TSCP Key Recovery Policy
Version 1.0

Prepared by: Shauna Russell, TPMA Chair

Approved by: TPMA

Version: 1.0

Date: August 25, 2014

THE TSCP KEY RECOVER POLICY VERSION 1 WAS APPROVED BY VOTE OF THE TPMA ON AUGUST 25, 2014.

X Shauna Russell - SIG

Digitally signed by Shauna Russell - SIG
DN: c=US, o=Cassidian Communications, ou=Subscribers, ou=TSCP INC, serialNumber=4300000159, cn=Shauna Russell - SIG
Date: 2015.04.28 11:24:41 -04'00'

Shauna Russell
TPMA Chair

Document Change History for the TSCP Key Recovery Policy

Version Number	Version Date	Revision Details	Author (s)	Approved by
0.1	7/11/2014	Initial Final Draft	Shauna Russell	
1.0	8/25/2014	Official Publication of TPMA Approved v.1	Shauna Russell	TPMA

Terms and Conditions

Transglobal Secure Collaboration Participation, Inc. (TSCP) is a consortium comprising a number of commercial and government members (as further specified at http://www.tscp.org) (each a "TSCP Member"). This specification was developed and is being released under this open source license by TSCP.

Use of this specification is subject to the disclaimers and limitations described below. By using this specification, you (the user) agree to and accept the following terms and conditions:

1. This specification may not be modified in any way. In particular, no rights are granted to alter, transform, create derivative works from or otherwise modify this specification. Redistribution and use of this specification, without modification, is permitted provided that the following conditions are met:

- Redistributions of this specification must retain the above copyright notice, this list of conditions, and all terms and conditions contained herein.
- Redistributions in conjunction with any product or service must reproduce the above copyright notice, this list of conditions, and all terms and conditions contained herein in the documentation and/or other materials provided with the distribution of the product or service.
- TSCP's name may not be used to endorse or promote products or services derived from this specification without specific prior written permission.

2. The use of technology described in or implemented in accordance with this specification may be subject to regulatory controls under the laws and regulations of various jurisdictions. The user bears sole responsibility for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products and/or services as a result of such laws or regulations.

3. THIS SPECIFICATION IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. TSCP AND EACH TSCP MEMBER DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, QUIET ENJOYMENT, ACCURACY, AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER TSCP NOR ANY TSCP MEMBER WARRANTS (A) THAT THIS SPECIFICATION IS COMPLETE OR WITHOUT ERRORS, (B) THE SUITABILITY FOR USE IN ANY JURISDICTION OF ANY PRODUCT OR SERVICE WHOSE DESIGN IS BASED IN WHOLE OR IN PART ON THIS SPECIFICATION, OR (C) THE SUITABILITY OF ANY PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF TSCP OR ANY THIRD PARTY.

4. IN NO EVENT SHALL TSCP OR ANY TSCP MEMBER BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS SPECIFICATION, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS SPECIFICATION, THE USER WAIVES ANY SUCH CLAIM AGAINST TSCP OR ANY TSCP MEMBER RELATING TO THE USE OF THIS SPECIFICATION. IN NO EVENT SHALL TSCP OR ANY TSCP MEMBER BE LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO ANY USER OF THIS SPECIFICATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5. TSCP reserves the right to modify or amend this specification at any time, with or without notice to the user, and in its sole discretion. The user is solely responsible for determining whether this specification has been superseded by a later version or a different specification.

6. These terms and conditions will be interpreted and governed by the laws of the State of Delaware without regard to its conflict of laws and rules. Any party asserting any claims related to this specification irrevocably consents to the personal jurisdiction of the U.S. District Court for the District of Delaware and to any state court located in such district of the State of Delaware and waives any objections to the venue of such court.

Table of Contents

1 INTRODUCTION

This Key Recovery Policy (KRP) is a companion document to the TSCP Certificate Policy (CP).

The TSCP Trust Framework Infrastructure supports escrow and recovery of Public Key Infrastructure (PKI) private keys used for decryption. The Key Recovery System (KRS) provides the personnel, computer system hardware, software, and procedures to store the private keys securely and recover them when appropriate. The KRS is established and operated under the responsibility of the Entity Principal Certification Authority (PCA) as described and defined in the TSCP CP.

Since the TSCP CP supports key escrow, this KRP details the requirements of the KRS and the responsibilities of key personnel required to support secure, timely, and appropriate decryption private key recovery for members' daily business operations. The procedural and technical security controls contained in this KRP help to ensure that the KRS is operational and secure, allowing timely private decryption key recovery.

In this Policy, the term "Entity" refers to a member organization that operates, or contracts for the operation of, a PKI that supports private decryption key escrow and recovery.

1.1 OVERVIEW

The TSCP Trust Framework Infrastructure was developed for the benefit of its members to support member business needs. Identity credentials issued by, or on behalf of, members to employees and other persons and devices allow encryption to protect the confidentiality of the business data and relationships. Since PKI supports encryption using a private key that, absent key escrow, allows only the possessor of the private key to decrypt the data, the policy and requirements in the TSCP CP and this KRP support the escrow and recovery of private decryption keys to ensure that member organizations have timely access to all of their data and communications for their business purposes, and also to support investigative and law enforcement purposes. The security, control, and authentication requirements contained herein provide a basis to ensure that information is only accessed by authorized persons for appropriate purposes.

