initial registration described in the Entity CPS.

For automated self-recovery, the subscriber must be authenticated to the KED using a valid Entity PKI issued public key certificate.  The authentication mechanism and the mechanism for linking the identity obtained from the authentication mechanism with the identity of the subscriber for the escrowed key to be recovered shall be detailed in the KRPS.  The certificate policy assurance level of the authentication certificate shall be equal to or greater than that of the certificate whose companion private key is being recovered.

### 3.3.2 Subscriber Authorization Verification

Current subscribers are authorized to recover their own escrowed key material.

## 3.4 KRA and KRO Authentication

### 3.4.1 KRA

The KRA shall authenticate to the KED directly or using a public key certificate issued by the Entity PKI.  The assurance level of the certificate shall be the same as or greater than that of the certificate whose companion private key is being recovered.

### 3.4.2 KRO

The KRO shall authenticate to the KRA using a public key certificate issued by the Entity PKI.  The assurance level of the certificate shall be the same as or greater than that of the certificate whose companion private key is being recovered.

## 3.5 Key Server

### 3.5.1 Key Server Authentication

The Key Server shall authenticate to the KED directly or using a public key certificate issued by the Entity PKI.  The assurance level of the certificate shall be the same as or greater than that of the highest level encryption certificates issued to the Enterprise.

### 3.5.2 Key Server Authorization Verification

The KED shall verify that the Key Server is authorized to obtain the keys for the claimed Enterprise.

# 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/Enterprise policy, as verified by the Organization’s/Enterprise's KRO, and by authorized law enforcement personnel with court order from a competent court.

### 4.1.2 Requirements for Requesting Escrowed Key Recovery

Subscribers may use electronic or manual means to request their own escrowed keys from the KRS. The subscriber may submit the request to the KED, KRA or KRO. If the request is made electronically, the subscriber shall digitally sign the request using the Entity PKI issued authentication certificate of assurance level equal to or greater than that of the escrowed key. Manual requests shall be on paper and shall be signed by hand.

Third party requestors may use electronic or manual means to request the subscribers’ escrowed keys. The requestor shall submit the request to the KRA or KRO. If the request is made electronically, the requestor shall digitally sign the request using the Entity PKI issued authentication certificate of assurance level equal to or greater than that of the escrowed key. Manual requests shall be on paper and shall be signed by hand.

Key Servers shall use electronic means to request subscribers’ escrowed keys. Requests shall be authenticated using means at least as strong as the key being recovered.

Practice Note: Examples of acceptable methods include direct physical connection; use of a certificate at the same as or greater assurance level than that of the highest assurance level encryption certificates issued to the Enterprise operating the Key Server; and Virtual Private Network (VPN) using FIPS validated cryptography with the same or greater security strength than that of the highest assurance level encryption certificates issued to the Enterprise operating the Key Server. These examples are not exhaustive.

## 4.2 Protection of Escrowed Keys

Escrowed keys shall be stored in a protected KED.

Key recovery (in particular automated key recovery) must be carried out with extreme caution, as the chance for compromise can be very high. Further, the risk of compromise and the scope of any potential compromise is implementation dependent.

### 4.2.1 Key Recovery through KRA

The KRA 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 KRAs. All copies of escrowed keys shall be protected continuously using two person control procedures during recovery and delivery to the authenticated and authorized third party requestor. The protection mechanisms shall be specified in the KRPS. Split key or password procedures are considered adequate two person controls.

The strength of the confidentiality provided by the delivery mechanism for copies of escrowed keys shall be equal to or greater than that provided by the key being protected.

### 4.2.2 Automated Self-Recovery

A current subscriber's escrowed keys may be provided directly to that subscriber without imposition of two person control requirements. The KED shall only provide escrowed keys to current subscribers without two person control upon:

- Verifying that the authenticated identity of the requestor is the same as the subscriber associated with the escrowed keys being requested. The KRPS shall describe how the identity of the authenticated subscriber is verified and ensured to be same as that associated with the subscriber's private key;
- Attempt to notify the subscriber of all attempts (successful or unsuccessful) to recover the subscriber's escrowed keys that are made by entities claiming to be the subscriber. If the KED does not have information (e.g., an e-mail address) necessary to attempt to notify the subscriber of a key recovery request, then the KED shall not provide the subscriber with the requested key material using the automated recovery process;
- Ensuring that the escrowed keys are being sent only to the authenticated subscriber associated with the escrowed keys; and
- Ensuring that the escrowed keys are encrypted during transmission using cryptography of equal or greater strength than provided by the escrowed keys.

