FPKIPA

Federal Public Key Infrastructure Policy Authority

Federal Public Key Infrastructure

Key Recovery Policy

Version 1.0

October 6, 2017

CHI HICKEY

Signature Page

Digitally signed by CHI HICKEY
DN: c=US, o=U.S. Government, ou=General Services Administration, cn=CHI HICKEY, 0.9.2342.19200300.100.1.1=47001002826503
Date: 2017.10.10 11:45:14 -04'00'

FPKI Policy Authority Chair DATE

Change Record

Date	Document Number	Change	Author
10/6/2017	1.0	Initial Document Release	FPKIPA

Table of Contents

1 INTRODUCTION

Key Recovery is the ability to escrow and recover private keys from public/private key pairs associated with public key certificates used for key or data encipherment. 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. The KRS consists of the Key Escrow Database (KED), Key Recovery Agent (KRA) Workstations, Key Recovery Official (KRO) Workstations and data decryption servers.

Since the KRS has a significant impact on the confidentiality services provided by a public key infrastructure (PKI), its design and operation must engender a high degree of trust. This document supplements the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* and describes the procedural and technical security controls required to operate a KRS securely in a manner that meets the requirements of the Federal PKI Policy Authority (FPKIPA). Where applicable, the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* is included by reference.

Any CA that issues key management certificates for PIV credentials shall implement a KRS.

1.1 Overview

The key recovery capability identified in this document is based on the principle that all encryption activities using public-key certificates are performed on behalf of the subject of the encryption certificate or on behalf of the organization that authorized the issuance of the public-key encryption certificates. Therefore, the organization 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 encrypted information for investigative and law enforcement purposes; while some Issuing Organizations require that the contents of incoming and/or outgoing e-mail be examined for compliance with the Organization's 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 associated with the implementation of key recovery operations in a manner that meets the requirements of the FPKIPA. This KRP requires a minimum of two Key Recovery Agents (KRAs) acting on a verified request from an authorized party in order to recover keys from the Key Escrow Database (KED). Where Subscriber key recovery is permitted, Subscribers may authenticate themselves to the KED and perform self-recovery without requiring anyone else's approval. Section 1.3.1.1 describes the KED. Section 1.3.2.2 describes the KRA.

There are two methods by which a CA may become a member of the FPKI Trust Community: subordination under the Federal Common Policy Certification Authority (FCPCA) Trust Anchor or cross certification with one of the Federal PKI CAs, either the FCPCA or the Federal Bridge Certification Authority (FBCA).

Any CA subordinate to the FCPCA that issues key management certificates shall develop a Key Recovery Practice Statement (KRPS) describing the procedures and controls implemented to comply with this KRP. The KRPS may be a separate document or may be combined with the appropriate Certification Practice Statement and/or Registration Practice Statement. FPKIPA will determine the KRPS compliance with this KRP.

Any organization offering key recovery services for key management certificates issued by a CA cross certified with a Federal PKI CA (FCPCA or FBCA) shall do one of the following:

- Adopt this KRP and develop a KRPS describing the procedures and controls implemented to comply with this KRP; or
- Develop a KRP that establishes security and authentication requirements similar to this document, such that it is found comparable to this KRP. This KRP may be a separate document or combined with the organization’s Certificate Policy (CP). And develop a KRPS describing the procedures and controls implemented to comply with the organization’s KRP.

In either case, the KRPS may be a separate document or may be combined with the organization’s Certification Practice Statement (CPS).

The Federal PKI Policy Authority (FPKIPA) will determine the KRPS compliance or KRP comparability with this KRP.

1.2 Document name and identification

Federal Public Key Infrastructure Key Recovery Policy.

1.3 PKI Participants

1.3.1 PKI Authorities

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* concerning PKI Authorities. For Key Recovery, the following additional PKI authority applies:

1.3.1.1 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 self-recovery by a current subscriber.

Section 5.2.1 contains the description of trusted roles required to operate the KED.

1.3.2 Key Recovery Authorities

1.3.2.1 Data Decryption Server

A data decryption server is an automated system that has the capability to obtain subscriber private keys from the KED or another data decryption server for data monitoring purposes (e.g. email inspection). Data decryption servers do not provide keys to subscribers or other third-party human requestors. A data decryption server is a type of Requestor and must adhere to physical, personnel, procedural and technical security requirements of the KED. Implementation of a data decryption server by an Issuing Organization is optional; when implemented, it shall adhere to the requirements established for the KED.