An Entity offering key recovery services shall develop a Key Recovery Practice Statement (KRPS) describing its procedures and controls which shall meet the requirements of this KRP. The TSCP Policy Management Authority (TPMA) determines whether the member KRPS is in compliance with this KRP.

1.2 IDENTIFICATION

N/A.

1.3 COMMUNITY AND APPLICABILITY

1.3.1 Key Escrow System Roles

- Key Recovery Agent (KRA)
- Key Recovery Official (KRO)
- Requestor
- Subscriber

A KRA is an individual who, using a two-party control procedure with a second KRA, is authorized, as specified in the applicable Key Recovery Practice Statement (KRPS) to interact with the key escrow database in order to copy or "recover" an escrowed key.

A KRO is a local individual who receives requests for escrowed keys, verifies the Requestor's identity and authorization and transmits that information to a KRA who can perform the requested extraction of the escrowed key.

A Requestor is an individual who requests an escrowed key and to whom the extracted key is to be delivered.

A Subscriber is the person or device that is the original holder of the private key.

This KRP applies to the Entity KRSs, and Subscribers whose decryption private keys are escrowed, and to any Organizations serviced by the Entities.

1.3.2 Key Escrow System Components

A KRS consists of the personnel who are responsible for its operation and the recovery of any escrowed keys and the following components:

- The key escrow database, where the escrowed keys are stored;
- KRA workstations, which KRAs use to copy an escrowed key in the key escrow database under two-party control; and
- KRO Workstations, which KROs use to facilitate protected delivery of copies of escrowed keys to the Requestor.

1.4 CONTACT DETAILS

1.4.1 KRA Policy Administration Organization

This Policy shall be administered by the TPMA.

1.4.2 Contact Person

The contact person is: Chair of the TPMA, tpma@tscp.org

TSCP Address: TSCP, 8000 Towers Crescent Drive, Suite 1350, Vienna, VA 22182

1.4.3 Person Performing Policy/Practice Compatibility Analysis

The TPMA shall determine the suitability of any KRPS to this policy.

2 GENERAL PROVISIONS

2.1 OBLIGATIONS

As part of the key escrow process, Subscribers are notified that the private keys associated with their encryption certificates will be escrowed. During delivery of a copy of an escrowed key to an authorized Requestor, the copy shall be protected against disclosure to any party other than the Requestor. The KRPS will describe the method for ensuring that each individual understands and complies with the obligations for any Key Recovery role they execute.

2.1.1 Entity Obligations

An Entity who provides escrowed keys to authorized Requestors under this Policy shall:

- Not escrow keys prior to approval of its KRPS by the TPMA, unless the Entity already has a KRPS approved by a bridge that is cross-certified with the FBCA, or the entity has a DoD-approved KRPS;
- Provide the KRPS to the KRAs and KROs;
- Operate the KRS in accordance with its KRPS and this KRP;

- Shall notify the Subscribers when their private keys have been escrowed preferably as part of the Subscriber agreement provided during the Subscriber registration process; and
- Monitor the KRS, including KRAs and KROs activity, for patterns of potentially anomalous activity as indicators of possible problems in the infrastructure, investigating as appropriate.

2.1.2 KRA Obligations

A KRA who provides escrowed keys to Requestors under the Policy defined in this document shall conform to the stipulations of this document. In particular, the following stipulations apply:

- The KRA shall maintain an approved copy of the KRPS that complies with this KRP.
- The KRA shall provide a KRPS (and any subsequent changes) to the TPMA for a compliance assessment, if not operating under a KRPS already approved by the TPMA.
- The KRA shall operate in accordance with the stipulations and requirements of the approved KRPS.
- The KRA shall protect copies of Subscribers' escrowed keys from unauthorized disclosure.
- The KRA shall release escrowed keys only for properly authenticated and authorized requests from Requestors, as specified in this Policy.
- The KRA shall protect all information, including the KRA's own key(s) that could be used in the recovery of Subscribers' escrowed keys.
- The KRA shall not release information (including Subscriber notification) regarding key recovery requests.
- The KRA shall monitor key recovery requests for each subordinate KRO to identify potentially anomalous activities and shall initiate investigative activities as deemed appropriate.

2.1.3 KRO Obligations

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

- The KRO shall protect copies of escrowed keys from compromise.
- The KRO, as an intermediary for the KRA, shall request escrowed keys only upon receipt of a request from an authorized key recovery Requestor.
- The KRO, as an intermediary for the KRA, shall request an escrowed key only for the purpose for which the request is authorized.
- The KRO shall protect all information, including the KRO's own key(s) that are used as part of the key recovery process.
- The KRO shall represent themselves accurately to all entities when requesting key recovery services.
- The KRO shall not release information (including Subscriber notification) regarding key recovery requests.

2.1.4 Requestor Obligations

A Requestor who initiates key recovery requests as described in this Policy shall comply with the following stipulations:

- Requestors shall protect copies of escrowed keys from compromise.