If the KED recovers and transmits the escrowed keys to the subscriber, the KED shall notify the CA that issued a certificate associated with the recovered key, of automated self-recovery in order for the CA to determine if the subscriber's public key certificate associated with the recovered key should be revoked. The criteria and the process for revocation shall be documented in the CA CPS.

### 4.2.3 Recovery By Key Server

An escrowed key may be provided directly to Key Server as long as the Key Server is operated under continuous two person control. The KED shall perform the activities prior to releasing the key:

- Authenticating the requestor as a legitimate Key Server;

- Verifying that the Key Server is authorized to recover the escrowed key for the Enterprise whom the key belongs to;
- Ensuring that the escrowed keys are protected during transmission using cryptography or other means of equal or greater strength than provided by the escrowed keys.

A combination of physical, procedural and technical security controls shall be used to enforce continuous two person control on the Key Servers. The Key Servers shall be designed to maximize the ability to enforce two-person control technically.

Practice Note: The Key Server is considered under continuous two person control when any human action performed on the Key Server require two persons.

Practice Note: Using existing technology, continuous two person control on the Key Server is not likely to be met by using remote administration.

## 4.3 Certificate Issuance

Not applicable. Certificate issuance is addressed in the Entity CP.

## 4.4 Certificate Acceptance

Not applicable. Certificate acceptance is addressed in the Entity CP.

## 4.5 Security Audit Procedures

Security auditing capabilities of the underlying KED and KRA workstation equipment operating system shall be enabled upon installation and remain enabled during operation.

### 4.5.1 Types of events recorded

The KED equipment shall be configured to record, at a minimum, the following event types. These events may be recorded as part of the electronic audit log or KED operations staff:

- KED application access (e.g., logon/logoff);
- Messages received from any source requesting KED actions, (i.e., escrowed key retrieval requests);
- Actions taken in response to requests for KED actions;
- Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying KED cryptographic modules;
- Receipt of keys for escrow and posting of these keys to the KED;
- Retrieval, packaging (e.g., keying or other cryptologic manipulations), securing, and shipping copies of escrowed keys;

- Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and
- Any known or suspected violations of physical security, suspected or known attempts to attack the KED equipment via network attacks, equipment failures, power outages, network failures, or violations of this KRP.

KRA workstation shall be configured and operated to record the following event types. These events may be recorded as part of the electronic audit log or by the KRA:

- KRA server installation;
- Modification to KRA (including changes in configuration files, security profiles, administrator privileges);
- KRA equipment access (e.g., room access);
- Messages received from any source requesting KRA actions, (e.g., key recovery requests, second party key recovery approval requests);
- Messages sent to any destination authorizing key recovery actions, (e.g., first party escrowed key retrieval authorizations, second party key recovery approvals);
- Access to KRA databases related to escrowed or recovered keys; and
- Any use of the KRA signing key.

The KRO shall record the following information for audit:

- Transfer of escrowed keys to requestors, if transmitted through the KRO;
- Any security-relevant actions performed in support of delivery of escrowed keys; and
- Requestor identity and authorization verification (including copies of authorizations; e.g., court orders) supporting key recovery requests acted upon by the KRO.

The Key Server shall be configured to record, at a minimum, the following event types. These events may be recorded as part of the electronic audit log or manually by Key Server operations staff:

- Key Server system access (e.g., logon/logoff);
- Requests from any source (e.g., key recovery request, decryption services, etc.);
- Actions taken in response to requests;
- Receipt of recovered keys from the KED or another Key Server;
- Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying Key Server cryptographic modules;
- Retrieval, packaging (e.g., keying or other cryptologic manipulations), securing, and shipping copies of escrowed keys;
- Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and

- Any known or suspected violations of physical security, suspected or known attempts to attack the Key Server equipment via network attacks, equipment failures, power outages, network failures, or violations of this KRP.