1.3.2.2 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 send the recovered key to the KRO or directly to the Requestor. The KRAs have high level, sensitive access to the KED and are considered Trusted Roles (see Section 5.2.1). Registration Authorities, (RA) as defined in the CP, may fill the role of KRA; however, because KRAs can recover large numbers of keys, the number and location of KRAs should be closely controlled.

KRAs may be employed by an issuing organization/enterprise receiving CA services from a shared service provider. In these cases, the KRAs are authorized to recover keys of subscribers from the KRAs' Organization/Enterprise only.

1.3.2.3 Key Recovery Official (KRO)

Issuing Organizations may choose to use the services of a Key Recovery Official (KRO) in performing identity verification and authorization validation tasks. KROs authenticate the Requestor. The KROs shall be defined as Trusted Roles if they have privileged access to the KED. Trusted Agents, as defined in the CP, may fill the role of KROs that do not have privileged access to the KED.

A KRO performs the following functions:

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

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

1.3.3 Trusted Agents

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 1.3.3.

1.3.4 Key Recovery Requestors

A Requestor is the person who requests the recovery of a decryption private key. A Requestor may be the Subscriber (for self-recovery, when permitted) or a third party (e.g., supervisor, corporate officer or law enforcement officer) authorized to request recovery of a Subscriber’s escrowed key on behalf of the Subscriber or on behalf of the organization. Any individual who can demonstrate a verifiable authority and a need to obtain a recovered key may be considered a requestor.

1.3.4.1 Subscriber

The individual named in the certificate associated with the key being recovered. For devices, this is the human sponsor of the device.

1.3.4.2 Internal Third-Party Requestor

An Internal Third-Party Requestor is any Requestor who is in the Subscriber’s supervisory chain or otherwise authorized to obtain the Subscriber’s key for the Issuing Organization. The Issuing Organization shall identify authorized Requestors and the KRS shall implement the KRP so that the existing Issuing Organization Policy regarding access and release of sensitive information can be met.

1.3.4.3 External Third-Party Requestor

An External Third-Party Requestor is someone (e.g. investigator) outside the Issuing Organization (i.e. the organization on behalf of which the CA issues certificates to subscribers) with a court order or other legal instrument to obtain the decryption private key of the Subscriber. Such court orders shall be validated by the KRA prior to recovery of the Subscriber private keys.

Issuing organizations shall determine internal notification requirements for External Third-Party key recovery requests and account for situations where the law requires the KED to release the Subscriber’s private key without organizational notification.

Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests. The KRS and Issuing Organizations shall implement the KRP so that the existing Issuing Organization policies regarding release of sensitive information can be met.

1.3.5 Relying Parties

Not Applicable

1.3.6 Other Participants

Not Applicable

1.3.7 Relationship to PKI Authorities from CP

The applicable requirements for physical, personnel, and procedural security controls (*X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* Section 5), technical security controls (*X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6), and Compliance Audit (*X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 8) are applied to the PKI Authorities in this KRP as follows:

- CA requirements are applied to the KED and to the data decryption server
- RA requirements are applied to the KRA and KRA automated systems
- RA requirements are applied to the KRO and KRO automated systems, when the KRO has privileged access to the KED

1.4 Certificate usage

Not Applicable

1.5 Policy Administration

The FPKIPA is responsible for the definition, revision and promulgation of this KRP. See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Section 1.5, for additional information. KRP and KRPS administration aligns with CP and CPS/RPS administration, respectively.

1.6 Definitions and Acronyms

See Appendices B and C.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

Not Applicable

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Not Applicable

3.2 Identity Validation

3.2.1 Method to Prove Possession of Private Key

Not Applicable

3.2.2 Authentication of Organization Identity

A third-party requestor shall have his/her authority to act on behalf of the organization validated during the initial identity proofing process described in Section 3.2.3.1 below.

3.2.3 Authentication of Individual Identity

3.2.3.1 Requestor Authentication

This section addresses the requirements for authentication of a third-party Requestor, i.e., a Requestor other than the Subscriber itself. The requirements for authentication, when the Requestor is the Subscriber, are addressed in Section 3.2.3.2.

Identity authentication shall be commensurate with the assurance level of the certificate associated with the key being recovered. Identity shall be established using one of the following methods:

- Procedures specified by the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* for authentication of an individual identity during initial registration for the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose companion private key is being recovered).