- Requestors shall request escrowed keys only to recover Subscriber data they are authorized to access.
- Requestors shall use the escrowed key only to recover Subscriber data they are authorized to access.
- Requestors shall represent themselves accurately during any key recovery service.
- If and when the copy of the escrowed key is no longer required for the requested purpose, the Requestor shall dispose of it in accordance with the applicable KRPS.
- Requestors shall acknowledge receipt of the escrowed key and their responsibilities for use, protection, and destruction of the escrowed key.
- Unless the key recovery is for purposes that require that the Subscriber not be made aware of the action, the Requestor shall notify the Subscriber regarding the key recovery request.

2.1.5 Subscriber Obligations

Subscribers shall comply with the following stipulations:

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

2.2 REQUIREMENTS SUPPORTING NON-U.S. GOVERNMENT SUBSCRIBERS

N/A.

2.3 LIABILITY

2.3.1 TSCP Disclaimers of Warranties

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TSCP, INC. DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTIES RELATING TO THE USE OF THIS KRP OR THE RECOVERY OF KEYS BY ENTITIES OPERATING UNDER THIS KRP.

2.3.2 TSCP Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL TSCP, INC. BE LIABLE FOR DAMAGES OF ANY KIND, INCLUDING DIRECT OR INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE, ARISING OUT OF OR RELATING TO THIS KRP OR THE RECOVERY OF KEYS BY ENTITIES OPERATING UNDER THIS KRP.

2.3.3 Entity Warranties and Limitations on Warranties

The Entity shall warrant that their procedures are implemented in accordance with this KRP and their KRPS, that all key escrow and recovery activities are done in accordance with this KRP and the Entity KRPS, and that the KRS, KRAs and KROs comply with the requirements and stipulations of this KRP and the procedures outlined in the Entity KRPS.

2.3.4 Entity Disclaimers of Warranty

Except for the warranties included in Section 2.3.3, an Entity may disclaim any and all warranties or obligations of any type concerning the accuracy of information provided by a Subscriber or Requestor, provided the procedures stated in the Entity KRPS were followed and the procedures were in compliance with the TSCP CP, Entity CP, and this KRP. An Entity may disclaim any and all liability arising solely from to negligence and/or lack of reasonable care by Subscribers and Requestors. An Entity may disclaim any liability for loss due to improper use of a recovered key, if the key was recovered in accordance with this KRP and the Entity KRPS.

2.3.5 Entity Limitation of Liability

The Entity shall identify in its CPS limits of losses due to operations that do not comply with the procedures defined in its CPS and its KRPS, which limits shall comply with the liability provisions contained in Section 9 of the TSCP CP. Any failure to operate in accordance with the stipulations and requirements of this Policy in the PCA's operation of the KRS shall be resolved in a manner that is consistent with the liability limitations in Section 9.8 of the TSCP CP.

2.4 FINANCIAL RESPONSIBILITY AND FIDUCIARY RELATIONSHIP

Neither the Entity nor its agents (e.g., KRA, KRO, etc.) is required to assume financial responsibility for improper use of a recovered key by Subscriber or by Requestor.

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

2.5 INTERPRETATION AND ENFORCEMENT

2.5.1 Governing Law

This KRP shall be governed by the laws of the State of Delaware in the United States of America, irrespective of other choice of law provisions in Memoranda of Agreement (MOA) and without a requirement to establish nexus in the state of Delaware.

2.5.2 Severability of Provisions, Survival, Merger, and Notice

Should it be determined by a court of competent jurisdiction that one section or set of sections of this KRP is incorrect or invalid, the other sections shall remain in effect to allow the KRP to be updated. Requirements for updating this Policy are described in Section 7. Responsibilities, requirements, and privileges of this Policy are merged to the new Policy upon release of the newer Policy.

2.5.3 Conflict Provision

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

2.5.4 Dispute Resolution Procedures

The TPMA shall decide any disputes over the interpretation or applicability of this KRP.

2.6 FEES

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

2.7 PUBLICATION AND REPOSITORY

N/A.

2.8 COMPLIANCE AUDIT

2.8.1 Frequency of Entity Compliance Audit

At a minimum, compliance audits of the KRS shall be conducted annually. Audits shall include audits of all KRS operations and components and may be conducted in conjunction with the audit of the other elements of the PKI.

In order to ensure the integrity of the KRS, in the event that a KRO or KRA is relieved of that responsibility for failure to comply with this KRP, the Entity PMA shall direct a special compliance audit to determine whether any key recovery activities of the removed KRO or KRA may have been improper or may have affected the integrity of the KRS. Appropriate corrective actions shall be taken.

2.8.2 Identity/Qualifications of Compliance Auditor

The auditor shall demonstrate competence in the field of compliance audits of PKI and Key Recovery systems, and shall be thoroughly familiar with the KRP and Entity KRPS. The compliance auditor shall maintain the expertise to perform PKI and Key Recovery compliance audits by performing such audits on a regular basis.

