IdenTrust
Key Recovery Practices Statement
for the
US Department of Defense
External Certification Authority (ECA) Program

Version 1.1
October 27, 2017

This is confidential and proprietary "eyes only" information of IdenTrust. Do not copy, reproduce, forward or otherwise disseminate without prior approval. Disseminate only to persons with a "Need to Know."

TABLE OF CONTENTS

1. INTRODUCTION 2
1.1 OVERVIEW 2
1.2 IDENTIFICATION 2
1.3 COMMUNITY AND APPLICABILITY 3
1.3.1 Key Recovery System Roles 3
1.3.2 Key Recovery System ("KRS") Components 4
1.3.3 Applicability 5
1.4 CONTACT DETAILS 5
1.4.1 Key Recovery Policy Administration Organization 5
1.4.2 Contact Office 5
1.4.3 Person Performing Policy/Practice Compatibility Analysis 6
2 GENERAL PROVISIONS 7
2.1 OBLIGATIONS 7
2.1.1 IdenTrust Obligations 7
2.1.2 KRA Obligations 7
2.1.3 KRO Obligations 8
2.1.4 Requestor Obligations 9
2.1.5 Subscriber Obligations 10
2.1.6 Subscribing Organization Obligations 10
2.2 LIABILITY 10
2.2.1 Warranties and Limitations on Warranties 10
2.2.2 Damages Covered and Disclaimer 11
2.2.3 Loss Limitations 11
2.2.4 Other Exclusions 11
2.2.5 US Federal Government Liability 11
2.3 FINANCIAL RESPONSIBILITY 12
2.3.1 Indemnification by Relying Parties and Subscribers 12
2.3.2 Fiduciary Relationships 12
2.3.3 Administrative Processes 12
2.4 INTERPRETATION AND ENFORCEMENT 12
2.4.1 Governing Law 12
2.4.2 Severability of Provisions, Survival, Merger, and Notice 12
2.4.3 Conflict Provision 12
2.4.4 Dispute Resolution Procedures 13
2.5 FEES 14
2.6 PUBLICATION AND REPOSITORY 14
2.7 COMPLIANCE AUDIT 14
2.7.1 Frequency of Entity Compliance Audit 14
2.7.2 Identity/Qualifications of Compliance Auditor 14
2.7.3 Compliance Auditor's Relationship to Audited Party 14

2.7.4 Topics Covered by Compliance Audit *15*
2.7.5 Actions Taken as a Result of Deficiency *15*
2.7.6 Communication of Results *15*
2.8 CONFIDENTIALITY 15
2.8.1 Type of Information to be Protected *15*
2.8.2 Information Release Circumstances *15*
3 IDENTIFICATION AND AUTHENTICATION 17
3.1 IDENTITY AUTHENTICATION 17
3.2 REQUESTOR 17
3.2.1 Requestor Authentication *17*
3.2.2 Requestor Authorization Confirmation *17*
3.3 SUBSCRIBER 18
3.3.1 Subscriber Authentication *18*
3.3.2 Subscriber Authorization Confirmation *19*
3.4 KRA AND KRO AUTHENTICATION 19
3.4.1 KRA *19*
3.4.2 KRO *20*
4 OPERATIONAL REQUIREMENTS 21
4.1 ESCROWED KEY RECOVERY REQUESTS 21
4.1.1 Who Can Request Recovery of Escrowed Keys *21*
4.1.2 Requirements for Requesting Escrowed Key Recovery *21*
4.2 PROTECTION OF ESCROWED KEYS 22
4.2.1 Key Recovery through KRA *23*
4.2.2 Automated Self-Recovery *24*
4.3 CERTIFICATE ISSUANCE 24
4.4 CERTIFICATE ACCEPTANCE 24
4.5 SECURITY AUDIT PROCEDURES 24
4.5.1 Types of events recorded *25*
4.5.2 Audit Log Processing *26*
4.5.3 Audit Log Retention Period *27*
4.5.4 Audit Log Protection *27*
4.5.5 Audit log back up procedures *27*
4.5.6 Audit Log Collection System (Internal vs. External) *27*
4.5.7 Subscriber Audit Notification *27*
4.5.8 Vulnerability assessments *27*
4.6 RECORDS ARCHIVAL 28
4.6.1 Types of information recorded *28*
4.6.2 Archive Retention Period *28*
4.6.3 Archive Protection *28*
4.6.4 Archive backup procedures *29*
4.6.5 Requirements for time-stamping of records *29*

4.6.6 Archive Collection System (Internal vs. External) *29*
4.6.7 Procedures to obtain and verify archive information *29*
4.7 KRA, KRO AND ADMINISTRATIVE KEY CHANGEOVER 29
4.8 KED COMPROMISE AND DISASTER RECOVERY 29
4.8.1 KED Compromise *29*
4.8.2 Disaster Recovery *30*
4.8.3 KRA or KRO Key Compromise *30*
4.8.4 KRA or KRO Certificate Revocation *30*
4.8.5 Administrative Private Key Compromise *31*
4.9 KRA TERMINATION 31
5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS 32
5.1 PHYSICAL CONTROLS 32
5.1.1 IdenTrust's Cryptographic Token and KRA Workstations Site *32*
5.1.2 Physical Access *32*
5.1.3 Power and Air Conditioning *33*
5.1.4 Water Exposures *33*
5.1.5 Fire Prevention and Protection *33*
5.1.6 Media Storage *33*
5.1.7 Waste Disposal *33*
5.1.8 Off-site Back-up *34*
5.2 PROCEDURAL CONTROLS 34
5.2.1 Trusted Roles *34*
5.2.2 Separation of Roles *36*
5.3 PERSONNEL CONTROLS 36
5.3.1 Background, qualifications, experience, and clearance requirements *36*
5.3.2 Background check procedures *36*
5.3.3 Training requirements *37*
5.3.4 Retraining frequency and requirements *38*
5.3.5 Job rotation frequency and sequence *38*
5.3.6 Sanctions for unauthorized actions *38*
5.3.7 Contracting personnel requirements *38*
5.3.8 Documentation supplied to personnel *38*
6 TECHNICAL SECURITY CONTROLS 40
6.1 PROTOCOL SECURITY 40
6.1.1 KED Protocol Security *40*
6.1.2 KRA - KRO Protocol Security *40*
6.1.3 Escrowed Key Distribution Security *41*
6.2 KED, KRA AND KRO PRIVATE KEY PROTECTION 42
6.2.1 Standards for Cryptographic Modules *42*
6.2.2 Private Key Control *42*
6.2.3 KED Key Backup *42*

6.2.4 Private Key Generation and Transport *42*
6.2.5 Method of Activating Private Key *43*
6.2.6 Method of Deactivating Private Key *43*
6.2.7 Method of Deactivating Storage Key *43*
6.3 PRIVATE KEY ACTIVATION DATA 43
6.4 COMPUTER SECURITY CONTROLS 43
6.4.1 KED *43*
6.4.2 KRA and KRO Workstation *44*
6.4.3 Anomaly Detection *44*
6.5 LIFE CYCLE TECHNICAL CONTROLS 45
6.6 NETWORK SECURITY CONTROLS 45
6.7 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 45
7 POLICY ADMINISTRATION 46
7.1 POLICY CHANGE PROCEDURES 46
7.2 PUBLICATION AND NOTIFICATION POLICIES 46
7.3 POLICY APPROVAL PROCEDURES 46
APPENDIX A: ACRONYMS AND ABBREVIATIONS 47
APPENDIX B: GLOSSARY 48
APPENDIX C: LETTER AGREEMENT: KEY RECOVERY REQUEST 49
APPENDIX D: KEY RECOVERY OFFICER ADDENDUM TO SUBSCRIBING ORGANIZATION AUTHORIZATION AGREEMENT 51
APPENDIX E: SUBSCRIBER AGREEMENT 53
APPENDIX F: KEY RECOVERY AGENT AUTHORIZATION AGREEMENT 54
APPENDIX G: ECA TECHNICAL SPECIFICATION DOCUMENT 55
APPENDIX H: REFERENCES 56

Revision History

Revision	Date	Summary of Changes/Comments
1.0	July 1, 2015	Original
1.1	October 27, 2017	Updated to current branding standards

Key Recovery Practices Statement for the
US Department of Defense External Certification Authority (ECA) Program

1. Introduction

IdenTrust Services, LLC (“IdenTrust”) operates as an External Certification Authority (“ECA”) in support of the United States (US) Government ECA program. One aspect of IdenTrust’s ECA program is the escrow and recovery of private keys associated with Encryption Certificates (“Decryption Keys”). This Key Recovery Practice Statement ("KRPS") is a statement of the policies, practices and procedures used by IdenTrust while acting as an External Certification Authority ("ECA").

This KRPS governs the escrow, recovery and management of the Decryption Keys for all assurance levels from the IdenTrust ECA CPS. This KRPS describes the procedural and technical security controls that IdenTrust uses to operate the Key Escrow and recovery system fulfilling the requirements defined in the Key Recovery Policy for External Certification Authorities Version 1.0 (06/04/2003), as published by the US Department of Defense (“DOD”) and downloadable from http://iase.disa.mil/pki-pke/Pages/policies.aspx (the "ECA KRP").

1.1 Overview

IdenTrust’s Key Recovery capability is based on the principle that all encryption activities using the Certificates are performed on behalf of the person holding the Certificate (i.e., Subscriber, see Appendix B: Glossary) or the Organization that authorized the issuance of Encryption Certificates (i.e., Subscribing Organization, see Appendix B: Glossary). Therefore, the Subscriber or the Subscribing Organization has the right to identify the persons authorized to recover the Decryption Key in order to maintain the continuity of business operations. In addition, there may be a need to access the information for investigative and law enforcement purposes. This KRPS implements the ECA KRP to ensure that encrypted data is recovered expeditiously when appropriate, while protecting the rights of both Subscribers and their Subscribing Organizations.

