
# GPO Public Key Infrastructure

# Key Recovery Practices Statement

**Version 1.0**

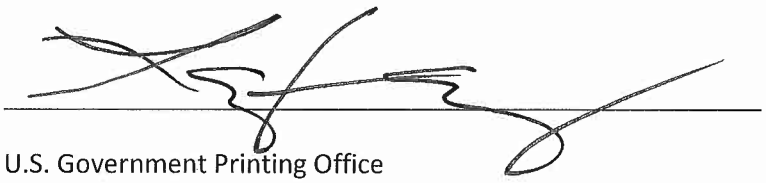
**Feb. 20, 2018**

# SIGNATURE PAGE

4/10/18

U.S. Government Printing Office DATE

Public Key Infrastructure Operating Authority



4/10/18

U.S. Government Printing Office DATE

Public Key Infrastructure Policy Authority Chair

Change Record

| Date | Document Number | Change | Author |
|---|---|---|---|
| 2/20/2018 | 1.0 | Initial Document Release | US GPO |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 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 concepts of a Key Recovery System (KRS) are embedded in the Entrust Authority Security Manager Administration (SMA) software, which is what the GPO PCA and SCA use for its CA functions. The GPO PKI provides the computer system hardware, software, staff and procedures to store the private keys securely and recover them when appropriate. The GPO PCA and SCA provides the all the required KRS elements, which consists of the Key Escrow Database (KED), and Key Recovery Agent (KRA) Workstations. All of the KRS elements are embedded in the Entrust Authority SMA software, along with cryptographic and computer server hardware, and the workstations controlled and administered by the GPO PKI trusted role staff, using the Entrust Authority SMA software and 2 factor hardware tokens.

Since the GPO KRS has a significant impact on the confidentiality services provided by the GPO public key infrastructure (PKI), its design and operation engenders a high degree of trust. The GPO PCA and SCA CPS and practices comply with the GPO PKI Certificate Policy (CP), which complies with the Federal PKI Key Recovery Policy.

## 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.

## 1.2 Document name and identification

GPO PKI Key Recovery Practices Statement (KRPS).

## 1.3 PKI Participants

The PKI Participants and Authorities are defined in the GPO PCA CPS and GPO SCA CPS, and these definitions are incorporated by reference in this GPO KRPS.

### 1.3.1 PKI Authorities

The PKI Participants and Authorities are defined in the GPO PCA CPS and GPO SCA CPS, and these definitions are incorporated by reference in this GPO KRPS.

#### 1.3.1.1 Key Escrow Database (KED)

The KED is embedded into the GPO PCA and SCA Entrust Authority SMA software and hardware systems. Therefore, for the GPO PCA and SCA, the KED is embedded and implemented in the GPO PCA and SCA Entrust Authority SMA software and hardware. The GPO KED, as embodied by the Entrust Authority SMA software and hardware implementation for the GPO PCA and SCA, embodies the functions that maintains the key escrow repository and responds to key registration requests. The GPO 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 GPO 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.

The GPO PKI does not utilize a Data Decryption Server.

#### 1.3.2.2 Key Recovery Agent (KRA)

For purposes of the GPO KRPS, the GPO KRA role can be fulfilled by either of the following two (2) following GPO PKI trusted roles:

- GPO Registration Authority (RA), including authorized GPO Local RA's
- GPO Security Officer (SO)

That is, for Key Recovery, either of the above GPO PKI trusted role staff are authorized by this GPO KRPS to serve in the role of the GPO KRA.

#### 1.3.2.3 Key Recovery Official (KRO)

GPO does not utilize the services of a Key Recovery Official (KRO) in the GPO KRPS.

### 1.3.3 Trusted Agents

GPO does not utilize Trusted Agents in this GPO KRPS.