2.8.3 Compliance Auditor's Relationship to Audited Entity

The compliance auditor shall be associated with a private firm that is independent from the Entity to be audited. To ensure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the Entity PKI or KRS.

2.8.4 Topics Covered by Compliance Audit

All the topics identified in this KRP document will be covered by the compliance audit. The purpose of a compliance audit shall be to verify that the KRS, including all personnel and components, are operating under the requisite procedures and with required controls in place. The audit shall also include a compliance analysis assessment that the applicable KRPS adequately addresses the requirements of the KRP.

2.8.5 Actions Taken Based on Findings of Compliance Audit

When the compliance auditor finds a discrepancy in KRS, KRA or KRO operations and the stipulations of the applicable KRPS, the following actions shall occur:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the Entity and the Entity PMA of the discrepancy;
- The Entity CA shall propose a remedy, including expected time for completion, to the Entity PMA; and
- The Subscriber's Organization shall be notified of audit results that may be relevant or pertain to the Organization.

The Entity PMA shall determine the appropriate remedy, up to and including revocation or non-recognition of the audited component's certificate. Upon correction of the deficiency, the Entity PMA may reinstate the audited component. TSCP shall be provided a summary of audit findings and the Entity PMA's remedy with any supporting reasoning.

2.9 CONFIDENTIALITY

2.9.1 Types of Information to be Protected

To verify a Requestor's identity and authorization for escrowed keys, the KRA or KRO is authorized to request authentication or authorization evidence from the Requestor that may be considered personal, confidential, or sensitive information. Any such information shall be explicitly identified in the KRPS. All such information stored at the KRA's or KRO's location shall be handled as sensitive and access to the information shall be restricted to those with an official need for access related to performance of their functions.

2.9.2 Information Release Circumstances

A KRA will not disclose, or allow to be disclosed, escrowed key or escrowed key-related information to any third party unless authorized by this Policy; required by law, government rule, or regulation; or by order of a court of competent jurisdiction. The identity of the Requestor of escrowed key or escrowed key-related information shall be authenticated per Section 3 below.

3 IDENTIFICATION AND AUTHENTICATION

Identification and Authentication verifies that Requestors are who they say they are and are authorized to access the requested escrowed key. The user's authenticated identity shall be the basis for determining the user's access permissions and providing user accountability.

3.1 IDENTITY AUTHENTICATION

Identity authentication shall be commensurate with the PKI certificate assurance level. It shall comprise the activities specified by the TSCP CP for authentication of individual identity during initial registration for at least the specified PKI certificate assurance level or be based on digital signatures that can be verified using public key certificates for at least the specified PKI certificate assurance level.

3.2 REQUESTOR

The requirements for authentication and authorization when the Requestor is the Subscriber are addressed in Section 3.3, Subscriber.

3.2.1 Requestor Authentication

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

3.2.2 Requestor Authorization Verification

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

3.3 SUBSCRIBER

3.3.1 Subscriber Authentication

The Subscriber shall establish his or her identity to the KRA or the KRO, as an intermediary for the KRA, as specified in Section 3.1. If the authentication is not based on digital signatures that can be verified

using the public key certificates for at least the given PKI certificate assurance level, the KRA or KRO shall personally verify the identity of the Subscriber prior to initiating the key recovery request. The authentication mechanism shall be detailed in the KRPS.

For automated recovery, the Subscriber must be authenticated to the key escrow system using a valid public key certificate. The authentication mechanism shall be detailed in the KRPS. The assurance level of the authentication certificate shall be equal to or greater than that of the certificate associated with the escrowed key.

3.3.2 Subscriber Authorization Verification

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

3.4 KRA AND KRO AUTHENTICATION

3.4.1 KRA

The KRA shall authenticate identity to the key escrow database using a digital signature. The PKI certificate assurance level associated with the certificate shall be at least the PKI certificate assurance level required to access the key escrow database.

3.4.2 KRO

The KRO shall authenticate identity to the KRA using a digital signature. The PKI certificate assurance level associated with the certificate shall be at least the PKI certificate assurance level required to access the key escrow database.

4 OPERATIONAL REQUIREMENTS

4.1 ESCROWED KEY RECOVERY REQUESTS

4.1.1 Who Can Request Recovery of Escrowed Keys

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

4.1.2 Requirements for Requesting Escrowed Key Recovery

Subscribers may act as a Requestor to use electronic means to request their escrowed keys from the KRS Database if they possess a valid PKI issued authentication certificate of appropriate assurance level. The Subscriber shall digitally sign the electronic request using the Entity PKI issued authentication certificate of assurance level equal to or greater than that of the escrowed key.

Subscribers may submit requests on their own behalf directly to the KRA. If the KRPS does not allow this procedure, the Subscriber must fill out a physical or electronic request, as specified in the applicable KRPS; sign it by hand or digitally, if they have a PKI certificate with a TSCP CP assurance level greater than or equal to that of the escrowed key; and submit the request to the KRO.

If the public key certificate for the requested escrowed key asserts one or more permission or access approval requirements, the Requestor must provide, and the KRO verify, evidence that the Requestor possesses permission or access approvals asserted in the certificate.