This KRPS describes the security and authentication requirements that IdenTrust uses to implement Key Recovery operations. IdenTrust’s Key Recovery System (“KRS”) exists as a module of its Certificate management system. This system consists of hardware, software, administrative private keys, staff and procedures to issue digital Certificates and store Decryption Keys securely and recover them when appropriate. Section 1.3.2 describes the KRS and its components.

Subscribers and other authorized employees within the Subscribing Organization can make requests to recover Decryption Keys through their Organization’s internal Key Recovery Official (“KRO”). Subscribing Organization’s KROs, Subscribers, and other authorized employees in Organizations without internal KROs make Key Recovery requests to IdenTrust’s Key Recovery Agents (“KRAs”). In specific situations, Subscribers and authorized employees may also request Key Recovery to an IdenTrust KRO who forwards the request to a KRA. Two KRAs—acting together under principles of separation of duties and multi-party control—are required to recover keys from the Key Escrow Database (“KED”). Section 1.3.1.1 describes the role and responsibilities of KRAs. Section 1.3.1.2 describers the role and responsibilities of KROs. Section 1.3.2.1 describes the KED. Section 4.2.1 and 4.2.2 explain the recovery processes for automated self-recovery and intermediated recovery.

1.2 Identification

Certificates issued pursuant to IdenTrust ECA CPS and this KRPS contain at least one of the Certificate Policy OIDs listed below. All policy OIDs from the ECA CP section 1.2 are included in this list. Those OIDs indicate that the IdenTrust ECA CPS, this KRPS, and the ECA CP apply in relation to the Certificate; see also section 1.4.3 in the IdenTrust ECA CPS.

This KRPS applies to the Decryption Keys associated with Certificates issued by IdenTrust with the following object identifiers:

id-eca-medium ID::= {id-eca-policies 1}
id-eca-medium-hardware ID::= {id-eca-policies 2}
id-eca-medium-token ID::= {id-eca-policies 3}
id-eca-medium-sha256::= {id-eca-policies 4}
id-eca-medium-token-sha256::= {id-eca-policies 5}
id-eca-medium-hardware-pivi::= {id-eca-policies 6}
id-eca-cardauth-pivi::= = {id-eca-policies 7}
id-eca-contentsigning-pivi::= {id-eca-policies 8}
id-eca-medium-device sha256::= {id-eca-policies 9}

where id-eca-policies represents the prefix:

{joint-iso-ccitt(2)country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1) eca-policies(12)}.

where id-eca-policies represents the prefix:

{joint-iso-ccitt(2)country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1) eca-policies(12)}.

1.3 Community and Applicability

This section describes some of the roles and systems involved in the Key Recovery process.

1.3.1 Key Recovery System Roles

1.3.1.1 Key Recovery Agent ("KRA")

KRA responsibilities are carried out by IdenTrust's employees in the following Trusted Roles: the Registration Authority Operator ("RA Operator") or Help Desk Representative position. These roles are explained in the IdenTrust ECA CPS sections 1.3.1.3, 5.2.1.2, and 5.2.1.4.4. Responsibilities specific to this KRPS are explained in section 5.2.1.1. KRAs are provided with an IdenTrust ECA Medium Hardware assurance Certificate in order to comply with some of their responsibilities.

Due to the highly sensitive nature of the access to the KED, IdenTrust has placed controls on these individuals' access to the KED. Physical controls on KRA access to the KED are explained in section 5.1.2 of this KRPS.

For simplicity, from this point on, this document will use the term KRA to refer to both the RA Operator and Help Desk Representatives. If there is any difference that needs to be clarified, the specific name and task will be specified.

1.3.1.2 Key Recovery Official ("KRO")

IdenTrust may use the services of Key Recovery Officials ("KRO") in performing identity and authority confirmation tasks. KROs authenticate the Requestor. IdenTrust recognizes two types of KROs: KROs within the Subscribing Organization and KROs within IdenTrust.

KROs from Subscribing Organizations are only able to participate in the recovery of keys of Subscribers from their Organization. A Subscribing Organization's Trusted Correspondents, described in section 1.3.2.1 of the IdenTrust ECA CPS, will perform the KRO obligations outlined in section 2.1.3. In order to comply with some of their obligations, KROs obtain an IdenTrust ECA Medium Token or Hardware assurance Certificate which is documented in an internal secured list maintained and managed by KRAs (Processes associated with Key Recovery are performed using a security of commensurate assurance level —with the understanding that Key Recovery of Medium Hardware Assurance Certificates may only be approved by

KROs who hold Medium Hardware Assurance Certificates after manual review of the Certificate and the entry for that KRO in the list by a KRA as described in section 3.4.2.)

IdenTrust will allow its employees in Trusted Roles to act as KROs solely for the purpose of performing in-person identity confirmation of Requestors, and all KRO requirements shall apply to such IdenTrust employees when they are acting in the KRO role.

For simplicity, from this point on, this document will use the term KRO to refer to the Trusted Correspondent of a Subscribing Organization authorized to be a KRO and clarify when reference to a KRO refers to an IdenTrust employee acting in the role of KRO.

1.3.1.3 Requestor

A Requestor is the person who requests the recovery of a Decryption Key. A Requestor is the Subscriber or a Third Party who is authorized by the Subscribing Organization (or by law and legal process) to request recovery of a Subscriber's escrowed key. Any individual who can demonstrate association with (and key-recovery authorization by) the Subscribing Organization, or who has legal authority pursuant to an order issued by a court (e.g. court order, search warrant) of competent jurisdiction to obtain a recovered key, is considered a Requestor.

Internal Requestor: An Internal Requestor is an individual explicitly authorized by the Subscribing Organization to request the recovery of Decryption Keys. The Subscribing Organization will provide the individual with the means, information and knowledge on how to request Key Recovery on behalf of the Organization so that the KRPS requirements regarding access and release of sensitive information are met.

External Requestor: An External Requestor is an investigator or someone outside the Subscribing Organization who serves a court order, subpoena, or search warrant to obtain the Decryption Key of a Subscriber. An External Requestor must work with an Internal Requestor, unless the court order, subpoena or search warrant is served directly upon IdenTrust.

IdenTrust and Subscribing Organizations appoint authorized personnel (e.g., KRAs and KROs) to implement the practices in this KRPS and meet policies on the release of sensitive information.

1.3.1.4 Subscriber

The Subscriber is the person or device that holds a private key that corresponds to a public key listed in an Encryption Certificate.

1.3.2 Key Recovery System ("KRS") Components

The KRS consists of the collection of systems used to hold and protect the escrowed Decryption Keys as well as the infrastructure to facilitate request and delivery of the recovered private keys. The KRS consists of a Key Escrow Database ("KED"), KRA and KRO workstations, and the administrative cryptographic token containing an administrative private key.

1.3.2.1 Key Escrow Database ("KED")

The KED is a table located within IdenTrust's main customer information database that holds all IdenTrust-generated Decryption Key Pairs for escrow. This KED is accessed only by the Certification Authority ("CA") applications that create the Decryption Keys and the KRA Workstation that extracts them during recovery. Every new Decryption Key created for ECA Subscribers by the CA system is encrypted with an administrative public key separately by the CA system prior to its storage in the KED. The CA system uses the administrative public key corresponding to the administrative private key that will be used to decrypt the Decryption Key at the time of Key Recovery.

Subscriber Decryption Keys remain encrypted in the KED until a Key Recovery request is performed. Escrowed Decryption Keys are kept stored in encrypted form as records in the database. Only designated IdenTrust employees, who comply with

ECA Trusted Role requirements, perform KED installation, maintenance and backups. Such system administrators do not have access to the administrative private key needed to decrypt the escrowed Decryption Keys.

Note that the KED does not have capability to decrypt the escrowed keys; that function is performed at the KRA Workstation.

For the purpose of this KRPS, the KED security requirements from the ECA KRP apply to the IdenTrust KRA Workstation, including those for no remote login.

1.3.2.2 KRA Workstation

The KRA Workstation provides functionality to extract encrypted Decryption Keys from the KED, decrypt them, and reconstitute the original Encryption Certificate chain. In this regard, the KRA Workstation performs the KED Key Recovery functions and therefore has the highest degree of security controls.

Other functions of the KRA Workstation include the insertion of recovered material into cryptographic tokens or other storage media (e.g., CD-ROM) for delivery to Requestors. KRA Workstations have no communication functionality outside of the services needed to connect to the KED. Remote connectivity to the KRA Workstation is not permitted or allowed by the architecture. In other words, e-mail and other remote messaging services are disabled. Access to the KRA Workstation is restricted through physical access controls (i.e. locked door with two-person, two-factor controls), system access controls (i.e. via user ID and password). In order to decrypt escrowed material, the cryptographic token hosting the administrative private key needs to be connected to the KRA Workstation and the token needs to be activated. Access to and activation of the cryptographic token in the KRA workstation room can only be performed under two-person control as described in Section 5.1.2.

Only KRAs, security officers, and system administrators have access to the KRA Workstation in order to perform updates and other administrative functions to the workstation itself. The KRA Workstation room is under two-person, two-factor as each function (e.g., updates or key recovery processes) requires two KRAs or a KRA and a security officer in order to perform.

1.3.2.3 KRO Workstation

KROs, or in limited circumstances trusted IdenTrust employees acting in the KRO role, perform their functions from a desktop computer that is used to securely communicate with the KRA. (Consistent with section 1.3.6.1 of the ECA CP, these systems do not have automated interfaces with Certificate Management Authority (CMA) functions.) The KRO workstation will be loaded with standard commercially available applications (i.e., Word processor, e-mail client, and spreadsheet), and in some particular cases, with IdenTrust proprietary clients that facilitate secure communications with the IdenTrust KRA. In either case, software applications will be configured in accordance with the parameters provided by IdenTrust to ensure appropriate security. An example is the email client configuration to require the use of specific signing and encryption algorithms.