For each auditable event defined in this section, the audit record shall include, at a minimum:

- The type of event;
- The time the event occurred;
- For requests from Key Servers, KRAs, KROs, or other entities to the KED, the request source, destination, and contents;
- For requested KED actions – a success or failure indication; and
- For operator initiated actions (including equipment and application access), the identity of the equipment operator who initiated the action.

Where possible, the security audit data shall be automatically collected; when this is not possible a log book, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and paper (manual), shall be retained in accordance with the requirements of Section 4.5.3, and made available during compliance audits.

### 4.5.2 Audit Log Processing

Automated audit logs shall be processed as required to prevent audit overflow, audit overwrite or stoppage of system operation.

### 4.5.3 Audit Log Retention Period

Audit logs shall be kept until they are moved to an appropriate archive facility. Security audit data shall be retained as archive records in accordance with Section 4.6.2.

### 4.5.4 Audit Log Protection

Audit logs shall be protected from unauthorized modification or unauthorized deletion. No one is authorized to modify the content of audit logs, except for appending new audit records without overwriting existing audit records.

Electronic audit logs shall be deleted only after they have been backed up to archive media. Only authorized audit administrators shall delete these logs. Before deleting any electronic audit log, the audit administrator shall verify that the audit log data has been successfully backed up to archive media.

No one shall delete or destroy audit data recorded on archive media.

### 4.5.5 Audit log back up procedures

Audit log processing personnel (i.e., the audit administrators) shall use the procedures described in the KRPS to perform regular back up of the audit log.

### 4.5.6 Audit Log Collection System (Internal vs. External)

The audit log process shall be internal to the KED, Key Server, KRA and KRO. Audit processes shall be invoked at component system startup and cease only at component system shutdown. Audit process shall run automatically without human intervention.

Should it become apparent that an automated audit process has failed, the affected KRS component (e.g., KED, Key Server, KRA or KRO) shall cease all operations until an audit capability can be restored.

### 4.5.7 Subscriber Audit Notification

There is no requirement to notify a subscriber of an audit event.

### 4.5.8 Vulnerability assessments

The KRA, system administrator, and other supporting personnel shall watch for attempts to violate the integrity of the KRS, including the equipment, physical location, and personnel. The audit logs shall be reviewed by the audit administrator regularly (at least once a month) for events such as repeated failed actions, requests for escrowed keys, attempted access of escrowed keys, unauthenticated requests, or other suspicious or unusual activity. The audit administrator shall also check for continuity of the audit log.

A statistically significant sample of KED audit records of successful key recoveries shall be reconciled against the KRA and KRO audit logs and requests. The objective of this reconciliation shall be to ensure that all key recoveries are being made by authorized parties and for legitimate reasons.

All KED audit records of unsuccessful key recoveries shall be analyzed to determine the cause and to ensure that the Key Escrow and Recovery system is operating correctly and securely and is not vulnerable to hacking and unauthorized users.

## 4.6 Records Archival

The KRS components shall maintain a trusted archive of information they store and of transactions they carry out. The primary objective of the archive is to be able to reconstruct the key recovery activities, in case of dispute. Examples of disputes may include:

- Key recovery request forms
- Validation of the identity of the recipient of a copy of the subscriber’s escrowed key;
- Verification of authorization and need of requestor to obtain the escrowed key copy; and

- Establishment of the circumstances under which a copy of the escrowed key was provided.

### 4.6.1 Types of information recorded

The following information shall be archived:

- KRP and KRPS;
- Agreements, if any (with KRAs, KROs, subscribers, and/or subscribers' Organizations/Enterprises)
- Audit log;
- Security audit data; and
- Escrowed keys.

The KRP shall be archived by the CPMA. All other information shall be archived by the Entity and Enterprises the Entity provides services to.