- Certificate-based authentication (e.g., digitally signed e-mail or client-authenticated TLS) that can be verified using current, valid (i.e., un-revoked) public key certificates issued by the Issuing Organization’s PKI at the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose companion private key is being recovered).

The KRA or KRO shall verify the identity of the Requestor prior to initiating the key recovery request.

3.2.3.2 Subscriber Authentication

The Subscriber shall establish his or her identity to the KED, KRA or the KRO as specified in Section 3.2.3.1 above.

If the authentication cannot be verified using the public key certificates issued by the associated PKI and for at least the given certificate policy assurance level, the KRA or KRO shall verify the identity of the Subscriber prior to initiating the key recovery request. The authentication mechanism shall be equal to or greater than the authentication mechanisms for initial registration described in the associated CPS for the assurance level of the certificate whose companion private key is being recovered.

For automated self-recovery, the Subscriber must be authenticated to the KED using a valid associated PKI-issued public key certificate. The assurance level of the subscriber certificate shall be equal to or greater than that of the certificate whose companion private key is being recovered.

3.2.3.3 KRA Authentication

The KRA shall authenticate to the KED directly or using a public key certificate issued by the associated 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 and shall meet the requirements of an RA credential as specified in the CP.

3.2.3.4 KRO Authentication

The KRO shall authenticate to the KRA using a public key certificate issued by the associated 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 and shall meet the requirements of an RA credential as specified in the CP.

3.2.3.5 Data Decryption Server Authentication

The data decryption server shall authenticate to the KED directly using a public key certificate issued by the associated PKI. The assurance level of the certificate shall be the same as or greater than that of the highest assurance level encryption certificates issued by the associated PKI.

3.2.4 Non-verified Subscriber Information

Not Applicable

3.2.5 Validation of Authority

3.2.5.1 Requestor Authorization Validation

The KRA or the KRO, as an intermediary for the KRA, shall validate the authorization of the Requestor in consultation with Issuing Organization management and/or legal counsel, as appropriate.

3.2.5.2 Subscriber Authorization Validation

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

3.2.5.3 KRA Authorization Validation

The KED shall verify that the KRA has appropriate privileges to obtain the keys for the identified subscriber’s organization.

3.2.5.4 KRO Authorization Validation

The KED or KRA shall verify that the KRO is authorized to request keys for the identified subscriber.

3.2.5.5 Data Decryption Server Authorization Validation

The KED shall verify that the data decryption server recovery request falls within the organizational scope for which the data decryption server was established.

3.2.6 Criteria for Interoperation

Not Applicable

3.3 Identification and Authentication for Re-key Requests

Not Applicable

3.4 Identification and Authentication for Re-key after Revocation

Not Applicable

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Key Recovery Application

4.1.1 Who Can Submit a Key Recovery Application

Subscribers may request recovery of their own escrowed keys. Key recovery may also be requested by internal third-party requestors permitted by the Issuing Organization policy, as verified by the KRO, and by authorized external third-party requestors (e.g. law enforcement personnel) with a court order from a competent court.

4.1.2 Key Escrow Process and Responsibilities

Subscriber private keys (i.e., decryption private keys) associated with a key management certificate shall be securely escrowed by the KED. The CA shall ensure that the keys are escrowed successfully prior to issuance of the key management certificates.

Subscriber private keys shall be protected during transit and storage using cryptography at least as strong as the key being escrowed.

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

4.1.3 Key Recovery Process and Responsibilities

Communications between the various key recovery participants (KED, data decryption server, KRA, KRO, Requestor and Subscriber) shall be secured 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.

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

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.

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 an associated PKI-issued authentication or signature certificate with an 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 an associated

PKI-issued authentication or signature certificate with an assurance level equal to or greater than that of the escrowed key. Manual requests shall be on paper and shall be signed by hand.

Data decryption servers shall use electronic means to request Subscribers' escrowed keys. Requests shall be authenticated as specified in Section 3.2.3.5.

4.1.3.1 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 using two-person control procedures during recovery and delivery to the authenticated and authorized Requestor. Split key or password procedures are considered adequate two-person controls.

> Practice Note: A combination of physical, procedural and technical security controls can be used to enforce continuous two-person control during recovery and delivery of escrowed keys. The KRS should be designed to maximize the ability to enforce two-person control technically.

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.