### 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 GPO. There are two (2) classes of Internal Third-Party Requestors, as follows: 1) GPO requestors; and 2) Non-GPO Subscriber requestors. For case #1 above, GPO has designated and identified authorized GPO Internal Third-Party Requestors as being any GPO supervisor or manager, as defined in the GPO Human Capital records. The KRA shall ensure that the GPO party is a supervisor or manager by reviewing the GPO Active Directory (AD) information for the requestor to ensure the person's title in the GPO AD lists them as Supervisor or Manager of the GPO organization involved, or by obtaining confirmation via email from the GPO Chief Human Capital Officer or designee. For Non-GPO Internal Third-Party Requestors (case #2 above), GPO has designated and identified the authorized parties as those parties on the MOA with the GPO PKI for Certificate Revocation. The GPO KRPS is implemented to comply with all GPO policies regarding access and release of sensitive GPO information, including the GPO IT Security Program Statement of Policy. For Non-GPO parties, the Non-GPO Requestor shall ensure that all Non-GPO Organizational policies for access to and any release of sensitive information are complied with.

#### 1.3.4.3 External Third-Party Requestor

Any External Third-Party (non-GPO) Requestor not affiliated with the Subscriber's organization 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 and the GPO Office of General Counsel prior to recovery of the Subscriber private keys. In addition, for any non-GPO Subscriber, the Office of General Counsel (or equivalent) for the Subscriber's organization must also validate and approve the court order.

For situations where the law requires the KED to release the Subscriber's private key without organizational notification, GPO shall still require the validation and approval of the GPO Office of General Counsel to ensure the law requirements are being interpreted by the

GPO Office of General Counsel. In addition, for any non-GPO Subscriber, the Office of General Counsel (or equivalent) for the Subscriber's organization must also validate and approve to ensure they have interpreted the law's requirements.

Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests. This GPO KRPS complies with the GPO CP KRP requirements such that GPO policies regarding release of sensitive information are complied with and 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 from the GPO PKI Certificate Policy (CP) Section 5), technical security controls (GPO PKI CP Section 6), and Compliance Audit (GPO PKI CP Section 8) are applied to the PKI Authorities in this GPO KRPS as follows:

- CA requirements are applied to the KED and to the data decryption server (NOTE: GPO PKI does not utilize a data decryption server.)
- RA requirements are applied to the KRA and KRA automated systems

## 1.4 Certificate usage

Not Applicable

## 1.5 Policy Administration

The GPO PKI Policy Authority and Operational Authority are responsible for the definition, revision and promulgation of this GPO KRPS.

## 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 GPO PKI Certificate Policy (CP) 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 GPO 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 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 or KRA 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 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.

In the specific case of a human Subscriber that was initially identity proofed using in-person identity proofing by the GPO PKI RA, using the procedures in the GPO PCA or SCA CPS document (section 3.2.3.1), a subsequent request for Key Recovery by that same human Subscriber can be submitted via valid email request to the GPO RA, using the email address of that subscriber during the initial identity proofing procedure, and which was embedded in the original certificate for that human subscriber. If the email request comes from a different email address, the request shall be rejected by the GPO RA. The GPO RA shall ensure that this valid email request for Key Recovery in this situation is submitted to and logged in the GPO IT Service Desk system as well.

#### 3.2.3.3 KRA Authentication

The KRA shall authenticate to the GPO KED (as embodied by the GPO PCA and SCA Entrust Authority SMA) directly or using a public key certificate issued by the GPO 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

No stipulation since the GPO PKI does not use the KRO role.

#### 3.2.3.5 Data Decryption Server Authentication

No stipulation since the GPO PKI does not use a data decryption server.

### 3.2.4 Non-verified Subscriber Information

Not Applicable

### 3.2.5 Validation of Authority

#### 3.2.5.1 Requestor Authorization Validation

The KRA shall validate the authorization of the Requestor as described above in section 1.3.4 of this GPO KRPS.

#### 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 (as embodied in the GPO PCA and SCA Entrust Authority SMA) 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

No stipulation since GPO PKI does not utilize the KRO role.

#### 3.2.5.5 Data Decryption Server Authorization Validation

No stipulation since GPO PKI does not utilize a data decryption server.

### 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 GPO PKI, as defined above in section 1.3.4 of this GPO KRPS, and by authorized external third-party requestors (e.g. law enforcement personnel) with a court order from a competent court and as validated and authorized as defined in section 1.3.4 of this GPO KRPS.

### 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, KRA, 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 or KRA. 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. 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, from the GPO PKI or a PKI cross-certified to the Federal PKI (FPKI). Manual requests shall be on paper and shall be signed by hand.