The necessary software and hardware (if appropriate) shall be retained, either as operational components or, after decommissioning, as archive retrieval components, to support interpretation of the information during the entire archive retention period.

### 4.6.2 Archive Retention Period

The archive retention period shall meet the requirements specified in CertiPath CP Section 5.5.2 for the certificate policy assurance level supported.

Escrowed keys shall be maintained within the online KED for a minimum of one year after the expiration of the associated public key certificate.

### 4.6.3 Archive Protection

No one shall be able to modify or delete archived data. The KRPS shall specify the roles authorized to back up archive data.

No one shall be able to delete or destroy data recorded on archive media. Transfer of media shall not invalidate digital signatures applied to the recorded data. Release of sensitive archive information will be as described in Section 2.8.

Archived escrowed keys shall be protected as specified in Section 4.2.

Archive media shall be stored in a separate, safe, secure storage facility, as described by the applicable KRPS. Archive media shall be labeled with the KRS component name and date of archival. If the KRS component has a distinguished name (e.g., CA associated with KED or subject field in the KRA certificate), the distinguished name shall be used for the component name. Otherwise, a meaningful and human readable name that unambiguously identifies the KRS component shall be used.

### 4.6.4 Archive backup procedures

No stipulation.

### 4.6.5 Requirements for time-stamping of records

The archived record shall contain information necessary to determine when the event occurred. The time precision shall be such that the sequence of events can be determined.

### 4.6.6 Archive Collection System (Internal vs. External)

The archival collection system shall be documented in the KRPS.

### 4.6.7 Procedures to obtain and verify archive information

The KRPS shall describe the procedures used to verify the accuracy of the archived information.

## 4.7 KRA Key Changeover

The KRA shall re-key every three (3) years.

## 4.8 KED Compromise and Disaster Recovery

Requirements for compromise or disaster notification and recovery procedures are necessary to ensure the KED remains in a secure state.

Practice Note: The KRPS should be based on an analysis of the implementation to ensure that if an infrastructure key (KED; Key Server; KRA; KRO) is compromised, other keys exposed due to this compromise/exposure are revoked.

### 4.8.1 KED Compromise

In the event that the KED is compromised or is suspected to be compromised, the Entity PMA shall be notified. The Entity PMA shall be granted sufficient access to information to determine the extent of the compromise. The Entity PMA shall direct the appropriate action. This may include revocation of certificates associated with the compromised private keys stored in the KED.

### 4.8.2 Disaster Recovery

The KED shall reestablish a secure environment. The procedures for reestablishing the secure environment after any disaster shall be detailed in the KRPS or the Disaster Recovery Plan. The disaster recovery plan shall also address the testing Entity's preparedness for Disaster Recovery.

### 4.8.3 KRA or KRO Key Compromise

If the KRA or KRO certificate is revoked due to compromise, there is a potential for some subscribers' escrowed keys to have been exposed during the recovery process. The audit administrator shall review the audit records to identify all potentially exposed escrowed keys. Each of the potentially exposed escrowed keys shall be revoked, according to procedures specified in CertiPath CP Section 4.9.3, and the subscriber shall be notified of the revocation. It is recognized that this circumstance will constitute implicit notification to the subscriber of key recovery.

### 4.8.4 KRA or KRO Certificate Revocation

If the KRA or KRO certificate is revoked for any reason, but the KRA or KRO remains authorized to perform his or her duties, then the KRA or KRO shall request a new KRA or KRO certificate from the Entity PKI. The CA that revoked the KRA or KRO certificate, shall ensure that all the requirements of the applicable CPS for revocation notification are met. The Entity PKI shall follow its CPS for certificate issuance for the new KRA or KRO public key certificate.

### 4.8.5 Key Server Compromise

In the event that a Key Server is compromised or is suspected to be compromised, the Entity PMA shall be notified. The Entity PMA shall be granted sufficient access to information to determine the extent of the compromise. The Entity PMA shall direct the appropriate action. This may include revocation of certificates associated with the compromised private keys stored in the KED.