4.1.3.2 Automated Self-Recovery

A current Subscriber's escrowed keys may be provided directly to the 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;
- Sending notification to 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 send notification to 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;

  > Practice Note: Where possible, the e-mail address will be from the subject alternative name field of the certificate being recovered.

- 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.

4.1.3.3 Key Recovery During Token Issuance

When a subscriber (individual and/or group/role sponsor or member) is issued a new certificate on a hardware token, encryption keys for the subscriber may be recovered as part of the issuance process as long as the KED uses secure means, such as Global Platform Secure Channel Protocol (SCP), to inject the key history onto the hardware token directly. The hardware token shall meet FIPS 140-2 Level 2 hardware requirements and the key shall be injected into the card such that it is not thereafter exportable. The KED shall notify subscribers (as described in Section 4.1.3.2) of all attempts to recover the subscriber's escrowed keys during token issuance.

This process is applicable also for key history recovery to the hardware token.

4.1.3.4 Key Recovery by Data Decryption Server

An escrowed key may be provided directly to the data decryption server provided the data decryption server is operated under two-person control. The KED shall perform the following activities prior to releasing the key:

- Authenticating the requestor as a legitimate data decryption server;
- Verifying that the data decryption server is authorized to recover the escrowed key for the Issuing Organization to which the key belongs;
- 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 data decryption servers. The data decryption servers shall be designed to maximize the ability to enforce two-person control technically.

> Practice Note: The data decryption server is considered under two-person control when any human action performed on the data decryption server requires two persons.

4.2 Certificate Application Processing

Not Applicable

4.3 Certificate Issuance

Not Applicable

4.4 Certificate Acceptance

Not Applicable

4.5 Key Pair and Certificate Usage

Not Applicable

4.6 Certificate Renewal

Not Applicable

4.7 Certificate Rekey

Not Applicable

4.8 Certificate Modification

Not Applicable

4.9 Certificate Revocation and Suspension

Certificates associated with the recovered private keys shall not be revoked simply because of key recovery. This does not prohibit subscribers from revoking their own certificates for any reason. This KRP neither prohibits nor requires a CA to revoke a certificate due to subscriber self-recovery. See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* for all other aspects of revocation.

4.10 Certificate Status Services

Not Applicable

4.11 End of Subscription

Not Applicable

5 Facility, Management, and Operational Controls

5.1 Physical Controls

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 5.1 and subsections.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

5.2.1.1 KED Roles

5.2.1.1.1 System Administrator

Authorized to configure and maintain the KED operating system, to include the hypervisor, if applicable; establish and maintain system accounts; configure operating system auditing; and perform system backup and recovery.

5.2.1.1.2 Application Administrator

Authorized to install, configure and maintain the KED software; generate KED keys; configure and maintain access controls to KED; and configure KED auditing.

5.2.1.1.3 Audit Administrator

Authorized to review, maintain, and archive audit logs.

5.2.1.2 Data Decryption Server Roles

5.2.1.2.1 System Administrator

Authorized to configure and maintain the data decryption server operating system; establish and maintain system accounts; configure operating system auditing; and perform system backup and recovery.

5.2.1.2.2 Application Administrator

Authorized to install, configure and maintain the data decryption server software; generate data decryption server keys; configure and maintain access controls to the data decryption server; and configure data decryption server auditing.

5.2.1.2.3 Audit Administrator

Authorized to review, maintain, and archive audit logs.

5.2.1.3 Key Recovery Agent (KRA)

All KRAs that operate under this KRP are subject to the stipulations of this KRP. A KRA’s responsibilities are to ensure that the following functions occur according to the stipulations of this KRP:

- Carry out KRO functions as described in Section 5.2.1.4, if no separate KRO is employed;
- Authenticate requests and recover copies of escrowed keys; and
- Distribute copies of escrowed keys to Requestors, with protection as described in Section 4.1.3.1.

5.2.1.4 Key Recovery Official (KRO)

All KROs that operate under this KRP are subject to the stipulations of this KRP. 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 associated KRPS.

5.2.2 Number of Persons Required per Task

Two or more persons are required for the following tasks:

- KED key generation
- Data decryption server key generation
- KED private key backup
- Data decryption server private key backup

Where multiparty control is required, at least one of the participants shall be a System Administrator. All participants must serve in a trusted role as defined in section 5.2.1. Multiparty control shall not be achieved using personnel that serve in the Auditor trusted role.

Under no circumstances shall a KRA or KRO perform a trusted role for a KED or data decryption server. Under no circumstances shall a KRA or KRO perform its own compliance audit function.