In all instances where the Requestor is neither the Subscriber nor the Subscriber's Supervisor or manager, the Requestor must fill out a physical or electronic request, as specified in the applicable

KRPS; sign it by hand or digitally, if they have a PKI certificate of equivalent or higher class than the escrowed key; and submit it to the KRO.

Key recovery operations that require release of escrowed keys outside the jurisdiction of the control of the Entity shall be bound, by legal and policy means, to the key protection and other provisions of the TSCP CP and KRP.

4.2 PROTECTION OF ESCROWED KEYS

Escrowed keys shall be stored in a protected key escrow database.

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

4.2.1 Key Recovery through the KRA

The KRA shall provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access shall require the actions of at least two KRAs. All copies of escrowed keys shall be protected continuously by two-person control procedures during recovery and delivery to the authenticated and authorized Requestor. The protection mechanisms shall be specified in the KRPS. Split key or password procedures are considered adequate two-person control.

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

4.2.2 Automated Recovery when the Requestor is the Subscriber

A current Subscriber's escrowed keys may be provided directly to that Subscriber without imposition of two-person control requirements. The Key Escrow Database shall only provide escrowed keys to current Subscribers without two-person control upon:

- Verifying that the authenticated identity of the Requestor is the same as the Subscriber associated with the escrowed keys being requested. The KRPS shall describe how the identity of the authenticated Subscriber is verified and ensured to be same as that associated with the Subscriber private key;
- Attempting to notify the Subscriber of all attempts (successful or unsuccessful) to recover the Subscriber's escrowed keys that are made by entities claiming to be the Subscriber. If the Key Escrow Database does not have information (e.g., an e-mail address) necessary to notify the Subscriber of a key recovery request, then the Key Escrow Database 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 strength equal to or greater than that provided by the escrowed keys.

4.3 CERTIFICATE ISSUANCE

Certificates are issued by the CA. Neither KRAs nor KROs issue certificates.

4.4 CERTIFICATE ACCEPTANCE

N/A**.**

4.5 SECURITY AUDIT PROCEDURES

Security auditing capabilities of the underlying key escrow database and KRA workstation equipment operating system shall be enabled during installation.

4.5.1 Types of Events Recorded

The key escrow database equipment shall be configured to record, at a minimum, the following event types:

- Key escrow database application access (e.g., logon/logoff);
- Messages received from any source requesting key escrow database actions (i.e., escrowed key retrieval requests);
- Actions taken in response to requests for key escrow database actions;
- Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying key escrow database cryptographic modules;
- Receipt of keys for escrow and posting of these keys to the key escrow database;
- Retrieval, packaging (e.g., keying or other cryptologic manipulations), securing, and shipping copies of escrowed keys;
- Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and
- Any known or suspected violations of physical security, suspected or known attempts to attack the key escrow database equipment via network attacks, equipment failures, power outages, network failures, or violations of this KRP.

KRA workstation equipment shall be configured to record the following event types:

- The KRA equipment shall record server installation, access, and modification (to include changes in configuration files, security profiles, administrator privileges).

The KRA shall record the following events for audit:

- KRA equipment access (e.g., room access);
- Messages received from any source requesting KRA actions (e.g., key recovery requests, second party key recovery approval requests);
- Messages sent to any destination authorizing key recovery actions (e.g., first party escrowed key retrieval authorizations, second party key recovery approvals);
- Access to KRA databases; and
- Any use of the KRA signing key.

The KRO shall record the following information for audit:

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

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

- The type of event;
- The time the event occurred;

- For messages from KRAs, KROs, or other entities requesting key escrow database actions, the message source, destination and contents;
- For requested key escrow database 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 non-electronic, shall be retained in accordance with the requirements of Section 4.5.3, and made available during compliance audits.

4.5.2 Audit Log Processing

If automated audit logs are required pursuant to Section 4.5.1, the applicable audit logs shall be processed as required to prevent audit overflow, audit overwrite, or stoppage of system operation.

4.5.3 Audit Log Retention Period

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

4.5.4 Audit Log Protection

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

Online audit logs may only be deleted after they have been backed up to archive media. Only authorized security auditors and system administrators are allowed to delete these logs. Before deleting any online audit log, the security auditor or systems administrator must verify that the audit log data has been successfully backed up to archive media. No one is allowed to delete or destroy audit data recorded on archive media.

4.5.5 Audit Log Back Up Procedures

Security audit processing personnel shall use the procedures described in the KRPS to perform regular back up of the audit log.

4.5.6 Audit Log Collection System (Internal vs. External)

The security audit process shall be internal to the key escrow database and KRA workstation. Security audit processes shall be invoked at component system startup and cease only at component system shutdown. The security audit process shall run automatically without human intervention.

Should it become apparent that an automated security audit system has failed, the affected key escrow system component shall cease all operations until a security audit capability can be restored.

4.5.7 Subscriber Audit Notification

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

4.5.8 Vulnerability Assessments

The KRA, and other supporting personnel, shall watch for attempts to violate the integrity of the KRS, including the equipment, physical location, and by or through personnel. The security audit data shall be

reviewed by the security auditor regularly (at least once a week) for events such as repeated failed actions, requests for escrowed keys, attempted access of escrowed keys, unauthenticated requests, or other suspicious or unusual activity. Security auditors shall also check for continuity of the security audit data.