1.3.3 Applicability

This KRPS applies to IdenTrust, ECA Subscribers, ECA Subscribing Organizations and Requestors.

1.4 Contact Details

1.4.1 Key Recovery Policy Administration Organization

The EPMA administers the ECA KRP, and IdenTrust administers this KRPS.

1.4.2 Contact Office

The contact office for IdenTrust is:

IdenTrust Services, LLC
ATTN: Policy Management Authority
5225 Wiley Post Way Suite 450
Salt Lake City, UT 84116
ecaservices@identrust.com (888) 248-4447

1.4.3 Person Performing Policy/Practice Compatibility Analysis

The compatibility analysis will be performed by the ECA Policy Management Authority, who will ensure that this KRPS is in compliance with the ECA KRP. The EPMA's address is:

ECA Policy Management Authority
9800 Savage Road, Suite 6718
Ft. George G. Meade, MD 20755-6718

2 GENERAL PROVISIONS

2.1 Obligations

As part of the Certificate issuance/Key Escrow process, Subscribers are notified that the private keys associated with their Encryption Certificates will be escrowed.

During delivery, recovered private keys are protected against disclosure to any party except the Requestor.

Individual Subscribers and Subscribing Organizations execute Subscriber Agreements acknowledging an understanding and a willingness to comply with their respective obligations under this KRPS.

KRAs and KROs will be provided copies of this KRPS.

KROs will be required to execute an agreement acknowledging their understanding and willingness to comply with their obligations under this KRPS.

Requestors are required to execute a letter agreement (attached as Appendix C) acknowledging their Key Recovery obligations as discussed below in section 2.1.4.

2.1.1 IdenTrust Obligations

In acting as an ECA, IdenTrust will conform to the stipulations of the ECA KRP document. In particular, the following stipulations apply:

- IdenTrust will obtain the EPMA's approval and compatibility determination for this KRPS.
- IdenTrust will provide a copy of this KRPS to each of its KRAs and any KROs, which contains only the level of information necessary for the KRA and KRO to perform their responsibilities and does not contain sensitive system information.
- IdenTrust will provide a copy of the ECA CP and the public version of IdenTrust's ECA CPS to each of its KRAs and any KROs.
- IdenTrust will operate its KRS in accordance with the stipulations of the ECA KRP and this KRPS.
- IdenTrust will automatically notify Subscribers that their Decryption Keys are being escrowed in the KED. This is accomplished via a "click-wrap" agreement that appears on a Subscriber's screen during the Certificate request process. A copy of this agreement is also provided to the Subscriber as part of the request process.
- IdenTrust will monitor KRA and KRO activity for patterns of potentially anomalous activity as indicators of possible problems in the infrastructure and initiate inquiries or investigations as appropriate. IdenTrust's risk management function will collect and analyze, both manually and electronically, information on time, average volume, and origin of requests to discover pattern changes that point to anomalous behavior.

2.1.2 KRA Obligations

Any KRA who performs a Key Recovery is instructed by IdenTrust to comply with the stipulations of the ECA KRP and this KRPS. In particular, the following stipulations apply as outlined in the Key Recovery Agent Authorization Agreement attached as Appendix F:

- KRAs will maintain a copy of the ECA KRP and the KRPS.
- KRAs will operate in accordance with the stipulations of the ECA KRP and this KRPS.

- KRAs will protect Subscribers' recovered Decryption Keys from unauthorized disclosure including; the encrypted files and associated Decryption Keys, RSA PKCS#12 files, P12 passwords, cryptographic tokens and passwords they obtain and send securely to Requestors.
- KRAs will maintain and observe multi-person control over the administrative private key used to recover Subscriber's escrowed keys.
- KRAs may rely upon KROs for confirmation of the identity and authority of the Requestor. KRAs will also authenticate the identity of the Requestor when the Requestor's digital signature is available, i.e., when the Requestor makes an electronic request that is digitally signed. In addition, KRAs may request additional information or confirmation from KROs if deemed necessary.
- KRAs will release Subscriber's escrowed keys only for properly authenticated and authorized requests. Requestor's identity and authority confirmation may be delegated to KROs. KRAs will authenticate KROs using the Medium Hardware or Medium Token assurance Certificates issued to KROs by IdenTrust (Certificate used for the authentication must be of the same or higher assurance level than that of the Encryption Certificate recovery request).
- KRAs will validate the authorization of the KRO. This will be done by ensuring that the KRO is authorized for the Subscriber whose key has been requested to be recovered. KRAs will assemble a list of authorized KROs that will be used as the basis for verification of authorization.
- KRAs will protect all information regarding all occurrences of Key Recovery. KRAs will communicate knowledge of a recovery process only to the KRO and Requestor involved in the Key Recovery. KRAs will not communicate any information concerning a Key Recovery to the Subscriber except when the Subscriber is the Requestor.
- KRAs will consider a KRO's departure from the practices outlined in this KRPS potentially anomalous and will inform the IdenTrust's risk management function of this situation. Examples of anomalies include but are not limited to: submittal of incomplete, unsigned or unconfirmed Key Recovery requests; significant changes in average request patterns; and, inconsistencies or mistakes in the delivery of recovered keys.

Any KRA who fails to comply with this KRPS will be subject to sanctions under IdenTrust's existing personnel discipline procedures listed within the IdenTrust Employee Security Handbook (maintained and available through the Security or Human Resources department by request).

2.1.3 KRO Obligations

A KRO initiates a Key Recovery request for a Requestor. The Requestor is generally a Third Party, but the Subscriber may seek the assistance of a KRO to recover the Subscriber's Decryption Key.

- In any case and for any reason that a KRO gains access to a Subscriber's recovered keys, the KRO is obligated to submit them to the Requestor without attempting to access or use them.
- The KRO will request the Subscriber's keys only upon receipt of a request from an authorized Requestor. The KRO, as an intermediary between the Requestor and the KRA, will confirm the identity of any Requestor seeking a Key Recovery. KROs shall follow the requirements for validating the identity of Requestors as defined in section 3.2.3 of IdenTrust's CPS. In the case of persons other than the Subscriber seeking a Key Recovery, the KRO will ensure that the Requestor has the authority and legitimate purpose to request the Subscriber's key.
- The KRO, as an intermediary for the KRA, will confirm the authorization for the request, consulting with legal counsel when appropriate.
- The KRO will protect all information including the KRO's own key(s) that could be used to request recovery of the Subscriber's Decryption Key.

- The KRO will protect all information regarding all occurrences of Key Recovery. The KRO will communicate knowledge of any recovery process only to the Requestor or the KRA. The KRO will communicate to the KRA(s) when the Requestor is not the Subscriber and will not communicate any information concerning a Key Recovery to the Subscriber except when the Subscriber is the Requestor.
- The KRO will accurately represent himself or herself to all entities when performing Key Recovery services.
- The KRO will keep records of all recovery requests and dispositions. The audit records will not contain Subscribers' keys in any form: plaintext, split, encrypted, etc.

With respect to any KRO who is an employee of IdenTrust, such a KRO who fails to comply with this KRPS will be subject to sanctions under IdenTrust's existing personnel discipline procedures listed within the IdenTrust Employee Security Handbook (maintained and available through the Security or Human Resources department by request). With respect to any KRO who is not an employee of IdenTrust (e.g. a Trusted Correspondent of a Subscribing Organization), where IdenTrust is aware of such a KRO failing to comply with this KRPS, that KRO shall no longer be regarded by IdenTrust as having KRO status.

2.1.4 Requestor Obligations

Prior to receiving a recovered key, the Requestor must formally acknowledge and agree to the obligations described here and as contained in Appendix C: Letter Agreement: Key Recovery Request. IdenTrust accomplishes this through a written agreement with the Requestor, either by requiring a written signature on a paper document or a digital signature, with an IdenTrust-issued ECA credential of the same or higher assurance level as the key being recovered, on an agreement made available to the Requestor online.

- A Requestor will protect the Subscriber's recovered key(s) from compromise.
- A Requestor will use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their own personal keys (if any) and the recovered Subscriber's keys. When the Requestor is not the Subscriber, the Requestor will destroy all copies of the Subscriber's Decryption Key when no longer required (i.e., when the Requestor has recovered the data that was encrypted--assuming that maintaining custody of the Decryption Key is not necessary for legal, evidentiary purposes).
- A Requestor will request a Subscriber's escrowed key(s) only to recover Subscriber's data that the Requestor is authorized to access.
- A Requestor will accurately represent himself or herself to all entities during any Key Recovery service. When the request is made to a KRO, the Requestor will 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. IdenTrust may choose to rely on a digitally signed and encrypted e-mail using an IdenTrust-issued ECA credential of the same or higher assurance level as the key being recovered to verify the Requestor's identity. The Requestor will also provide information to aid in the confirmation of his or her authority to request the Key Recovery.
- A Requestor, who is not a Subscriber, will protect information concerning each Key Recovery operation. The Requestor will communicate information concerning the recovery to the Subscriber when appropriate as determined by the reason for the recovery. The decision to notify the Subscriber or not, will be based on the law, and Subscriber Organization's policies and procedures for Third Party information access. Included with the Key Recovery request, the Requestor will provide copies of such laws, organizational policies, and procedures to the KRA and/or the KRO, if applicable. In the event that the Requestor notifies the Subscriber of a Key Recovery, the Requestor will advise the Subscriber to determine whether or not the recovery circumstances warrant revoking the associated public key Certificate.