The participation of two KRAs shall be required for third-party key recovery.

5.2.3 Identification and Authentication for Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Roles Requiring Separation of Duties

No one individual may occupy more than one of the five roles listed in Section 5.2.1 above: System Administrator, Application Administrator, Audit Administrator, KRA or KRO. A System Administrator, Application Administrator and Audit Administrator may perform the same role on both the KED and data decryption server.

5.3 Personnel Controls

KRS trusted role personnel controls shall meet the requirements set forth in the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Section 5.3 for CA trusted role personnel.

5.4 Audit Logging Procedures

Security auditing capabilities of the hypervisor, operating systems and underlying applications of the KED, data decryption server, KRA workstation, and KRO workstation shall be enabled upon installation and remain enabled during operation.

5.4.1 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 by KED operations staff:

Auditable Event	KED	Data Decryption Server	KRA	KRO
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X	X
Obtaining a third-party time-stamp	X	X	X	X
IDENTITY-PROOFING				
Successful and unsuccessful attempts to assume a role	X	X	X	X

Auditable Event	KED	Data Decryption Server	KRA	KRO
The value of *maximum number of authentication attempts* is changed	X	X	X	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login	X	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X	X
LOCAL DATA ENTRY				
All security-relevant data that is entered in the system	X	X	X	X
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system	X	X	X	X
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X	X
KEY GENERATION				
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X	X
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys	X	X	X	X
All access to certificate subject Private Keys retained within the CA for key recovery purposes	X	--	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE				
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X	X
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication	X	X	X	X
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X
CERTIFICATE REGISTRATION				
All certificate requests	N/A	N/A	N/A	N/A
CERTIFICATE REVOCATION				
All certificate revocation requests	N/A	N/A	N/A	N/A

Auditable Event	KED	Data Decryption Server	KRA	KRO
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a certificate status change request	N/A	N/A	N/A	N/A
PKI COMPONENT CONFIGURATION				
Any security-relevant changes to the configuration of the Component	X	X	X	X
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	X	X	X	X
The access control privileges of a user account or a role are modified	X	X	X	X
CERTIFICATE PROFILE MANAGEMENT				
All changes to the certificate profile	N/A	N/A	N/A	N/A
CERTIFICATE STATUS AUTHORITY MANAGEMENT				
All changes to the CSA profile (e.g. OCSP profile)	N/A	N/A	N/A	N/A
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile	N/A	N/A	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT				
All changes to the certificate revocation list profile	N/A	N/A	N/A	N/A
MISCELLANEOUS				
Appointment of an individual to a Trusted Role	X	X	X	X
Designation of personnel for multiparty control	X	X	N/A	N/A
Installation of the Operating System	X	X	X	X X
Installation of the PKI/Key Escrow/Key Recovery Application	X	X	X	X
Installation of hardware cryptographic modules	X	X	X	X
Removal of hardware cryptographic modules	X	X	X	X
Destruction of cryptographic modules	X	X	X	X
System Startup	X	X	X	X
Logon attempts	X	X	X	X
Receipt of hardware / software	X	X	X	X
Attempts to set passwords	X	X	X	X
Attempts to modify passwords	X	X	X	X

Auditable Event	KED	Data Decryption Server	KRA	KRO
Back up of the internal database	X	X	-	-
Restoration from back up of the internal database	X	X	-	-
File manipulation (i.e., creation, renaming, moving)	X	X	-	- -
Posting of any material to a PKI Repository	N/A	N/A	N/A	N/A
Access to the internal database	X	X	-	-
All certificate compromise notification requests	N/A	N/A	N/A	N/A
Loading tokens with certificates	X	N/A	X	X
Shipment of Tokens	X	N/A	X	X
Zeroizing and Destroying Tokens	X	N/A	X	X
Re-key of the Component	X	X	X	X
CONFIGURATION CHANGES				
Hardware	X	X	X	X
Software	X	X	X	X
Operating System	X	X	X	X
Patches	X	X	X	X
Security Profiles	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to room housing Component	X	X	-	-
Access to the Component	X	X	-	-
Known or suspected violations of physical security	X	X	X	X
ANOMALIES				
Software error conditions	X	X	X	X
Software check integrity failures	X	X	X	X
Receipt of improper messages	X	X	X	X
Misrouted messages	X	X	X	X
Network attacks (suspected or confirmed)	X	X	X	X
Equipment failure	X	X	-	-
Electrical power outages	X	X	-	- -
Uninterruptible Power Supply (UPS) failure	X	X	-	-

Auditable Event	KED	Data Decryption Server	KRA	KRO
Obvious and significant network service or access failures	X	X	-	-
Violations of Certificate or Key Recovery Policy	X	X	X	X
Violations of Certification Key Recovery Practice Statement	X	X	X	X
Resetting Operating System clock	X	X	X	X

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 data decryption 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 5.4.3, and made available during compliance audits.