4.6 RECORDS ARCHIVAL

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

- Validation of the identification of the recipient of a copy of the Subscriber's escrowed key.
- Establishment of the circumstances under which the escrowed key copy was provided.
- Verification of authorization and need of Requestor to obtain the escrowed key copy.

4.6.1 Types of Information Recorded

The following information shall be archived by the Entity:

- KRP and KRPS
- Security audit data
- Escrowed keys
- Agreements with Subscribers, and/or Subscribers' Organizations
- Audit log

The KRP shall be archived by the TPMA.

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

4.6.2 Archive Retention Period

The key escrow system archive retention period shall meet the requirements specified in the TSCP CP Section 5.5.2 for the PKI certificate assurance level supported. Escrowed keys shall be maintained within the key escrow database for a minimum of one year after the expiration of the key.

4.6.3 Archive Protection

No one shall be able to modify or delete archive data unless it has been backed up to archive media. The KRPS shall specify the roles authorized to back up archive data.

No one shall be able to delete or destroy data recorded on archive media. Transfer of medium shall not invalidate digital signatures applied to the recorded data. Release of sensitive archive information will be as described in Section 2.9.2.

Archived security audit data shall be protected as specified in Section 4.5.4. Archived escrowed keys shall be protected as specified in Section 4.2.

Archive media shall be stored in a separate, safe, secure storage facility, as described by the applicable KRPS. Prior to storage, the records shall be labeled with the Entity CA's distinguished name, the date, and the classification.

4.6.4 Archive Backup Procedures

No stipulation.

4.6.5 Requirements for Time-Stamping of Records

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

4.6.6 Archive Collection System

Archive data shall be collected in any expedient manner.

4.6.7 Procedures to Obtain and Verify Archive Information

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

4.7 KRA KEY CHANGEOVER

The KRA's individual and/or role-based certificates shall be re-keyed every three (3) years in accordance with the TSCP CP Section 4.7 and the Entity CPS for the PKI certificate assurance level of the associated certificates.

4.8 KEY ESCROW DATABASE COMPROMISE AND DISASTER RECOVERY

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

4.8.1 Key Escrow Database Compromise

In the event that the key escrow database is compromised or is suspected to be compromised, recovery procedures are required to return it to a secure state. If a compromise of the key escrow database is suspected, the Entity PMA shall be notified. The Entity PMA shall determine the extent of the compromise and direct the appropriate action.

4.8.2 Disaster Recovery

The key escrow database shall reestablish a secure environment. The procedures for reestablishing the secure environment after any disaster must be detailed in the Entity KRPS.

4.8.3 KRA Key Compromise

If the KRA's certificate is revoked due to compromise, there is a potential for some Subscriber escrowed keys to have been exposed during the recovery process. Security auditor or system administrator personnel 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 the TSCP CP Section 4.9.3, and the Subscriber notified of the revocation.

4.8.4 KRA Key Revocation

If the KRA's 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 key pair from the appropriate CA. The CA shall report the old KRA key as revoked using the CA's revocation notification policy. The CA shall follow its policy for certificate issuance for the new KRA public key certificate.

4.9 KRA TERMINATION

Upon KRA termination, the Entity PMA shall take possession of all KRA archive records. The KRPS shall document the process for transferring KRA archive records to the Entity PMA.

4.10 KRO TERMINATION

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

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

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

Physical controls for the key escrow database shall be equivalent to those specified in the TSCP CP Section 5.1 for CA and CMA equipment. Physical controls for KRA workstations shall be equivalent to those specified in the TSCP CP Section 5.1.

Key escrow database and KRA workstation physical controls shall be described in the Entity KRPS.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

The primary trusted roles defined by this Policy are the KRA and the KRO. (See the TSCP CP Section 5.2.1 for details on what constitutes a trusted role.)

5.2.1.1 Key Recovery Agent

All KRAs that operate under this Policy are subject to the stipulations of this Policy and of the TPMA-approved Entity KRPS under which it operates. The KRA's role and the corresponding procedures shall be defined in the Entity KRPS. A KRA's responsibilities are to ensure that the following functions occur according to the stipulations of this Policy:

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

5.2.1.2 Key Recovery Official

All KROs that operate under this Policy are subject to the stipulations of this Policy and of the PMA-approved Entity KRPS under which it operates. The KRO's role and corresponding procedures shall be defined in the Entity KRPS. A KRO's responsibilities are to ensure that the following functions occur according to the stipulations of this Policy:

- Verify Requestor identity and authorization as stated by this Policy;
- 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 Entity KRPS.

The KRO role is highly dependent on public key infrastructure implementations and local requirements. The responsibilities and controls for KROs shall be explicitly described in the Entity KRPS.