## 4.9 KRA Termination

Upon KRA termination, the Entity or the KRA Organization/Enterprise shall take possession of all KRA archive records. The KRPS shall document the process for transferring KRA archive records.

## 4.10 KRO Termination

Upon KRO termination, the Entity or the KRO Organization/Enterprise shall take possession of all KRO archive records. The KRPS shall document the process for transferring KRO archive records.

## 4.11 Key Server Termination

Upon Key Server termination, the Entity or the Key Server Organization/Enterprise shall take possession of all Key Server archive records. The KRPS shall document the process for transferring Key Server archive records.

# 5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

## 5.1 Physical Controls

The KED shall consist of equipment dedicated to the key recovery function and, optionally, CA functions.

The Key Server shall consist of equipment dedicated to the key recovery function.

Physical controls for the KED and Key Server shall be equivalent to those specified in the CertiPath CP Section 5.1 for CA equipment. Physical controls for KRA and KRO workstations shall be equivalent to those specified in the CertiPath CP Section 5.1 for Registration Authority (RA) equipment.

KED, Key Server, KRA, and KRO workstation physical controls shall be described in the KRPS.

## 5.2 Procedural Controls

### 5.2.1 Trusted roles

The primary trusted roles defined by this KRP are the KRA and the KRO.

#### 5.2.1.1 Key Recovery Agent (KRA)

All KRAs that operate under this KRP are subject to the stipulations of this KRP and of the Entity KRPS. The KRA's role and the corresponding procedures shall be defined in the KRPS. A KRA’s responsibilities are to ensure that the following functions occur according to the stipulations of this KRP:

- KRO functions as described in Section 5.2.1.2, if no separate KRO is employed;
- Enable (i.e., initiate or approve) the recovery of copies of escrowed keys; and
- Distribute copies of escrowed keys to requestors, with protection as described in Section 4.2.

#### 5.2.1.2 Key Recovery Official (KRO)

All KROs that operate under this KRP are subject to the stipulations of this KRP and of the Entity KRPS. The KRO’s role and corresponding procedures shall be defined in the KRPS. A KRO’s responsibilities are to ensure that the following functions occur according to the stipulations of this KRP:

- Verify a requestor’s  identity and authorization as stated by this KRP;
- Build key recovery requests on behalf of authorized requestors;

- Securely communicate key recovery requests to and responses from the KRA; and
- Participate in distribution of escrowed keys to the requestor, as described by the KRPS.

The responsibilities and controls for KROs shall be explicitly described in the KRPS.

#### 5.2.1.3 Other Trusted Roles

The KRPS shall define trusted roles (e.g., system administrators, crypto officers, operators, audit administrators, etc.) for the secure operation of the KED and Key Server. The responsible persons who are identified in these trusted roles shall be named and made available during compliance audits. The following responsibilities shall be divided among these roles:

- Initial configuration of the system, including installation of applications, initial setup of new accounts, configuration of initial host and network interface;
- Receipt, initialization, key generation, usage and management of the cryptographic tokens and modules;
- Creation of devices to support recovery from catastrophic system loss;
- Performance of system backups, software upgrades and system recovery;
- Perform secure storage and distribution of the backups and upgrades to an off-site location;
- Change of the host or network interface configuration;
- Assignment of security privileges and access controls to key escrow system personnel;
- Backup and archival of the security audit log and other data as described in Sections 4.5 and 4.6 of this document;
- Review of the audit log; and
- Performance of compliance audit.

### 5.2.2 Separation of Roles

Under no circumstances shall a KRA or KRO perform a trusted role for a KED facility as defined in Section 5.2.1.3. Under no circumstances shall a KRA or KRO perform their own compliance audit function.

Separation of responsibilities among trusted roles for the KED shall be described in the KRPS.

Practice Note: It is acceptable for a person to hold similar trusted roles on the KRS and PKI. For example Registration Authority (RA) and Local Registration Authority (LRA) can act as KRA or KRO; an individual can be system administrator for the CA, KED, and Key Server; an individual can be audit administrator for the CA, KED, and Key Server; etc.