5.4.2 Frequency of Processing Logs

KED, KRA, KRO and data decryption server audit log processing frequency shall align with CA audit log processing frequency as described in the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Section 5.4.2.

5.4.3 Retention Period for Audit Log

KED, KRA, KRO and data decryption server Audit logs shall be retained on-site until reviewed, in addition to being archived as described in Section 5.5.

5.4.4 Protection of Audit Logs

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. KED, KRA, KRO and data decryption server system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. KRS configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated.

5.4.6 Audit Collection System (internal vs. external)

The audit log collection system may or may not be external to the KRS. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations shall be suspended until the problem has been remedied.

5.4.7 Notification to Event-causing Subject

There is no requirement to notify anyone of an event. No one, including the subscriber shall be notified of a third-party key recovery.

5.4.8 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 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 data decryption server, 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 KRS is operating correctly and securely and is not vulnerable to hacking and unauthorized users.

5.5 Records Archival

The KRS shall follow the General Records Schedules established by the National Archives and Records Administration.

The KRS components (i.e., KED, data decryption server, KRA workstation or KRO workstation) shall maintain a trusted archive of information they store and of transactions they carry out. The primary objective of the archive is reconstruction of key recovery activities, in case of dispute. Examples of disputes may include:

- Validation of 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;
- Verification of transfer of custody of escrowed keys to authorized requestor; and
- Establishment of the circumstances under which a copy of the escrowed key was provided.

5.5.1 Types of Information Recorded

The following information/documentation shall be archived:

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

This KRP shall be archived by the FPKIPA. All other information shall be archived by the KRS and Issuing Organizations to which the KRS provides services.

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.

5.5.2 Retention Period for Archives

The archive retention period shall meet the requirements specified in the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, 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.

5.5.3 Protection of Archive

Protection of the archive shall meet the requirements specified in the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Section 5.5.3.

5.5.4 Archive Backup Procedures

There is no requirement to perform further back up of the archives.

5.5.5 Requirements for Time-stamping of Records

KRS archive records shall be automatically time-stamped as they are created. The time precision shall be such that the sequence of events can be determined. The KRPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal vs. External)

The archival collection system shall be documented in the KRPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures, detailing how to create, verify, package, transmit, and store the KRS archive information, shall be recorded in the KRPS.

5.6 Key Changeover

KED keys shall be changed when necessary to ensure they are at least as strong as the keys being protected.

> Practice Note: To ensure the KED does not get too large, organizations may wish to consider establishing a new KED with its own HSM when the number of keys being protected reaches a predetermined threshold (e.g. 500,000 keys).

A data decryption server, KRA and KRO, when issued certificates, shall be considered end entities and their keys shall be changed in accordance with the requirements set forth in the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.*

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Section 5.7.1 for KRS incident and compromise handling procedures.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Section 5.7.2 for requirements associated with the corruption of computing resources, software, and/or data.

5.7.3 Entity (KRS) Private Key Compromise Procedures

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

If a KRA or KRO certificate is revoked due to compromise, the potential exists for some subscribers' escrowed keys to have been exposed during a 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 *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* 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.

If a 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 associated 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 PKI shall follow its CPS for certificate issuance for the new KRA or KRO public key certificate.

In the event that a data decryption server is compromised or is suspected to be compromised, the FPKIPA shall be notified. The FPKIPA shall be granted sufficient access to information to determine the extent of the compromise. The FPKIPA shall direct the appropriate action. This may include revocation of certificates associated with the compromised private keys obtained by the KED.

5.7.4 Business Continuity Capabilities After a Disaster

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 5.7.4 for requirements to restore KRS functionality after a disaster. KED and data decryption server may take more than 72 hours to restore depending on the business needs of the operator.

5.8 Authority Termination

5.8.1 KED Termination

Upon KED termination, the KRS shall provide archived data to an archive facility as specified in the KRPS.