- As a condition prior to receiving a recovered key, a Requestor will sign an acknowledgement of agreement to follow the Subscribing Organization's policies and legal limitations relating to protection and release of the recovered key. The acknowledgement of agreement letter, attached as Exhibit C, includes a statement substantively containing the following:

  I, <Requestor's Name>, declare under penalty of perjury punishable under the provisions 18 U.S.C. § 1621 that I have a legitimate and official need to recover the private decryption key of the Subscriber identified below in order to obtain (recover) the encrypted data that I have authorization to access. I certify that I have accurately identified myself to [the KRO], and truthfully described all reasons for which I require access to data protected by the recovered key, identified below. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to [the KRO] when no longer needed. I understand that I am bound by Subscribing Organization's policies, applicable laws and Federal regulations concerning disclosure of key recovery to the Subscriber and the protection of the recovered key and any data recovered using the key.

2.1.5 Subscriber Obligations

Subscribers will comply with the following stipulations as outlined in the Subscriber Agreement attached as Appendix E:

- Subscribers will 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 will determine whether revocation of the public key Certificate associated with the recovered key is necessary. If necessary the Subscriber will request the revocation.

2.1.6 Subscribing Organization Obligations

Subscribing Organizations will ensure that:

- KROs operate in accordance with the applicable sections of the ECA KRP, the public version of IdenTrust's CPS and the portions of this KRPS that are made available to KROs;
- IdenTrust is notified about an employee's or contractor's nomination to or removal from the KRO position or separation from employment;
- Appropriate disciplinary procedures are in place to address any breach by a KRO of the KRO duties contained herein; and
- Audit procedures related to the KRO workstation (see section 2.7.5) are fulfilled and an individual within the Organization is designated in order to receive audit reports.

2.2 Liability

2.2.1 Warranties and Limitations on Warranties

Subject to the disclaimers and limitations of liability stated herein, IdenTrust warrants that its procedures are implemented in accordance with this KRPS, the ECA CP and the ECA KRP and that all key escrow and recovery are done in accordance with this KRPS and in accordance with the ECA KRP.

IdenTrust warrants that KRAs will operate, and IdenTrust requires Subscribing Organizations to warrant that KROs will operate, in accordance with the applicable sections of the ECA CP, the public version of IdenTrust's ECA CPS, the ECA KRP, and this KRPS.

2.2.2 Damages Covered and Disclaimer

Except to the extent that the ECA CP, the IdenTrust ECA CPS, the ECA KRP, this KRPS, or other applicable law require otherwise, IdenTrust disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.

IDENTRUST SHALL HAVE NO LIABILITY FOR LOSS DUE TO USE OF A RECOVERED DECRYPTION KEY, UNLESS THE LOSS IS PROVEN TO BE A DIRECT RESULT OF A BREACH BY IDENTRUST AND IDENTRUST'S AGENTS OF THIS KRPS OR A PROXIMATE RESULT OF THE NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT OF IDENTRUST AND IDENTRUST'S AGENTS.

IN NO EVENT SHALL IDENTRUST BE LIABLE FOR ITS ACTS OR THE ACTIONS OF ITS AGENTS ANY CONSEQUENTIAL, INDIRECT, REMOTE, EXEMPLARY, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR BUSINESS INTERRUPTION, LOSS OF PROFITS, REVENUES, SAVINGS, OPPORTUNITIES OR DATA, OR INJURY TO CUSTOMER RELATIONSHIPS, REGARDLESS OF THE FORM OF ACTION AND REGARDLESS OF WHETHER IDENTRUST WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IDENTRUST SHALL INCUR NO LIABILITY FOR ITS ACTIONS OR THE ACTIONS OF ITS AGENTS IF THEY ARE PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMIT TO PERFORM, OR IS REQUIRED TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER, THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY PARTY OTHER THAN THEM OR ANY ACT OF GOD, EMERGENCY CONDITION OR WAR OR OTHER CIRCUMSTANCE BEYOND THEIR CONTROL.

2.2.3 Loss Limitations

IdenTrust's entire liability, in law or in equity, for losses due to its operations at variance with its procedures defined in this KRPS shall not exceed either of the following limits:

- One thousand U.S. dollars (USD $1,000) for all recoverable losses sustained by each person, whether natural or legal, as a result of a single transaction involving the reliance upon or use of a Certificate.
- One million U.S. dollars (USD $1,000,000) maximum total liability for all Recoverable Losses sustained by all persons as a result of a single incident. In cases where multiple parties suffer recoverable losses caused by the same Incident, (i.e. the aggregate of all transactions arising out of the reliance upon or use of a Certificate).

2.2.4 Other Exclusions

No stipulation.

2.2.5 US Federal Government Liability

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

As an ECA acting pursuant to the ECA KRP, IdenTrust has no claim for loss against the EPMA.

Subscribers and Requestors shall have no claim against the US Federal Government arising from erroneous Key Escrow and Key Recovery operations by IdenTrust.

2.3 Financial Responsibility

2.3.1 Indemnification by Relying Parties and Subscribers

IdenTrust's contracts with Subscribing Organizations and/or Individual Subscribers may provide for indemnification of IdenTrust and its directors, officers, employees for loss or damage arising from or pertaining to wrongful or grossly negligent acts or omissions of the Subscriber, the Subscribing Organization, or by any Requestor associated with the Subscribing Organization.

IdenTrust, its KRAs and KROs assume no financial responsibility for improper use of a recovered key by a Subscriber, Subscribing Organization or by a Requestor.

2.3.2 Fiduciary Relationships

Escrow and recovery of Decryption Keys in accordance with this KRPS does not make IdenTrust (nor any KRA or KRO) an agent, fiduciary, trustee, or other representative of Subscribers or Requestors.

2.3.3 Administrative Processes

IdenTrust maintains records related to its financial responsibilities for accounting or auditing which are available to IdenTrust's auditors in accordance with section 2.7.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

The laws of the United States of America will govern the enforceability, construction, interpretation, and validity of this KRPS relative to the ECA KRP and the Memorandum of Agreement between the EPMA and IdenTrust. With respect to US Government Subscribers or US Government Relying Parties, this KRPS and its interpretation shall be governed by the Contracts Disputes Act of 1978, as amended (41 US.C. § 601 et seq.). In all other cases, the law of the State of Utah shall govern the enforceability, construction, interpretation, and validity of this KRPS, without reference to its rules regarding conflicts of laws.

2.4.2 Severability of Provisions, Survival, Merger, and Notice

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

2.4.3 Conflict Provision

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

2.4.4 Dispute Resolution Procedures

As provided in the ECA KRP, the EPMA will decide any disputes over the interpretation or applicability of the KRP. Other disputes arising from the operation of the Key Recovery service shall be resolved as provided in this section.

If a Subscriber, Relying Party or Subscribing Organization of a Certificate covered by the IdenTrust ECA CPS is an individual employed by or acting on behalf of the United States Government, a dispute arising in connection with Key Recovery for such Certificate shall be resolved under applicable Federal law. If the United States Government has purchased a service or a Certificate provided under the IdenTrust ECA CPS, a dispute arising in connection with such service or Certificate, and asserted on behalf of any such entity shall be resolved under the Contract Disputes Act of 1978, as amended (41 U.S.C. § 601 et. seq.).

Where the Subscriber, Relying Party or Subscribing Organization is not the United States Government or a Government employee, the dispute resolution procedures specified in this section shall provide the sole remedy for any claim against IdenTrust for any loss sustained by such party, whether that loss is claimed to arise from recovery of a Decryption Key, from breach of a contract, from a failure to perform according to the ECA KRP and/or this KRPS, or from any other act or omission. No Relying Party, Subscriber, or Subscribing Organization shall require IdenTrust to respond to any attempt to seek recourse through any other means.

2.4.4.1 Claims and Claim Determinations

Before making a claim to recover a loss for which IdenTrust may be responsible, a Subscriber, Relying Party, or Subscribing Organization that is not the United States Government or a Government employee (the "Claimant") shall make a thorough investigation. IdenTrust will cooperate reasonably in that investigation. The Claimant will then present to the IdenTrust Appeal Officer reasonable documented proof:

- That the Claimant has suffered a recoverable loss as a result of a transaction;
- Of the amount and extent of the recoverable loss claimed; and
- Of the causal linkage between the alleged transaction and the recoverable loss claimed, itemized as necessary.

Upon the occurrence of any loss arising out of a transaction, the Claimant shall file notice and all required proof of the claim using a procedure accessed through IdenTrust's web site no later than one year after the date of discovery of the facts out of which the claim arose. Notice of the claim must be given on a form downloadable from https://secure.identrust.com/certificates/policy/eca/index.html Instructions for completion and submission of the claim form also appear on that web page.

On receipt of a claim form, IdenTrust may determine to pay the claim or deny it. IdenTrust may also pay the claim in an amount less than the amount claimed if IdenTrust determines that the loss calculations exceed the amount that IdenTrust is obligated to pay. IdenTrust will notify the Claimant of its determination within 30 days of receipt of the claim form.

If the Claimant is not satisfied with IdenTrust's determination of the claim, the Claimant may seek judicial relief as provided in the next section.

2.4.4.2 Judicial Review

A Relying Party, Subscriber, or Subscribing Organization who is not the U.S. Government may contest the determination of the claim by IdenTrust under section 2.4.4.1 by filing suit as provided herein within one year after IdenTrust's determination of the claim.

Except for suits and disputes in which the United States Government is a party, the courts of the State of Utah have exclusive subject matter jurisdiction over all suits and any other disputes arising out of or based on this KRPS, including suits for judicial review of claims decided according to section 2.4.4.

2.5 Fees

Fees for performing Key Recovery services may be published or established contractually by IdenTrust. IdenTrust makes Key Recovery information available to authorized US Federal, State, and Local government Requestors, including authorized law enforcement personnel with legitimate authority or as otherwise required by law.

2.6 Publication and Repository

Not Applicable.

2.7 Compliance audit

2.7.1 Frequency of Entity Compliance Audit

IdenTrust's external auditor conducts audits of all KRS components that are within IdenTrust's control as part of its annual WebTrust for Certification Authorities audit, including operation of the KED, KRO and KRA functions.