## 5.3 Personnel Controls

### 5.3.1 Background, qualifications, experience, and clearance requirements

Persons selected for KRA, KRO, and other trusted roles as specified in Section 5.2.1.3 shall meet the requirements specified in the CertiPath CP Section 5.3.1.

### 5.3.2 Background check procedures

Background check procedures shall be as specified in the CertiPath CP Section 5.3.2.

### 5.3.3 Training requirements

#### 5.3.3.1 KED Personnel Training

All personnel involved in KED operation shall be appropriately trained. Topics shall include:

- Operation of the KED software and hardware;
- Operational and security procedures;
- Stipulations of this KRP; and
- Entity KRPS.

The specific training required will depend on the equipment used and the personnel selected. A training plan shall be established for KED installation. Training completed by the personnel shall be documented.

#### 5.3.3.2 Key Server Personnel Training

All personnel involved in Key Server operation shall be appropriately trained. Topics shall include:

- Operation of the Key Server software and hardware;
- Operational and security procedures;
- Stipulations of this KRP; and
- Entity KRPS.

The specific training required will depend on the equipment used and the personnel selected. A training plan shall be established for Key Server installation. Training completed by the personnel shall be documented.

#### 5.3.3.3 KRA and KRO Training

Appropriate KRAs and KROs shall be trained in the subscribers’ Organization/Enterprise policy relating to release of key escrow information.

### 5.3.4 Retraining frequency and requirements

Significant changes to KED or Key Server operation shall require implementation of a training (awareness) plan that includes any retraining required for KED or Key Server operation staff, KRA or KRO personnel. The execution of such plan shall be documented.

### 5.3.5 Job rotation frequency and sequence

Job rotation frequency and sequence shall be as specified in the CertiPath CP Section 5.3.5.

### 5.3.6 Sanctions for unauthorized actions

Entities shall commence appropriate administrative and disciplinary actions against personnel who violate this KRP.

Subscribers’ Organizations/Enterprises shall commence appropriate administrative and disciplinary actions against personnel who violate the Organization’s/Enterprise's policy relating to key recovery requests.

### 5.3.7 Contracting personnel requirements

Entities shall establish procedures to ensure that any subcontractors perform in accordance with the Entity KRPS and this KRP. Subcontracts shall permit pursuance of appropriate administrative and disciplinary actions against subcontractor personnel who violate this KRP or Entity KRPS.

### 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. This at a minimum shall include, administrative and operations manuals for the host operating system, key escrow and recovery applications, and cryptographic modules; this KRP; and Entity KRPS.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 Protocol Security

When recovered by the KRAs, all copies of escrowed keys shall be protected continuously by two person controls during recovery and delivery to the authenticated and authorized requestor. Furthermore, the delivery mechanism for copies of escrowed keys shall provide cryptographic protection against disclosure with assurance equal to or greater assurance level of the certificates associated with the escrowed keys.

When a subscriber uses automated self-recovery, the subscriber's own escrowed keys may be provided directly to subscriber through authenticated and encrypted channels without imposition of two-person control requirements. The authentication and encryption shall be done using cryptographic means that are of equal or greater strength than that provided by the keys being recovered. All public key certificates involved in authentication and/or encryption shall be issued by the Entity PKI and shall have the assurance level of equal or greater than that of the certificates associated with escrowed keys.

Key Servers, when deployed, shall be protected continuously by two person controls. The recovered keys shall be protected during transmission to the Key Server using cryptography or other means of equal or greater strength than provided by the escrowed keys.

### 6.1.1 KED Protocol Security

Communications between the KED and KRAs, KED and Key Server, or between the KED and subscribers shall be secure from protocol threats such as disclosure, modification, replay, and substitution on transactions between the KED and communicating entities. The strength of all cryptographic protocols shall be equal to or greater than that of the keys they protect.

### 6.1.2 KRA - KRO Protocol Security

Communications between the KRA and KRO shall be secure from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols shall be equal to or greater than the keys they protect.

### 6.1.3 Escrowed Key Distribution Security

Communication of distributed copies of escrowed keys between the KED and requestor shall be secure from protocol threats such as disclosure, modification, replay, and substitution. The strength of all cryptographic protocols shall be equal to or greater than that of the keys they protect.