#### 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.

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;
- 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

There is no stipulation for this, since the GPO PKI does not use a separate, dedicated Data Decryption Server. Key Recovery is always accomplished by the GPO PKI using the GPO Entrust Authority SMA used by the GPO PCA and SCA.

## 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 following the procedures of the GPO PCA/SCA CPS. The GPO PKI CP neither prohibits nor requires the GPO PCA or SCA to revoke a certificate due to subscriber self-recovery. See the GPO PKI CP 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 GPO PKI CP 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.

The GPO PKI Auditor role, from the GPO PCA and SCA CPS documents, fulfills this role for the GPO PKI for this GPO KRPS.

#### 5.2.1.2 Data Decryption Server Roles

The GPO PKI does not employ a separate, distinct Data Decryption Server, therefore the roles below for this do not apply.

##### *5.2.1.2.1 System Administrator*

No stipulation since the GPO PKI does not employ a separate, distinct Data Decryption Server.

##### *5.2.1.2.2 Application Administrator*

No stipulation since the GPO PKI does not employ a separate, distinct Data Decryption

Server.

#### *5.2.1.2.3 Audit Administrator*

No stipulation since the GPO PKI does not employ a separate, distinct Data Decryption Server.

### 5.2.1.3 Key Recovery Agent (KRA)

All KRAs that operate under this GPO KRPS are subject to the stipulations of the GPO PKI CP. A KRA's responsibilities are to ensure that the following functions occur according to the stipulations of the GPO PKI CP and this GPO KRPS:

- Carry out KRO functions as described in Section 5.2.1.4, since 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)

The GPO PKI does utilize the KRO role. Therefore no stipulation for this.

### 5.2.2 Number of Persons Required per Task

Two or more persons are required for the following tasks:

- KED key generation
- KED 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 perform a trusted role for a KED. Under no circumstances shall a KRA 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 four roles listed in Section 5.2.1 above: System Administrator, Application Administrator, Audit Administrator or KRA.

## 5.3 Personnel Controls

KRS trusted role personnel controls shall meet the requirements set forth in the GPO PKI CP, Section 5.3 for GPO-CA trusted role personnel.

## 5.4 Audit Logging Procedures

Security auditing capabilities of the hypervisor, operating systems and underlying applications of the KED and KRA 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 (does not apply to GPO PKI) | KRA | KRO (does not apply to GPO PKI) |
|---|---|---|---|---|
| **SECURITY AUDIT** | | | | |
| Any changes to the Audit parameters, e.g., audit frequency, type of event audited | X | N/A | X | N/A |
| Any attempt to delete or modify the Audit logs | X | N/A | X | N/A |
| Obtaining a third-party time-stamp | X | N/A | X | N/A |
| **IDENTITY-PROOFING** | | | | |
| Successful and unsuccessful attempts to assume a role | X | N/A | X | N/A |