5.8.2 KRA Termination

Upon KRA termination, the KRS or KRA Organization shall take possession of all KRA archive records.

5.8.3 KRO Termination

Upon KRO termination, the KRS or KRO Organization shall take possession of all KRO archive records.

5.8.4 Data Decryption Server Termination

Upon data decryption server termination, the KRS or Organization controlling the data decryption server shall take possession of all data decryption server archive records.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6.1.1 for key pair generation requirements.

6.1.2 Private Key Delivery to Subscriber

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6.1.2 for private key delivery requirements.

6.1.3 Public Key Delivery to Certificate Issuer

Not Applicable

6.1.4 CA Public Key Delivery to Relying Parties

Not Applicable

6.1.5 Key Sizes

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6.1.5.

6.1.6 Public Key Parameters Generation and Quality Checking

Not Applicable

6.1.7 Key Usage Purposes (as per X.509 v3 usage field)

Not Applicable

6.2 Private Key Protection and Cryptographic Module Engineering Controls

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6.2 and subsections.

6.3 Other Aspects of Key Pair Management

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6.3 and subsections.

6.4 Activation Data

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6.4 and subsections for activation data requirements.

6.5 Computer Security Controls

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6.5 and subsections.

Remote administration for KED and data decryption server, if implemented, shall not bypass two-person control on their operations.

KRA and KRO workstation operating systems shall meet the following requirements:

- Require authenticated logins
- Provide discretionary access control
- Provide a security audit capability
- Require identification and authentication
- Require a trusted path for identification and authentication
- Provide residual information protection for storage objects such as memory, disk sectors, device registers.
- Provide operating system self-protection
- Provide domain isolation for application processes

6.6 Life Cycle Technical Controls

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6.6 and subsections.

6.7 Network Security Controls

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6.7.

A network guard, firewall, or filtering router shall protect network access to a KRA/KRO workstation. The network guard, firewall, or filtering router shall limit services allowed to and from the KRA/KRO workstation to those required to perform KRA/KRO functions.

Protection of KRA/KRO workstation shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the KRA/KRO workstation shall be necessary to the functioning of the KRA/KRO application.

6.8 Time Stamping

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 6.8.

7 CERTIFICATE, CRL, AND OCSP PROFILES

Not Applicable

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 8.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No stipulation for key escrow and key recovery services.

9.2 Financial Responsibility

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.2.

9.3 Confidentiality of Business Information

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.3.

9.4 Privacy of Personal Information

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.4

9.5 Intellectual Property Rights

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.5.

9.6 Representations and Warranties.

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.6.

9.6.1 KED Representations and Warranties

A KED that provides escrowed keys to Requestors under this KRP shall conform to the stipulations of this document. In particular, the following stipulations apply:

- The FPKIPA shall approve the KRPS prior to key escrow.
- The KED shall operate in accordance with the stipulations of the KRPS and this KRP.
- The KED shall automatically notify the subscribers when their private keys have been escrowed (e.g., a dialog box may appear on a subscriber’s screen during the certificate request process).

Practice Note: This notification may be part of the subscriber agreement provided during the subscriber registration process.

- The KED 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.

9.6.2 KRA/KRO Representations and Warranties

9.6.2.1 KRA Obligations:

KRAs that submit requests as described in this KRP shall comply with the stipulations of this KRP and the applicable KRPS. In particular, the following stipulations apply:

- KRAs shall keep a copy of this KRP and the applicable KRPS.
- KRAs shall operate in accordance with the stipulations of this KRP and the applicable KRPS.
- KRAs shall protect subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.
- KRAs shall protect all information associated with key recovery, 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.
- KRAs shall release Subscribers' escrowed keys only for properly authenticated and authorized requests from Requestors.
- When applicable, KRAs shall authenticate the KROs using strong authentication techniques.
- KRAs shall validate the authorization of the KRO by ensuring that the KRO is an authorized KRO for the Subscriber for whom key recovery has been requested.
- 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 behavior as indicators of possible problems in the infrastructure, and initiate inquiries or investigations as appropriate.

9.6.2.2 KRO Obligations

A KRO initiates a key recovery request for a Requestor. When using the services of a KRO, 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.
- 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.
- When the Requestor is authenticated on the basis of digital signature, the KRO shall forward the Requestor's digitally signed object to the KRA in a form verifiable by the KRA.
- 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 private decryption 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 associated with key recovery, including the KRO's own private key(s), that could be used to obtain the Subscriber's recovered private decryption 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.
- 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 himself when requesting key recovery services.
- The KRO shall keep records of all recovery requests and disposition, including acknowledgement of receipt by the Requestor.