When any mechanism that includes a shared secret (e.g., a password) is used to protect the key in transit, the mechanism shall ensure that the requestor and the transmitting party are the only holders of this shared secret.

## 6.2 KED, Key Server, KRA and KRO 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]. Cryptographic modules shall be validated to the FIPS 140 level identified in this section.

The KED and Key Servers shall use hardware cryptographic modules that meet at least the criteria specified for FIPS 140 Level 3.

The KRA and KRO shall use hardware cryptographic modules that meet at least the criteria specified for FIPS 140 Level 2.

### 6.2.2 Private Key Control

The private components of KRA and KRO signature key pairs and encryption key pairs shall be under single person control. The KED and Key Server keys shall be under two or more person control. The names of the individuals used for two person control shall be maintained on a list that shall be made available for compliance audits.

When not in use, the KED and Key Server cryptographic module shall be stored in a secured container, such as a safe, in a facility that meets the physical security requirements of Section 5.1 of this KRP.

### 6.2.3 KED Key Backup

The KED key shall be backed up as necessary to provide secure continuity of key recovery operations. The backup keys shall only be created, stored, and restored under two person control. The process of restoring the backup KED key shall maintain two party control throughout, as required in Section 6.2.2.

### 6.2.4 Private Key Generation and Transport

Private components of KED, Key Server, KRA, and KRO encryption key pairs shall be generated by and in a cryptographic module. In the event that the private component of a KED, Key Server, KRA, or KRO encryption key pair is to be transported from one cryptographic module to another, it shall be encrypted during transport using the FIPS 140 approved method for the cryptographic module. Assurance level of any certificate used shall be commensurate with the highest assurance level of keys escrowed, but shall be at least Medium Hardware assurance level. The strength of cryptographic algorithm shall meet or exceed the strength of the key being transported.

### 6.2.5 Method of Activating Private Key

Activation of private keys shall be in accordance with the CertiPath CP, Section 6.2.8.

### 6.2.6 Method of Deactivating Private Key

The private component of the KED, Key Server, KRA, or KRO encryption key pair shall be deactivated as specified in Section 6.2.9 of the CertiPath CP.

### 6.2.7 Method of Deactivating Key Recovery

Activated cryptographic modules used for key escrow and recovery operations shall not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated (e.g. via a manual logout procedure or by a passive timeout).

Hardware cryptographic modules shall be removed from operational systems and stored when not in use. If a cryptographic module contains a complete (versus split) key for recovering subscriber keys, all storage procedures and mechanisms for that module shall require two-person control.

## 6.3 Private Key Activation Data

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

## 6.4 Computer Security Controls

### 6.4.1 KED

The KED shall be hosted on a trusted operating system that is designed, implemented, and operated using the following security features:

- Individual identification and authentication;
- Secure audit;
- Residual information protection;
- Discretionary access controls;
- Operating system self-protection;
- Process isolation; and
- Meet Common Criteria (CC) Evaluation Assurance Level (EAL) 3 assurance requirements. The Entity PMA may determine that other comparable validation, certification, or verification standards are sufficient.

The KED shall be configured to run with the minimal number of accounts and network services required to operate them. Only the required network services and ports shall be enabled, all other network services and ports shall be disabled. The KED shall be dedicated to running key recovery related or other PKI-related applications. The KED shall disable remote login and remote administration features.

### 6.4.2 KRA and KRO Workstation

KRA and KRO computers shall use operating systems that:

- Require authenticated logins;
- Provide discretionary access control;
- Provide operating system self-protection;
- Provide process isolation; and
- Provide a security audit capability.

When KRA or KRO workstation equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as received the evaluation rating.

Reasonable care shall be taken to prevent malicious software from being loaded on KRA and KRO workstation equipment. Only applications required to perform Entity PKI functions shall be loaded on the KRA workstation. Only applications required to perform the Organization's/Enterprise's mission shall be loaded on the KRO workstation, and all such software shall be obtained from sources authorized by Organization/Enterprise policy. Data on KRA and KRO workstation equipment shall be scanned for malicious code on first use and periodically afterward.