5.2.1.3 Other Trusted Roles

The Entity KRPS shall define trusted facility roles (e.g., system administrators, security officers, operators, compliance auditors) to which shall be allocated responsibilities that ensure the proper, safe, and secure operation of the key escrow database equipment and procedures. The responsible persons who are identified in these trusted roles must be named and made available during compliance audits. The responsibilities include:

- Initial configuration of the system, including installation of applications, initial setup of new accounts, configuration of initial host and network interface;
- Performance of compliance audit;
- Creation of devices to support recovery from catastrophic system loss;
- Performance of system backups, software upgrades and system recovery;
- Perform secure storage and distribution of the backups and upgrades to an off-site location;
- Change of the host or network interface configuration;
- Assignment of security privileges and access controls to key escrow system personnel;
- Archival of the security audit log and other data as described in Sections 4.3 and 4.6 of this document; and
- Review of the security audit log.

5.2.2 Separation of Roles

Under no circumstances shall a KRO perform trusted facility responsibilities for a key escrow database facility. Under no circumstances shall a KRA or KRO perform their own compliance or security audit function. Where separation among roles can be established, a KRA shall not perform trusted facility responsibilities for a key escrow database facility.

Separation of responsibilities among trusted facility roles shall be described in the Entity KRPS.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

Persons selected for KRA or trusted facility roles shall meet the requirements specified in the TSCP CP Section 5.3.1 for CMA roles. Persons selected for the KRO role shall meet the requirements specified in the TSCP CP Section 5.3.1 for trusted roles other than CMAs.

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

All personnel involved in key escrow database operation shall be appropriately trained. Topics shall include:

- Operation of the key escrow database software and hardware;
- Operational and security procedures;

- Stipulations of this Policy; and
- Local guidance.

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

5.3.4 Retraining Frequency and Requirements

Significant changes to key escrow database operation shall require implementation of a training (awareness) plan that includes any retraining required for KRA or KRO personnel. The execution of such a plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions shall commence against personnel who violate this Policy.

5.3.7 Contracting Personnel Requirements

Contractor personnel requirements shall be as specified in the TSCP CP Section 5.3.7.

5.3.8 Documentation Supplied to Personnel

Documentation requirements shall be as specified in the TSCP CP Section 5.3.8. At a minimum, the documentation provided to personnel shall include applicable portions of the TSCP CP, the Entity CPS, the TSCP KRP, and the Entity KRPS.

6 TECHNICAL SECURITY CONTROLS

6.1 PROTOCOL SECURITY

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

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

6.1.1 Key Escrow Database Protocol Security

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

6.1.2 KRA - KRO Protocol Security

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

6.1.3 Escrowed Key Distribution Security

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

6.2 KRA AND KRO PRIVATE KEYAND STORAGE KEY PROTECTION

6.2.1 Standards for Cryptographic Modules

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [the current version of Federal Information Processing Standard (FIPS)]. The TPMA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the TPMA. Cryptographic modules shall be validated to the FIPS level identified in this section, or validated, certified, or verified via one of the standards published by the TPMA.

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

The key escrow database and servers shall use hardware cryptographic modules that meet at least the criteria specified for FIPS 140 Level 3.

6.2.2 Private and Storage Key Control

The private components of KRA and KRO signature key pairs and encryption key pairs shall be under single person control. The key escrow database storage key shall be under two-person control. The names of the individuals used for two-person control shall be maintained on a list that shall be made available for compliance audits.

Storage procedures and mechanisms for the hardware cryptographic module associated with the key escrow database encryption key pair shall require two-person control. When not in use, the cryptographic module shall be stored in a secured container, such as a safe, in a facility that meets the physical security requirements of Section 5.1 of this policy.

6.2.3 Storage Key Backup

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

6.2.4 Private Key Generation and Transport

Private components of key escrow database and server, KRA, and KRO encryption key pairs shall be generated by, and in, a cryptographic module. In the event that the private component of a key escrow database, KRA, or KRO encryption key pair is to be transported from one cryptographic module to another, it shall be encrypted during transport. The assurance level of the transport encryption shall be commensurate with the PKI certificate assurance level of the key escrow database, but shall be at least at the assurance level of Medium Hardware, and the strength of the cryptographic algorithm shall meet or exceed the strength of the key being transported.

6.2.5 Method of Activating Private Key

Activation of private keys shall be in accordance with the TSCP CP section 6.2.8.

6.2.6 Method of Deactivating Private Key

The private component of the key escrow database, KRA, or KRO encryption key pair shall be deactivated as specified by the TSCP CP section 6.2.9.

6.2.7 Method of Deactivating Storage Key

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

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

6.3 PRIVATE KEY ACTIVATION DATA

Generation, change, and management of private key activation data shall be in accordance with the TSCP CP Section 6.4.

6.4 COMPUTER SECURITY CONTROLS

6.4.1 Key Escrow Database

The key escrow database shall be based on trusted operating systems that are designed, implemented, and operated using the following security features:

- Individual identification and authentication;
- Secure audit;
- Residual information protection;
- Discretionary access controls;
- Operating system self-protection;
- Process isolation; and

Meet Common Criteria (CC) Evaluation Assurance Level (EAL) 3 assurance requirements. The Entity PMA may determine that other comparable validation, certification, or verification standards are sufficient.