If an Issuing Organization chooses not to implement the KRO role, then these obligations become the responsibility of the KRA in addition to the obligations in Section 9.6.2.1 above.

9.6.3 Subscriber Representations and Warranties

Subscribers shall comply with the following:

- Subscribers shall provide accurate identification and authentication information during initial 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.

9.6.4 Requestor Representations and Warranties

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.
- Third-party Requestors shall destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- Requestors shall request and use the Subscriber's escrowed key(s) 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 (e.g. the Requestor sends a digitally signed request using the credential issued by the Entity PKI at the same or higher assurance level as the key being recovered).
- The Third-Party Requestor shall protect information concerning each key recovery operation.
- The Third-Party Requestor shall communicate information concerning the recovery to the Subscriber when appropriate as determined by the reason for the recovery. The decision to notify the Subscriber shall be based on the law and the Issuing Organization's policies and procedures for third party information access.
- In the event that the Third-Party Requestor notifies the Subscriber of a key recovery, the Requestor shall consult with 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 Issuing Organization's policies relating to protection and release of the recovered key.

- Upon receipt of the recovered key(s), the Third-Party Requestor shall sign[1] an attestation to the effect:

  > "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 *[Subscriber Name]*. 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 *[Issuing Organization]* policies, applicable laws and Federal regulations concerning the protection of the recovered key and any data recovered using the key."

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Data Decryption Server Representations and Warranties

Prior to the beginning of the operation of a data decryption server, the Issuing Organization shall formally acknowledge and agree to the obligations described here by signing an appropriate document.

- The data decryption server shall protect Subscribers' recovered key(s) from compromise. The data decryption 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 data decryption server shall destroy Subscribers' keys when no longer required (i.e., when the data has been recovered).
- The data decryption server shall request the Subscriber's escrowed key(s) only upon receiving a request to decrypt subscriber data from an authenticated authorized Enterprise system (e.g., an e-mail Server)
- The data decryption 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 data decryption server shall provide accurate identification and authentication information at the same or higher assurance level as required for issuing new PKI certificates at the assurance level of the key being requested.

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

9.7 Disclaimers of Warranties

KRSs operating under this KRP may not disclaim any responsibilities described in this KRP.

9.8 Limitations of Liability

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.8.

9.9 Indemnities

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.9.

9.10 Term and Termination

9.10.1 Term

This KRP becomes effective when approved by the FPKIPA. This KRP has no specified term.

9.10.2 Termination

Termination of this KRP is at the discretion of the FPKIPA.

9.10.3 Effect of Termination and Survival

The requirements of this KRP remain in effect through the end of the archive period for the certificate corresponding to the last escrowed key.

9.11 Individual Notices and Communications with Participants

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.11

9.12 Amendments

This KRP shall be subject to the requirements set forth for the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.12 and subsections.

9.13 Dispute Resolution Provisions

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.13.

9.14 Governing Law

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.14.

9.15 Compliance with Applicable Law

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.15.

9.16 Miscellaneous Provisions

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.16 and subsections.

9.17 Other Provisions

See the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Section 9.17.

APPENDIX A: ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
DN	Distinguished Name or Directory Name
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FPKI	Federal PKI
FPKIPA	Federal PKI Policy Authority
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
RPS	Registration Practice Statement
VPN	Virtual Private Network

APPENDIX B: GLOSSARY

Encryption Certificate	A certificate containing a public key that is used to encrypt and possibly 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 referred to as key escrow.
Issuing Organization	The organization on behalf of which the CA issues certificates to subscribers and which therefore maintains jurisdiction over all issued certificates.
Key Escrow	The retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.
Key Escrow Database	The function, system, or subsystem that maintains the key escrow repository and responds to key escrow and key recovery requests from one or more Key Recovery Agents, as specified by the Key Recovery Policy.
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 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 request forms	Any documentation required by the KRA or KRO in order to perform key recovery on a subscriber's or third-party requestor's behalf.
Key Recovery System (KRS)	The hardware, software, staff, policies and procedures utilized to store the private decryption keys of Subscribers securely and recover them when appropriate.
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.
data decryption server	An automated system that obtains subscriber private keys from the Key Escrow Database or another data decryption 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.
Policy 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.
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.
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.