| Auditable Event | KED | Data Decryption Server (does not apply to GPO PKI) | KRA | KRO (does not apply to GPO PKI) |
|---|---|---|---|---|
| The value of *maximum number of authentication attempts* is changed | X | N/A | X | N/A |
| The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login | X | N/A | X | N/A |
| An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts | X | N/A | X | N/A |
| An Administrator changes the type of authenticator, e.g., from a password to a biometric | X | N/A | X | N/A |
| **LOCAL DATA ENTRY** | | | | |
| All security-relevant data that is entered in the system | X | N/A | X | N/A |
| **REMOTE DATA ENTRY** | | | | |
| All security-relevant messages that are received by the system | X | N/A | X | N/A |
| **DATA EXPORT AND OUTPUT** | | | | |
| All successful and unsuccessful requests for confidential and security-relevant information | X | N/A | X | N/A |
| **KEY GENERATION** | | | | |
| Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys) | X | N/A | X | N/A |
| **PRIVATE KEY LOAD AND STORAGE** | | | | |
| The loading of Component private keys | X | N/A | X | N/A |
| All access to certificate subject Private Keys retained within the CA for key recovery purposes | X | N/A | X | N/A |
| **TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE** | | | | |
| All changes to the trusted Component Public Keys, including additions and deletions | X | N/A | X | N/A |
| **SECRET KEY STORAGE** | | | | |
| The manual entry of secret keys used for authentication | X | N/A | X | N/A |
| **PRIVATE AND SECRET KEY EXPORT** | | | | |
| The export of private and secret keys (keys used for a single session or message are excluded) | X | N/A | X | N/A |
| **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 (does not apply to GPO PKI) | KRA | KRO (does not apply to GPO PKI) |
|---|---|---|---|---|
| **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 | N/A | X | N/A |
| **ACCOUNT ADMINISTRATION** | | | | |
| Roles and users are added or deleted | X | N/A | X | N/A |
| The access control privileges of a user account or a role are modified | X | N/A | X | N/A |
| **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 | N/A | X | N/A |
| Designation of personnel for multiparty control | X | N/A | N/A | N/A |
| Installation of the Operating System | X | N/A | X | N/A |
| Installation of the PKI/Key Escrow/Key Recovery Application | X | N/A | X | N/A |
| Installation of hardware cryptographic modules | X | N/A | X | N/A |
| Removal of hardware cryptographic modules | X | N/A | X | N/A |
| Destruction of cryptographic modules | X | N/A | X | N/A |
| System Startup | X | N/A | X | N/A |
| Logon attempts | X | N/A | X | N/A |
| Receipt of hardware / software | X | N/A | X | N/A |
| Attempts to set passwords | X | N/A | X | N/A |
| Attempts to modify passwords | X | N/A | X | N/A |

| Auditable Event | KED | Data Decryption Server (does not apply to GPO PKI) | KRA | KRO (does not apply to GPO PKI) |
|---|---|---|---|---|
| Back up of the internal database | X | N/A | - | N/A |
| Restoration from back up of the internal database | X | N/A | - | N/A |
| File manipulation (i.e., creation, renaming, moving) | X | N/A | - | N/A |
| Posting of any material to a PKI Repository | N/A | N/A | N/A | N/A |
| Access to the internal database | X | N/A | - | N/A |
| All certificate compromise notification requests | N/A | N/A | N/A | N/A |
| Loading tokens with certificates | X | N/A | X | N/A |
| Shipment of Tokens | X | N/A | X | N/A |
| Zeroizing and Destroying Tokens | X | N/A | X | N/A |
| Re-key of the Component | X | N/A | X | N/A |
| **CONFIGURATION CHANGES** | | | | |
| Hardware | X | N/A | X | N/A |
| Software | X | N/A | X | N/A |
| Operating System | X | N/A | X | N/A |
| Patches | X | N/A | X | N/A |
| Security Profiles | X | N/A | X | N/A |
| **PHYSICAL ACCESS / SITE SECURITY** | | | | |
| Personnel Access to room housing Component | X | N/A | - | N/A |
| Access to the Component | X | N/A | - | N/A |
| Known or suspected violations of physical security | X | N/A | X | N/A |
| **ANOMALIES** | | | | |
| Software error conditions | X | N/A | X | N/A |
| Software check integrity failures | X | N/A | X | N/A |
| Receipt of improper messages | X | N/A | X | N/A |
| Misrouted messages | X | N/A | X | N/A |
| Network attacks (suspected or confirmed) | X | N/A | X | N/A |
| Equipment failure | X | N/A | - | N/A |
| Electrical power outages | X | N/A | - | N/A |
| Uninterruptible Power Supply (UPS) failure | X | N/A | - | N/A |

| Auditable Event | KED | Data Decryption Server (does not apply to GPO PKI) | KRA | KRO (does not apply to GPO PKI) |
|---|---|---|---|---|
| Obvious and significant network service or access failures | X | N/A | - | N/A |
| Violations of Certificate or Key Recovery Policy | X | N/A | X | N/A |
| Violations of Certification Key Recovery Practice Statement | X | N/A | X | N/A |
| Resetting Operating System clock | X | N/A | X | N/A |

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 KRAs 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 and KRA audit log processing frequency shall align with CA audit log processing frequency as described in the GPO PKI CP, Section 5.4.2.

### 5.4.3 Retention Period for Audit Log

KED and KRA 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 and KRA 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 KRA 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 for PKI systems established by the National Archives and Records Administration.