When key escrow databases are hosted on evaluated platforms in support of computer security assurance requirements, then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system that received the evaluation rating.

6.4.2 KRA Workstation

KRA workstation equipment shall use operating systems that:

- Require authenticated logins;
- Provide discretionary access control; and
- Provide a security audit capability.

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

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

6.4.3 KRO Equipment

Reasonable care shall be taken to prevent malicious software from being loaded on equipment used by the KRO. Only applications required to perform the organization's mission shall be loaded on the computer, and all such software shall be obtained from sources authorized by local policy. Data on the equipment shall be scanned for malicious code on first use and periodically afterward. The equipment shall be located on internal networks behind boundary/perimeter network defenses level. KRO-related activities shall be performed only on systems approved for use by the Entity CA.

6.4.4 Anomaly Detection

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

6.5 LIFE CYCLE TECHNICAL CONTROLS

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

6.6 NETWORK SECURITY CONTROLS

Network access to the key escrow database and server shall be protected as specified in the TSCP CP Section 6.7 for CA equipment.

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

6.7 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are stated in section 6.2.1 of this KRP.

7 POLICY ADMINISTRATION

7.1 POLICY CHANGE PROCEDURES

This Policy shall be maintained under the specification change procedures identified in the TSCP CP Section 9.12.

7.2 PUBLICATION AND NOTIFICATION POLICIES

This policy shall be published and notification performed as specified in the TSCP CP Section 9.12.

7.3 POLICY APPROVAL PROCEDURES

This policy shall be approved based on the procedures specified in the TSCP CP Section 9.12.

8 LIST OF ACRONYMS

CA Certification Authority

CC Common Criteria

CM Certificate Management

CMA Certificate Management Authority

CP Certificate Policy

CPS Certification Practice Statement

DN Distinguished Name or Directory Name

EAL Evaluation Assurance Level

FIPS Federal Information Processing Standard

KMI Key Management Infrastructure

KRA Key Recovery Agent

KRO Key Recovery Official

KRP Key Recovery Policy

KRPS Key Recovery Practice Statement

NSM Network Security Manager

PKI Public Key Infrastructure

PMA Policy Management Authority

PMO Program Management Office

TBD To Be Defined

9 GLOSSARY OF TERMS

Encryption Certificate: A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing, protecting, and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.

Key Escrow: The retention of the private component of the key pair associated with a Subscriber's encryption certificate to support key recovery.

Key Recovery: Production of a copy of an escrowed key and delivery of that key to an authorized Requestor.

Key Recovery Agent (KRA): An individual authorized to interface with the key escrow database in conjunction with one or more other key recovery agents) to cause the key escrow database to carry out key recovery requests, as specified by the Key Recovery Policy.

KRA Workstation: The workstation from which the Key Recovery Agent interfaces with the key escrow database system.

Key Escrow Database: The function, system, or subsystem that maintains the key escrow repository and responds to key registration and key recovery requests from one or more Key Recovery Agents, as specified by the Key Recovery Policy.

Key Recovery Official (KRO): An individual authorized to authenticate and submit key recovery requests to the Key Recovery Agent on behalf of Requestors, as specified by the Key Recovery Policy.

Key Recovery Policy (KRP): Specifies the conditions under which key recovery information must be created and conditions under which and to whom escrowed keys may be released; it also indicates who are allowable Key Recovery Agent(s) and Key Recovery Officials and how or where escrowed keys must be maintained.

Key Recovery Practice Statement (KRPS): A Key Recovery Practice Statement is a statement of the practices, procedures, and mechanisms that a key escrow system employs in registering and recovering escrowed keys.

Requestor: An individual who is authorized, under the Key Recovery Policy, to request recovery of a Subscriber's escrowed key. Subscribers can always request recovery of their own keys.

Policy Management Authority: Body established to oversee the creation and update of Certificate and Key Recovery Policies, review Certification and Key Recovery Practice Statements, review the results of CA and Key Recovery audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate and Key Recovery policies.

Public Key Infrastructure: Framework established to issue, maintain, and revoke public key certificates.

Security auditor: Local automation security personnel.

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.

Storage Key: The cryptographic key that is used to protect the escrowed keys in the key escrow database.

Subscriber: "An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate." [17] **Current Subscribers** possess valid 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 policy, two-person control is a process that requires two independent, authorized parties to consent to activities involving extraction and restoration of private key data.

10 REFERENCES

a) *Security Requirements for Cryptographic Modules (*FIPS140-2), June 2001, http://csrc.nist.gov/publications/index.html

b) Minimum Security Requirements for Multi-User Operating Systems, CSL, NISTIR 5153, NISTIR

c) 5153, March 1993

d) *Common Criteria for Information Technology Security Evaluation,* Common Criteria Implementation Board, CCIB-98- 026, Version 2.1, August 1999

e) TSCP X.509 Certificate Policy for The TSCP Bridge Certification Authority (TBCA), TSCP CP, Version 1.0, March 24, 2014

f) Requirements for Key Recovery Products: Report of the Technical Advisory Committee (TAC) to Develop a FIPS for the Federal Key Management Infrastructure, Final Report, November 1998