In cases that the KRO workstation is hosted in the Subscribing Organization facilities, IdenTrust will rely on the Organization's auditing function to perform the audit when requested by IdenTrust annually. IdenTrust will provide guidance on the steps to follow and a pre-defined report that the Organization will complete and submit back to IdenTrust.

In the event that an IdenTrust KRO or KRA is relieved of that responsibility due to failure to comply with this KRPS, then at the EPMA's request, IdenTrust will direct that an ad hoc internal auditor conduct a special internal audit and prepare a report to the EPMA. The purpose of the audit will be to determine whether any Key Recovery activities of the removed KRO or KRA may have been improper or may have affected the integrity of the KRS.

When the KRO is external to IdenTrust, IdenTrust will request the special audit and will provide guidance and support to the Organization's auditor. Audit reports will be collected by IdenTrust and made available during the annual audit.

2.7.2 Identity/Qualifications of Compliance Auditor

Internal auditors will meet the following qualifications:

- Be familiarized with this KRPS, the KRP, the CPS and IdenTrust's certification and key escrow operations;
- Have previous knowledge of and/or experience with auditing practices; and
- Have expertise in information security, cryptography and PKI.

External auditors of IdenTrust's Key Recovery System will meet the foregoing qualifications in addition to those identified in the IdenTrust ECA CPS, Section 8.2.

2.7.3 Compliance Auditor's Relationship to Audited Party

External auditors of IdenTrust's Key Recovery System will meet the criteria identified in the IdenTrust ECA CPS, Section 8.3.

For special audits within IdenTrust, the ad hoc internal auditor will be selected ensuring he or she does not belong or report to the Operations organizational branch of IdenTrust.

For the annual and special audits within the Subscribing Organization, IdenTrust will require that the Subscribing Organization successfully proves independence of the auditor from the department that performs the KRO-related functions.

2.7.4 Topics Covered by Compliance Audit

All the topics identified in this KRPS will be covered by the compliance audit. The purpose of the annual external compliance audit will be to verify that the KED, and KRA/KRO workstations comply with the procedures and controls explained in this KRPS and IdenTrust's ECA CPS.

2.7.5 Actions Taken as a Result of Deficiency

For annual compliance audits there is no stipulation beyond this KRPS.

On conclusion of the annual audit, the auditor sends a report, which includes a KRS section, of the outcome of the audit to IdenTrust and the EPMA. That report notes discrepancies between IdenTrust's operations and the requirements of this KRPS and the ECA KRP. IdenTrust will notify the EPMA immediately of each such discrepancy, propose a remedy, and note the time necessary for completion of that remedy. Based on a mutually agreed plan, IdenTrust will proceed to implement the remedy.

For KRO workstations hosted in the Subscribing Organization facility, the Organization's auditor will perform the audit. In case of discrepancies the Organization will inform and collaborate with IdenTrust in addressing the concerns. An expected time for completion will be mutually agreed on, but shall not exceed thirty (30) calendar days.

In the event of a special directed compliance audit following removal of a KRA or KRO, IdenTrust, and when necessary the Subscribing Organization, will cooperate with the EPMA and proceed as necessary based on the special compliance audit results and on a mutually agreed timeframe.

2.7.6 Communication of Results

For a KRS compliance audit, the compliance auditor will include a KRS specific section in the submitted report of the compliance audit to IdenTrust, which will be forwarded to the EPMA.

For a KRO compliance audit, in addition to informing IdenTrust, the Subscribing Organization's auditor will provide the report to the Subscribing Organization's designated representative.

2.8 Confidentiality

2.8.1 Type of Information to be Protected

The KED, KRA, KRO and Requestor will protect personal or sensitive information used to identify and authenticate participants in the recovery process. Such information may include a Social Security Number ("SSN"), identification credential serial numbers, and affiliation with investigative agencies when specified by the Requestor as sensitive. Protections are described in sections 4, 5, and 6 of this KRPS.

When Key Recovery is requested as part of an investigation, search warrant, subpoena, or court order, information concerning the request will also be protected.

2.8.2 Information Release Circumstances

A KRA will not disclose or allow to be disclosed the recovered Decryption Key or key-related information to any Third Party unless authorized by the ECA KRP and this KRPS; required by the law, government rule, or regulation; by the Subscribing Organization's policy; or by search warrant, subpoena or order of a court of competent jurisdiction such as a civilian or military court. When Key Recovery is requested as part of a Subscribing Organization or law enforcement investigation, the KRS will also protect all information concerning the request. The identity of the Requestor of an escrowed key will be

authenticated per Section 3. External Requestors must furnish a court order, search warrant, or judicially issued subpoena and demonstrate that the Subscribing Organization's current practices for releasing other types of personnel information to law enforcement officials and other External Requestors have been followed.

3 IDENTIFICATION AND AUTHENTICATION

Identification and Authentication is the process used by IdenTrust to Confirm the identity of Key Recovery Requestors and that these individuals are authorized to access an escrowed key.

3.1 Identity Authentication

KROs and KRAs will perform identity authentication that is commensurate with the assurance level of the IdenTrust-issued Certificate associated with the key being recovered. Identification and Authentication will be performed as specified by IdenTrust in Section 3.2.3 of the CPS for authentication of individual identity during initial registration or will be based on digital signatures that can be verified using public key Certificates for at least the specified IdenTrust ECA Certificate assurance level.

3.2 Requestor

This section addresses the requirements for authentication and authorization of Third Party Requestor, i.e., a Requestor other than the Subscriber. The requirements for authentication and authorization, when the Requestor is the Subscriber, are addressed in Section 3.3.

3.2.1 Requestor Authentication

In order for a Key Recovery request to be accepted, the Requestor will establish his or her identity to the KRA, or the KRO as an intermediary for the KRA, through in-person identity proofing or through verification of their digital signature.

KROs may Confirm the identity of the Requestor by in-person identification prior to processing a Key Recovery request. This method can be used if the Requestor does not have access to their digital signature as described in section 3.2.2. Should in-person identification be used, KRAs and KROs will be acting as Registrars as discussed in IdenTrust's ECA CPS 3.2.3.1.1.

The Requestor may use a digital signature to authenticate his or her identity based on meeting the criteria in the ECA CPS section 3.2.3.2. To do this IdenTrust's KRA or a KRO may validate the Requestor's digital signature by reference to an IdenTrust-issued ECA Certificate. The confirmation requires the digital signature be created by a Valid Certificate with an assurance level equal to or higher than the Decryption Key requested to be recovered, which is verified manually by comparing the Certificate Policy OIDs in the Requestor's Certificate with the assurance level of the Certificate being requested.

3.2.2 Requestor Authorization Confirmation

The KRA or the KRO as an intermediary for the KRA will Confirm the authorization of the Requestor in consultation with Subscribing Organization's management and/or legal counsel as appropriate.

Internal Requestor by Organization's KRO

The Subscribing Organization's KRO will establish a Requestor's authority by verifying a supervisory relationship to the Subscriber. Authority is also established if the Requestor is an Organization's officer, a member of the personnel office, a security officer, or a PKI Point of Contact of the Subscribing Organization.

In cases where there may be ambiguity due to multiple Requestors with the same name, the KRO will use the email address and name in the Certificate associated with the digital signature to verify that the Requestor is the person with the authority being verified.

Internal Requestor by IdenTrust KRO

Authority of an Internal Requestor to request Key Recovery may be pre-established through IdenTrust's process for enrolling Subscribing Organizations. The Subscriber Organization may submit an attachment to the Subscribing Organization Authorization Agreement indicating authorization of one or more identifiable individuals or organizational roles or job titles (e.g., CIO, Security Officer, HR Director, etc.) to request Key Recovery. Requests submitted by authorized Internal Requestors may be authenticated by digital signature with reference to an IdenTrust-issued Certificate, or if the authorization is role-based, by confirming with the Subscribing Organization's Human Resource function that the authenticated Requestor is the person in said job position.

In cases where there may be ambiguity due to multiple Requestors with the same name, the KRO will use the email address and name in the Certificate associated with the digital signature to verify that the Requestor is the person with the authority being verified.

External Requestor by Organization's KRO

A Subscribing Organization's internal procedures for responding to a subpoena or search warrant that requests data encrypted with a Decryption Key shall dictate the procedures used to request Key Recovery. The Subscribing Organization's KRO, in collaboration with the Subscribing Organization's management and/or its legal department, shall determine the permission of the Requestor to request Key Recovery.

External Requestor by IdenTrust's KRO

In the case in which a subpoena, court order or search warrant is served directly upon IdenTrust, IdenTrust will forward such writ to its legal counsel. The legal counsel will determine whether it is legally valid and enforceable against IdenTrust and will determine whom to respond. In the event such counsel determines that the writ is valid and enforceable, he or she will forward the recovery request to the KRA with instructions to deliver the Decryption Key to the party to whom he or she has determined a response is due.

3.3 Subscriber

3.3.1 Subscriber Authentication

The Subscriber will establish his or her identity to the KRA, or the KRO as an intermediary for the KRA, in person or via digital signature authentication. Authentication will be commensurate to the assurance level of the key being requested and will be in accordance with the processes described in the IdenTrust ECA CPS.

IdenTrust's KRA or the Organization's KRO can authenticate Subscribers in person or using digital signatures. IdenTrust's KROs may only perform in-person authentication, since a Subscriber performing self-authentication with a digital Certificate would communicate directly through electronic means with an IdenTrust KRA.

KROs will personally Confirm the identity of the Subscriber prior to initiating the Key Recovery request using practices specified in section 3.2.3.1 of IdenTrust's ECA CPS. KRAs and KROs will be acting as Registrars as defined in IdenTrust's ECA CPS 3.2.3.1.1.

The Subscriber may also use a digital signature to authenticate his or her identity. An IdenTrust KRA or Subscribing Organization KRO may accept a digital signature created with the Signature Key corresponding to the Subscriber's IdenTrust-issued ECA Certificate of at least the same assurance of the Decryption Key to be recovered. The confirmation process will follow the practices outlined in section 3.2.3.2 of IdenTrust's ECA CPS.