The KRS components (i.e., KED or KRA 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:

- The GPO PKI CP and GPO PKI KRPS;
- Agreements, if any (with KRAs and subscribers, and LRA Organizations)
- Security audit data; and
- Escrowed keys.

This KRPS shall be archived by the GPO PKI. All other information shall be archived by the GPO KRS.

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 GPO PKI 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.

### 5.5.3 Protection of Archive

Protection of the archive shall meet the requirements specified in the GPO PKI CP, 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 GPO KRPS uses the same method as the GPO PCA and SCA for how the system clocks used for time-stamping are maintained in synchrony with the authoritative NIST time standard servers.

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

The archival collection system is the same as for the GPO PCA and SCA (internal) and as described in the GPO PCA and SCA CPS documents.

### 5.5.7 Procedures to Obtain and Verify Archive Information

Procedures, detailing how to create, verify, package, transmit, and store the KRS archive information, are the same as for the GPO PCA and SCA CPS and are documented in the GPO PCA and SCA CPS documents.

## 5.6 Key Changeover

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

A KRA (which equates for the GPO PKI to a GPO RA role), when issued certificates, shall be considered an end entity and their keys shall be changed in accordance with the requirements set forth in the GPO PKI CP.

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Incident and Compromise Handling Procedures

The GPO KRS incident and compromise procedures are the same as the GPO PCA and SCA procedures as documented in the GPO PCA and SCA CPS documents, which are all in compliance with the GPO PKI CP.

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

The GPO procedures and practices for this are the same as those documented in the GPO PCA and SCA CPS documents. The GPO PCA and SCA documents define the procedures and practices for this for GPO KRS.

### 5.7.3 GPO KRS Private Key Compromise Procedures

In the event that the GPO KED is compromised or is suspected to be compromised, the GPO PKI Policy Authority shall be notified, and the GPO PKI shall notify the FPKIPA. The GPO PKI Operational Authority shall be granted sufficient access to GPO KRS information to understand the extent of the compromise. The GPO PKI Operational Authority shall direct the appropriate action. This may include revocation of certificates associated with the compromised private keys stored in the KED.

If a KRA 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, in conjunction with the GPO PKI Operational Authority, shall review the audit records to identify all potentially exposed escrowed keys. Each of the potentially exposed escrowed keys shall be revoked, according to GPO PCA and SCA CPS procedures specified in the GPO PCA and SCA CPS documents, 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 certificate is revoked for any reason, but the KRA remains authorized to perform his or her duties, then the KRA shall request a new KRA or KRO certificate from the GPO PKI, which equates to the procedures for requesting a GPO PKI RA certificate. The GPO PCA or SCA that revoked the KRA certificate shall ensure that all the requirements of the GPO PCA or SCA CPS for revocation notification are met. The GPO PKI shall follow the GPO PCA and SCA CPS procedures for certificate issuance for the new KRA public key certificate (which equates to the RA procedures).

### 5.7.4 Business Continuity Capabilities After a Disaster

See the GPO PKI CP, along with the GPO PCA and SCA CPS documents, Section 5.7.4 for requirements to restore KRS functionality after a disaster. The time to restore the KED is the same as the definitions for the GPO PCA and SCA continuity after a disaster, as defined in the GPO PCA and SCA CPS documents.

## 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 GPO PCA and SCA CPS documents.

### 5.8.2 KRA Termination

Upon KRA termination, the KRS and GPO shall take possession of all KRA archive records, as specified in the GPO PCA and SCA CPS documents.

### 5.8.3 KRO Termination

No stipulation since the GPO PKI does not utilize the KRO role.

### 5.8.4 Data Decryption Server Termination

No stipulation since the GPO PKI does not utilize a data decryption server.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key Pair Generation

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA documents (Section 6.1.1 for key pair generation requirements).

### 6.1.2 Private Key Delivery to Subscriber

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA documents (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

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (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

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 6.2 and subsections).

## 6.3 Other Aspects of Key Pair Management

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 6.3 and subsections).

## 6.4 Activation Data

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 6.4 and subsections for activation data requirements).

## 6.5 Computer Security Controls

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 6.5 and subsections).