### 6.4.3 Key Server

Key Servers shall meet the requirements for KED stated in Section 6.4.1.

### 6.4.4 Anomaly Detection

Key recovery (in particular automated key recovery) must be carried out with extreme caution, as the chance for compromise can be very high. Further, the risk of compromise and the scope of any potential compromise are highly dependent upon the implementation. Therefore, the key recovery infrastructure shall be capable of detecting anomalous key recovery activities and behavior and reporting them to the Entity PMA for further action.

## 6.5 Life Cycle Technical Controls

Individuals with trusted roles in the KED and Key Server facilities (e.g., system administrators, crypto officers, audit administrators, operators, etc.) shall use security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements. These tools and procedures shall check the integrity of the system data, software, discretionary access controls, audit profile, firmware, and hardware to ensure secure operation.

## 6.6 Network Security Controls

Network access to the KED and Key Servers shall be protected as specified in the CertiPath CP Section 6.7 for CA equipment.

Network access to KRA and KRO shall be protected as specified in the CertiPath CP Section 6.7 for RA equipment.

## 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 KRP shall be maintained under the specification change procedures identified in the CertiPath CP Section 9.12.1.

## 7.2 Publication and Notification Policies

This KRP shall be published as specified in the CertiPath CP Section 9.12.2.

## 7.3 Policy Approval Procedures

This KRP shall be approved by the CPMA using the procedures specified in the CertiPath CP Charter.

# APPENDIX A: REFERENCES

The following documents contain information that provides background, examples, or details about the contents of this KRP.

| Number | Title | Revision | Date |
|---|---|---|---|
| FIPS140-2 | *Security Requirements for Cryptographic Modules*<br>http://csrc.nist.gov/publications/index.html | | June 2001 |
| NISTIR 5153 | *Minimum Security Requirements for Multi-User Operating Systems, CSL, NISTIR 5153* | | March 1993 |
| CCIB-98-026 | *Common Criteria for Information Technology Security Evaluation,* Common Criteria Implementation Board | Version 2.1 | August 1999 |
| CertiPath CP | *CertiPath X.509 Certificate Policy* | Version 3.24 | November 2013 |
| | *Requirements for Key Recovery Products: Report of the Technical Advisory Committee (TAC) to Develop a FIPS for the Federal Key Management Infrastructure, Final Report* | | November 1998 |

## APPENDIX B: ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| CA | Certification Authority |
| CC | Common Criteria |
| CP | Certificate Policy |
| CPMA | CertiPath Policy Management Authority |
| CPS | Certification Practices Statement |
| DN | Distinguished Name or Directory Name |
| EAL | Evaluation Assurance Level |
| FIPS | Federal Information Processing Standard |
| I&A | Identification and Authentication |
| IT | Information Technology |
| KED | Key Escrow Database |
| KRA | Key Recovery Agent |
| KRO | Key Recovery Official |
| KRP | Key Recovery Policy |
| KRPS | Key Recovery Practices Statement |
| KRS | Key Recovery System |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| SSN | Social Security Number |
| US | United States |
| VPN | Virtual Private Network |

# APPENDIX C:  GLOSSARY

| | |
|---|---|
| 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 escrow database 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. |
| Key Server | An automated system that obtains subscriber private keys from the Key Escrow Database or another Key Server in order to support decryption of data entering and leaving the Enterprise. An example of such data is e-mail. |
| KRA Workstation | The workstation from which the Key Recovery Agent interfaces with the key escrow database. |
| Key Escrow Database | 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) | A 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 | A person or thing that (1) is the subject named or identified in a certificate issued to such person or thing, and (2) holds a private key that corresponds to a public key listed in that certificate. **Current subscribers** possess valid Entity PKI issued certificates. |
| Third Party | A person other than the subscriber who requests escrowed keys (e.g., law enforcement, supervisor). |
| Two person control | For the purpose of this KRP, two person control is a process that requires two independent, authorized parties to consent to activities involving extraction and restoration of private key data. |