3.3.2 Subscriber Authorization Confirmation

IdenTrust will deem a Subscriber "authorized" to request a Key Recovery when:

- Authentication has been established satisfactorily based on section 3.3.1;
- Key Recovery request is associated to an account owned by the Subscriber; and
- Subscriber is still affiliated to Subscribing Organization.

For authorization, three scenarios are possible:

Subscriber does not have a valid IdenTrust Signing ECA Certificate. In this case, the authorization is based on the authentication paperwork completed by the Subscribing Organization's KRO. An IdenTrust KRA will compare the information contained in that paperwork to information listed in the account associated with the Key Recovery request. The KRA will find the account using one of the account attributes (e.g. e-mail, name, account number) in the paperwork; and will ensure that the Subscribing Organization, Subscriber's full name, citizenship and e-mail match. If information matches, the authorization is confirmed, otherwise the request is denied.

Subscriber has a valid IdenTrust Signing ECA Certificate, but it is from a different account than the Certificate being requested for Key Recovery. In this case, the authorization is confirmed using electronic authentication based on a digital signature. The IdenTrust KRA will compare the information in the Certificate used to sign the request against the information in the account that is associated with the Key Recovery request. The KRA will find the accounts using one of the account attributes (e.g. e-mail, name, account number); and ensure that the Subscribing Organization, Subscriber full name, citizenship, and e-mail match. If information from both accounts match, the authorization is confirmed, otherwise the request is denied.

Subscriber has a valid IdenTrust Signing ECA Certificate and it is from the same account the Certificate being requested for Key Recovery request. In this case, the authorization is confirmed using electronic authentication based on a digital signature. The IdenTrust KRA will compare the information in the Certificate used to sign the request against the information in the account that is associated with the Key Recovery request. The KRA will find the account using an attribute listed in the Certificate (e.g. e-mail, name); and ensure that the Subscribing Organization, Subscriber's full name, citizenship, e-mail, and the disambiguating number (see IdenTrust ECA CPS section 3.1.5) match. If the information matches the authorization is confirmed, otherwise the request is denied.

3.4 KRA and KRO Authentication

3.4.1 KRA

KRAs authenticate to the KED by activating the administrative private key that decrypts the KED's user ID and password held in the KRA Workstation. Once the administrative private key is provided by the KRA, the KED user ID and password is submitted securely and automatically to the KED. KRA Workstation user IDs are assigned only to active KRAs by the Security Officer and configured into the KED system by the System Administrator. When an individual is no longer performing KRA functions, the user ID is removed. Passwords are created by the KRA and are memorized and never written. Communication of the KED's user ID and password is protected as explained in section 6.1.1 and 6.7 of this KRPS. Physical access to the KRA Workstation is explained in section 5.1.1.

3.4.2 KRO

KROs will be required to use IdenTrust's ECA Certificates of commensurate assurance level or higher of the key being requested (e.g., Medium Hardware Assurance Decryption Key requests may only be approved by a KRO holding a Medium Hardware Assurance Certificate) in all their communication with IdenTrust's KRAs. In every communication with IdenTrust from a KRO, KRAs will verify the following:

- the KROs' signature in the e-mail request is valid;
- the thumbprint of that Certificate matches the entry of the KRO in the secured list (described below) to ensure they are authorized for the Subscribing Organization; and
- compare the Certificate Policy OID listed in the properties of the KRO's Certificate with the requested Certificate's assurance level to verify it is of commensurate or higher assurance level.

IdenTrust maintains an updated and secured list of every Subscribing Organization's authorized KRO(s) that is checked to ensure that the request is valid as noted in the second bullet point above. This list is protected by a password known only to KRAs and located in a file within the internal network with access restricted to KRA roles. This list is assembled and updated by an IdenTrust designated KRA. Once updated, the password-protected list is made available to all other KRAs through a central Repository where the changes are immediately available.

The KRO is added to the list based on the information submitted by the Subscribing Organization during the nomination process and contained in the "Key Recovery Officer Addendum to Subscribing Organization Authorization Agreement". As part of the process, IdenTrust will require the KRO to submit a signed email using his or her Certificate, and information contained in the Certificate (i.e., serial number, thumbprint and assurance level based on the Certificate policy OID will be added to the list along with the KRO's name, Subscribing Organization's name and email address). IdenTrust's KROs will also be listed in the same document.

When the individual ceases to perform KRO functions, the Subscribing Organization must inform the IdenTrust Registration Desk. Upon confirmation from the Subscribing Organization the KRO's name is removed from the list. The request for removal from the list should be submitted by the officer who signed the original nomination. If the original nominating officer is not available, another KRO, a Trusted Correspondent, the KRO's supervisor, a member of the personnel office, a security officer, or a PKI Point of Contact can also submit the request. The request should be digitally signed to allow identity verification. Additionally, if the request is not submitted by the original nominating officer, the IdenTrust Registration Desk will verify the authority of the Requestor by confirming that the submitter is in one of the aforementioned positions.

If the individual performing the KRO function has not separated from the Subscribing Organization and is not in breach of any of the applicable terms of the "Key Recovery Officer Addendum to Subscribing Organization Authorization Agreement", then the Certificate will not be revoked. In all other cases, IdenTrust may at its sole discretion revoke the KRO's Certificate.

4 OPERATIONAL REQUIREMENTS

4.1 Escrowed Key Recovery Requests

4.1.1 Who Can Request Recovery of Escrowed Keys

Subscribers, authorized employees from the Subscribing Organization, and law enforcement can request recovery of escrowed keys.

Subscribers may submit requests for recovery of their own escrowed keys directly to IdenTrust or through their Organization's KRO.

Other employees within the Subscribing Organization can request Key Recovery for Certificates that do not belong to them. The Subscribing Organization must indicate explicitly in writing who are authorized Internal Requestors.

KROs do not have inherent authority to request Key Recovery on behalf of the Organization. KROs only perform Requestors' identity and authority confirmation and forward such requests to IdenTrust. Subscribing Organizations must not appoint KROs as Internal Requestors and vice versa.

In cases where law enforcement is the Requestor, a subpoena, search warrant or court order will be served upon the Subscribing Organization or IdenTrust. In response, the Organization's KRO or IdenTrust, as the case may be, may elect to treat the writ as a Key Recovery request. In either case, the identity and authority of the Requestor will be confirmed. Assistance of legal counsel of the Subscribing Organization or IdenTrust, depending on who is served with the subpoena, search warrant or court order, maybe sought in confirming the identity and validating the request.

4.1.2 Requirements for Requesting Escrowed Key Recovery

In order for a Key Recovery request to be approved, the Requestor must submit appropriate, sufficient information, sign the request, and, direct the request to the appropriate person.

4.1.2.1 Key Recovery through KRA

To start a Key Recovery, a Requestor should download a copy of Appendix C: Letter Agreement: Key Recovery Request, located at IdenTrust's ECA program web page, The Requestor must specify the following:

- Subscriber's identity including first name, middle initial, last name and email;
- Data needed to establish what Decryption Key(s) need to be recovered (i.e., Certificate's use date and serial number);
- Subscribing Organization name;
- Requestor's identity including first name, middle initial and last name (In cases that the Requestor does not have a valid IdenTrust ECA Certificate, two forms of identification need to be provided to the KRO or KRA in person as specified in section 3.2.2;
- Data needed to establish Requestor's authority to request recovery including job title and Organization that employs him or her; and

- Reason for Key Recovery *(e.g., lost or damaged Cryptographic Module, Subscriber is unavailable, official investigation, etc.).*

The Requestor will complete the request form, an electronic document (e.g. PDF file), and sign it with his or her Signature Key. This signature will correspond to the Requestor's valid IdenTrust ECA Signing Certificate. The Requestor will submit the forms within an email encrypted with an IdenTrust ECA encryption key belonging to the KRO or KRA that received the request. All Certificates that sign the forms, sign and encrypt the email must be of the same or higher assurance level of the Decryption Key being requested. Each request is verified by a KRA manually to Confirm the assurance levels of the Certificates used for the Key Recovery request by reviewing the signature Certificate OIDs. When a valid IdenTrust ECA Signing Certificate is not available, the Requestor may submit a Key Recovery Request Form completely filled out and signed by hand and verified by a KRO or KRA according to section 3.2.2.

The Key Recovery request should be submitted to a KRO. In Subscribing Organizations with KROs, they can process the request. If the Subscribing Organization does not have a KRO available, a digitally signed form and encrypted email request must be submitted directly to an IdenTrust KRA or a manually signed request must be presented in person to an IdenTrust KRO or KRA. A Subscribing Organization's KRO, the IdenTrust's KRO or KRA, as the case may be, will Confirm the identity and authority of the Requestor in accordance with these KRPS sections 3.2.1, and 3.2.2 respectively. In cases where a Subscriber provides a digitally signed form within an encrypted email to an intermediary such as a Subscribing Organization's KRO, this encrypted email with the signed form attached will be forwarded to IdenTrust along with the request so that IdenTrust's KRA can also verify the digital signature and assurance level.

4.1.2.2 Automated Self Recovery

IdenTrust does not provide self-recovery services at this time.

4.2 Protection of Escrowed Keys

The KED is a set of tables within a secure database that holds Decryption Keys for escrow. This KED is accessed only by the CA applications that create the Decryption Keys and the KRA Workstation that extracts them when requested. The CA applications and the KRA Workstation access the KED using the controls specified in section 6.1.1 and in IdenTrust's ECA CPS section 6.1.2.