Remote administration for the KED, if implemented, shall not bypass two-person control on their operations and comply with the GPO PCA and SCA CPS documents.

KRA 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

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 6.6 and subsections).

## 6.7 Network Security Controls

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 6.7).

A network guard, firewall, or filtering router protects network access to all the GPO KRA workstations. The network guard, firewall, or filtering router shall limit services allowed to and from the KRA workstation to those required to perform KRA functions.

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

## 6.8 Time Stamping

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 6.8).

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

Not Applicable

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 8).

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 Fees

No stipulation for key escrow and key recovery services.

## 9.2 Financial Responsibility

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 9.2).

## 9.3 Confidentiality of Business Information

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 9.3).

## 9.4 Privacy of Personal Information

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 9.4).

## 9.5 Intellectual Property Rights

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA documents (Section 9.5).

## 9.6 Representations and Warranties.

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA documents (Section 9.6).

### 9.6.1 KED Representations and Warranties

The GPO KED that provides escrowed keys to Requestors under this GPO KRPS shall conform to the stipulations of the GPO PKI CP and this KRPS. In particular, the following stipulations apply:

- The GPO PKI Operational Authority and Policy Authority shall approve the GPO KRPS prior to key escrow.
- The GPO KED shall operate in accordance with the stipulations of this GPO KRPS and the GPO PKI CP.
- The GPO KED shall notify the subscriber as part of the Subscriber Agreement provided during the Subscriber registration process.

- The GPO PCA and SCA shall be monitored for KRA 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 shall comply with the requirements and practices of this GPO KRPS. In particular, the following stipulations apply:

- GPO KRAs shall have and keep a copy of this GPO KRPS available.
- GPO KRAs shall operate in accordance with the stipulations of the GPO PKI CP, the GPO PCA and SCA CPS documents, and this GPO KRPS.
- GPO KRAs shall protect subscribers' escrowed keys from unauthorized disclosure, including the encrypted files and associated decryption keys.
- GPO KRAs shall protect all information associated with key recovery, including the KRA's own key(s), which could be used to recover subscribers' escrowed keys.
- GPO KRAs shall release Subscribers' escrowed keys only for properly authenticated and authorized requests from Requestors.
- GPO KRAs shall protect all information regarding all occurrences of key recovery.
- GPO KRAs shall communicate knowledge of a recovery process only to the Requestor involved in the key recovery.
- GPO KRAs shall not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the Requestor.

#### 9.6.2.2 KRO Obligations

Since the GPO does not implement the KRO role, then these obligations below become the responsibility of the KRA in addition to the obligations in Section 9.6.2.1 above.

- 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.

### 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 below. For Subscribers, these obligations are contained in the Subscriber Agreement during the certificate registration process. For Third-Party Requestors, a GPO PKI Key Recovery Registration form is processed by the KRA (same as GPO RA and Security Officer roles) and the Third-Party Requestor.

- 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 the KRA, 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 (when not the Subscriber) 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 KRA, 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 KRA 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

No stipulation since the GPO PKI does not utilize a separate data decryption server.

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

## 9.7 Disclaimers of Warranties

KRSs operating under this KRPS may not disclaim any responsibilities described in the GPO PKI CP or GPO PCA and SCA CPS documents.

## 9.8 Limitations of Liability

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 9.8).

## 9.9 Indemnities

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 9.9).

## 9.10 Term and Termination

### 9.10.1 Term

This KRPS becomes effective when approved by the GPO PKI Policy Authority and GPO PKI Operational Authority. This KRPS has no specified term.

### 9.10.2 Termination

Termination of this KRPS is at the discretion of the GPO PKI Policy Authority.

### 9.10.3 Effect of Termination and Survival

The requirements of this GPO KRPS 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

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 9.11).

## 9.12 Amendments

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 9.12 and subsections).

## 9.13 Dispute Resolution Provisions

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA CPS documents (Section 9.13).

## 9.14 Governing Law

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA documents (Section 9.14).

## 9.15 Compliance with Applicable Law

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA documents (Section 9.15).

## 9.16 Miscellaneous Provisions

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA documents (Section 9.16.and subsections).

## 9.17 Other Provisions

The GPO KRPS requirements and practices are the same as defined in the GPO PCA and SCA documents (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. |