After the key is generated in the FIPS 140 level 2 HSM, it is exported to the CA server and it is encrypted with a public key associated with an administrative Certificate and is stored in the KED. After the encryption is complete, the CA server memory is de-allocated and may be overwritten by other data. The encryption algorithm is commensurate in strength to the key being escrowed (see table below). The Certificates associated with the Certificate chain are also stored in the KED although they are not encrypted. The Decryption Key remains encrypted all the time in the KED until a Key Recovery request is performed.

At recovery, the encrypted "blob" is downloaded to the KRA Workstation for further processing. The KRA Workstation operating system is configured to disable the ability to page memory to the swap space to prevent the memory content from being written to disk. Furthermore, any keys left in memory on the KRA Workstation are erased by a memory scrubbing program that is used every time a key recovery is performed, and by shutting down the workstation after the Key Recovery sessions for the day are complete. The administrative Certificate is a self-signed Certificate with a key pair of commensurate strength as the keys being escrowed (See table below) and validity of 10 years. The administrative private key, corresponding to the administrative Certificate, is under two-person control. The administrative private key is held on a cryptographic token that is stored in a safe that requires at least two KRAs to access it. The KRA token containing the administrative private key is never left unattended while in use. When not in use, the KRA token is securely stored in the safe. Controls around the KRA

token are explained in section 5.1.2. For the complete recovery of an escrowed key, the administrative private key needs to be utilized in conjunction with the KRA Workstation to decrypt the escrowed material.

Escrowed Key Type Size	KED Encryption Algorithm	Administrative Certificate Key Size
RSA 1024	RSA	RSA 2048
RSA 2048	RSA	RSA 2048

The KRA Workstation provides functionality to extract the encrypted Decryption Key from the KED, decrypt the key, assemble the Certificate chain and provide support for basic administrative tasks related to the distribution of the recovered key and Certificates. Access to the KRA functionality is restricted only to ECA KRA personnel. Only the KRA Workstation with the administrative private key activated can decrypt the files stored in the KED.

Delivery of the recovered key to the Requestor is performed using two pieces of information that are passed to the Requestor through two different channels. The two separate pieces of information will vary depending on whether the recovered key will be delivered to the Requestor on a cryptographic token. The two parts are either: (1) for Medium Assurance Certificates--an RSA PKCS#12 and P12 password; or (2) for medium token and hardware assurance Certificates--a token and its protecting password, as illustrated in Figure 1.

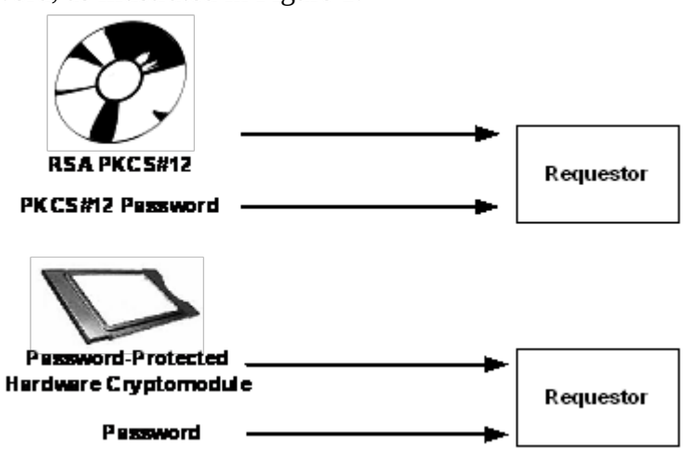

Figure 1.

Delivery methods are explained in greater detail below in section 6.1.3.2 of this KRPS. As a rule, IdenTrust will deliver both parts using different channels, but the end of the channels will always be the original Requestor.

4.2.1 Key Recovery through KRA

Two KRAs will provide access to a copy of an escrowed key only in response to a properly authenticated and authorized Key Recovery request. KRAs may receive Key Recovery requests in two ways:

- A KRO, either from a Subscribing Organization or IdenTrust, will forward an authenticated and authorized request; or
- A Requestor will contact the KRA directly.

Upon receipt of a Key Recovery request, a KRA will perform the following confirmations:

- Integrity of the request and validity of the KRO's digital signature;
- Verification that the KRO's Certificate assurance level is of commensurate or higher level than the assurance level of the requested Certificate;
- Authority of the KRO to forward a Key Recovery request to the KRA on behalf of that Organization by looking in the list of authorized KROs (See section 3.4.2);
- If available, the validity of the Requestor's Certificate and authenticity of Requestor's digital signature;
- If available, verification that the Requestor's Certificate assurance level is of commensurate or higher level than the assurance level of the requested Certificate; and
- Completeness of Key Recovery request information (See section 4.1.2.).

Upon receipt of a Key Recovery request directly from a Requestor, the KRA will perform the following confirmations:

- Requestor's identity in accordance with section 3.1 of this KRPS;
- Requestor's authority in accordance with sections 3.2.2 and 3.3.2 of this KRPS; and
- Completeness of Key Recovery request information (See section 4.1.2)

If all confirmations are satisfactorily completed, the extraction of the Decryption Key is authorized and initiated.

Access to the administrative private key, which enables the KRA Workstation to extract and decrypt escrowed Decryption Keys, is under two-person control and requires two KRAs. As described below in section 5.1.2, the hardware Cryptographic Module and the operator key that activates it are kept in separate safes protected with combinations each held separately by a different KRA--both KRAs are needed to activate the Cryptographic Module.

After the escrowed key is recovered and the Encryption Certificate is reconstituted, the Certificate and recovered key pair are delivered to the Requestor as explained in section 6.1.3.

4.2.2 Automated Self-Recovery

IdenTrust does not provide automated self-recovery at this time.

4.3 Certificate Issuance

Not applicable. Certificate issuance is addressed in section 4.3 of IdenTrust's ECA CPS.

4.4 Certificate Acceptance

Not applicable. Certificate acceptance is addressed in section 4.4 of IdenTrust's ECA CPS.

4.5 Security Audit Procedures

Security auditing capabilities of the underlying KED and KRA Workstation equipment operating system are enabled upon installation and remain enabled during operation.

Records of the events described below are made by IdenTrust personnel, the CA system, or KRA equipment for purposes of security audit. Whether the events are attributable to human action (in any role) or automatically invoked by the equipment is indicated. At a minimum, the information recorded includes the type of event and the time the event occurred. Information recorded for requested KED actions will include a success or failure indication and an individual's identity (when the action is started by an operator). In addition, for some types of events, it is appropriate to record the success or failure, the source or

destination of a message, or the disposition of a created object (e.g., a filename). Where possible, the audit data is collected automatically. When this is not possible, a logbook or other physical mechanism is used.

4.5.1 Types of events recorded

The KRS equipment is configured to record, at a minimum, the following event types and event data. These events may be recorded as part of the electronic audit log or manually:

- KED application access – date and time of action, type of event, identity of user accessing system and success or failure are automatically logged by the application;
- Messages received from any source requesting KED actions, (i.e., Key Escrow, extraction of encrypted blobs)-date and time of event, and content of message (excluding any encrypted/unencrypted Decryption Keys), and a success or failure indication are automatically logged by the appropriate application (i.e., CA system or KRA Workstation);
- Actions taken in response to requests for KED actions (i.e. responses received in the application) - date and time of action, and a success or failure indicator are automatically logged by the appropriate application (i.e. CA system or KRA Workstation);
- Physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying cryptographic token– date and time of action, identification of cryptographic token (i.e. serial number), type of action taken, name of person performing action and the signature of person performing action are manually logged;
- Receipt of Decryption Keys for escrow and posting of these keys to the KED – date and time of event, key identifier, and a success or failure indicator are automatically logged by the CA system application;
- Packaging, and shipping copies of escrowed keys – date and time of action, type of action, identity of person performing action, shipping information are logged manually;
- Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages – date and time of event and description of event are automatically logged by the application reporting the event or by the operating system; and
- Any known or suspected violations of physical security, suspected or known attempts to attack the KED equipment via network attacks, equipment failures, power outages, network failures, or violations of this Key Recovery policy – date and time of event, description of event, name of person reporting event and resolution are manually recorded by the Security Officer.

KRA system(s) are configured and operated to record the following event types and event data. These events may be recorded as part of the electronic audit log or manually recorded:

- KRA Workstation installation date and time of server installation, name of installer and details of server installation process are manually recorded by the installer;
- Modification to KRA Workstation, including changes in configuration files, security profiles, administrator privileges - date and time of change or modification, details of change, name of person performing change and authorization details are manually logged via change management system;
- KRA room access – date and time of entry and exit and identity of person presenting badge when entering the KRA room are automatically logged by the electronic security system;
- KRA safe access – date and time of access, identity of individual(s) accessing safe, reason for access (use of administrative cryptographic token or mailing information), and signature of person accessing safe are manually logged;

- Messages received from any source requesting KRA actions, (e.g., Key Recovery requests, second party Key Recovery approval requests) – date and time of request, identity of sender, Requestor's digital signature if available, and contents of message are manually logged by the KRA;
- Messages sent to any destination authorizing Key Recovery actions, (e.g., first party escrowed key retrieval authorizations, second party Key Recovery approvals) – date and time of action, identity of sender and recipient and contents of message are manually logged by KRA;
- Retrieval of encrypted blobs containing escrowed Decryption Keys – date and time of retrieval, key identifier and success or failure indicator are automatically logged by the KRA Workstation's application;
- Injection of keys into appropriate storage device (CD-ROM or Cryptographic Module) – date and time of action, type of action, flag of success or failure logged automatically by the KRA Workstation's application;
- Any use of the KRA's Signing Key – date and time of action, action taken and a success or failure indicator, are automatically logged by the application;
- Any use of the administrative private key – date and time of action, action taken are manually logged by the KRA;
- Transfer of recovered keys (i.e., RSA PKCS#12 or Cryptographic Module) to Requestors - date and time recovered keys are sent, method of delivery, identity of sender, identity of recipient, and delivery information are manually logged by the KRA;
- Any security-relevant actions performed in support of delivery of recovered keys – date and time of action, description of action and identity of person performing action are manually logged; and
- Requestor identity and authorization confirmation (including copies of authorizations; e.g., court orders) supporting Key Recovery requests acted upon by the KRO.

The KRO manually logs receipt of documentation including date and time of receipt, description of document, identity of KRO receiving document and any information regarding confirmation of these documents. The KRO retains electronic or physical copies of authorizations and identity documentation presented during confirmation.

All security audit logs, both electronic and paper (manual), are retained in accordance with the requirements of Section 4.5.3, and made available during compliance audits.

4.5.2 Audit Log Processing

Audit logs are processed in a manner to protect the integrity of the files. Restrictions are applied to the logs to prevent unauthorized access, deletion or overwriting of data. Storage capability is monitored to ensure that sufficient space exists in order to prevent overflow conditions. Alerts are sent if space available becomes inadequate.

The KED application and database audit logs are processed, protected and maintained using the same processes and procedures applicable to CMA equipment described in the IdenTrust CPS Sections 5.4.2 and 5.4.4.

IdenTrust's Security Officer will collect and analyze logs from the KRA Workstation. The logs are collected and analyzed offline, utilizing software designed to find pre-defined anomaly indicators. All logs are processed, protected and maintained using the same procedures described in the IdenTrust CPS Sections 5.4.2 and 5.4.4 to ensure the integrity, confidentiality and availability of the archived material.

4.5.3 Audit Log Retention Period

KRS audit logs are retained in the same manner described in the IdenTrust ECA CPS section 5.4.3. Audit log information generated on IdenTrust Key Recovery equipment is kept on the equipment until the information is moved to the offsite archive facility described in the IdenTrust ECA CPS Section 5.5.2.

IdenTrust will ensure that Subscribing Organizations also maintains KRO records in accordance with the ECA CP and the IdenTrust ECA CPS sections 5.5.2.

4.5.4 Audit Log Protection

KRS audit logs are protected from unauthorized modification or unauthorized deletion in the same manner described in the IdenTrust ECA CPS Section 5.4.4.

Subscribing Organizations will be obligated by contract, the ECA KRP and this KRPS to protect the KRO logs in accordance with the ECA KRP and this section of the KRPS.

4.5.5 Audit log back up procedures

KRS audit logs are backed up in the same manner described in the IdenTrust ECA CPS Section 5.4.4.

Subscribing Organizations will be obligated by contract, the ECA KRP and this KRPS to implement equivalent audit log backup procedures in accordance with the ECA KRP and this section of the KRPS.

4.5.6 Audit Log Collection System (Internal vs. External)

The audit log process is internal to the KED and the KRA Workstation. Audit processes are invoked at component system startup and cease only at component system shutdown. Audit processes run automatically without human intervention. IdenTrust will invoke audit processes at system startup, which cease only at system shutdown.

Since the KRA Workstation is in its own secure network segment with no communication to the security logging server, the KRA Workstation logs are manually backed up by a Security Officer monthly.

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

4.5.7 Subscriber Audit Notification

IdenTrust does not normally notify Subscribers of audit events.

4.5.8 Vulnerability assessments

The Security Officers monitor system and application logs from KRA equipment for evidence of events or actions that violate the integrity, confidentiality or availability of the KRS, including the equipment, physical location, and personnel. Vulnerability assessments related to the KRS is performed by the Security Officer at least weekly.

The KRA and Security Officer monitor e-mail communication and patterns of behavior from KROs for evidence of events or actions that violate the integrity, confidentiality, or availability of the KRS including the equipment, physical location and personnel.

Event logs are reviewed to ensure the integrity of the KRS. At a minimum, events listed in sections 4.5.1 of this KRPS and section 5.5.1 of the IdenTrust ECA CPS are reviewed for content, anomalies, consistency, access events, and retrieval events.

4.6 Records Archival

IdenTrust maintains a trusted archive of information it stores and of transactions it carries 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:

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

4.6.1 Types of information recorded

IdenTrust favors the use of electronic records and will electronically archive scanned paper records in every possible case. IdenTrust maintains and archives the following records in either electronic or paper format:

- ECA KRP and KRPS - Electronic;
- Agreements, if any (with KRAs, KROs, Subscribers, and/or Subscribing Organizations) - Paper;
- Request forms or data submitted requesting Key Recovery - Paper;
- Audit log – Paper / Electronic; and
- Escrowed keys - Electronic.

The ECA KRP is archived by the EPMA. All other information is archived by IdenTrust.

To support interpretation of the information during the entire archive retention period applications, and hardware if appropriate, required to process the archive data are maintained for at least as long as the data they process.

Subscribing Organizations are obligated by contract, the ECA KRP and this KRPS to maintain and archive records of the identification and authorization verification process followed by the Organization's KROs. The Subscribing Organization will select the best format, electronic or paper, based on their specific policies.

4.6.2 Archive Retention Period

Escrowed keys are maintained within the online KED for a minimum of one year after the expiration of the associated public key Certificate; however, IdenTrust may retain keys online within the KED for longer periods of time to facilitate Key Recovery. Besides the online KED retention, the Escrowed keys are encrypted as described in section 4.6.3 and handled in the manner described in the IdenTrust ECA CPS Section 4.6.2 and the KRS's archive records are handled in the manner described in the IdenTrust ECA CPS Section 5.5.2.

4.6.3 Archive Protection

No one will be able to modify or delete archived data. KRS Archived data is protected utilizing the same procedures and controls described in the IdenTrust ECA CPS Section 5.5.3. The KED sensitive fields are encrypted with 2048 RSA separate from the AES-256-CFB used to encrypt the KRS data and the KED data for archive. The KRS archive data being backed up, including the KED, is encrypted using AES-256-CFB. The escrowed Encryption Keys stored in the KED sensitive fields are not decrypted for this process. The password for the AES 256-CFB encryption of the archive copies is written to CD-ROM. A checksum is produced from the CD-ROM to further protect that data. Once that is completed the contents are placed into a metal lockbox. These lockboxes are inventoried, logged and sealed with padlocks under dual control. The labels on the boxes provide no indication of their contents that is decipherable to anyone outside of the company. These boxes are then

transported by bonded courier to the offsite vault that is described in section 5.1.6 of the IdenTrust ECA CPS. IdenTrust's procedures ensure multi-party control and segregation of duties. Only Trusted Role employees preauthorized by the CIO or VP of Operations may call the offsite storage facility for media.

4.6.4 Archive backup procedures

No stipulation.

4.6.5 Requirements for time-stamping of records

The archived records contain information necessary to determine when the events occurred. The time precision is such that the sequence of events can be determined. IdenTrust synchronizes the internal clocks on all production KRS equipment using the Network Time Protocol (NTP). IdenTrust uses a stratum 3 time server that gets its time from external sources and sits in the inner tier of the network inheriting the security controls for the network explained in IdenTrust CPS Section 6.7. The database server, where the KED is maintained, connects to the IdenTrust time server via its UDP port. The KRA Workstation is connected to the database server through its UDP port. Trusted external time sources operated by government agencies are used to maintain an average accuracy of one (1) minute or better.

4.6.6 Archive Collection System (Internal vs. External)

Archive data is collected in an expedient manner. IdenTrust's archives of KRS-related data, are collected internally but stored externally.

4.6.7 Procedures to obtain and verify archive information

IdenTrust uses procedures described in IdenTrust ECA CPS Section 5.5.7 to create, package and send KRS archive data.

4.7 KRA, KRO and administrative Key Changeover

KRAs will re-key at least every three (3) years.

Administrative Keys will be re-generated every ten (10) years. Administrative Keys no longer active will still be kept, in the same cryptographic token, for recovery of old escrowed keys. The new active administrative key will be used to encrypt new Decryption Keys.

All KROs will re-key in correspondence with their Certificate type.

4.8 KED Compromise and Disaster Recovery

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

4.8.1 KED Compromise

In the event that the KED or the administrative key that encrypts the escrowed Decryption Keys is compromised or is suspected to be compromised, IdenTrust will notify the EPMA. Then IdenTrust will re-encrypt the database with a new public administrative key generated and held in a new cryptographic set (i.e., primary token and two backups), quarantine all instances of the database that were encrypted with the old public administrative key and zeroize all remaining cryptographic tokens holding compromised keys. The EPMA will be granted sufficient access to information necessary to determine the

extent of the compromise and the EPMA will direct the appropriate action. This may include revocation of Certificates associated with the compromised Decryption Keys stored in the KED.

4.8.2 Disaster Recovery

In the event of a disaster the KRS will re-establish a secure environment. The procedures for reestablishing the secure environment after the disaster are detailed in the IdenTrust ECA CPS section 5.7.4, IdenTrust's Disaster Recovery Plan and Business Continuity Plan procedures. In the event of a catastrophic disaster, IdenTrust maintains backup cryptographic materials at an off-site data storage facility. The KRS cryptographic material would be retrieved from that facility utilizing Business Continuity Plan procedures to ensure multi-party control and services would be re-established within the KRS secure environment.

IdenTrust formally tests its Business Continuity Plan and Disaster Recovery procedures at least annually. In the event there are major changes to the operations platform; IdenTrust will evaluate the need to retest portions of the plans or initiate a complete retest and evaluation of the policies, procedures and plans.

IdenTrust will notify the DOD PKI Root CA and the EPMA of any such disaster or compromise informally via telephone call as soon as reasonably possible. Such call will be followed formally by a Certificate-based communication if possible or otherwise by a written letter sent by courier service.

4.8.3 KRA or KRO Key Compromise

For the performance of their daily activities, individuals performing the KRA and KRO roles are provided with IdenTrust ECA Certificates. These ECA Certificates are revoked in case of compromise. If the KRA or KRO's Certificate is revoked due to compromise, there is a potential for some Subscribers' escrowed keys to have been exposed. The Security Officer will follow established incident response procedures and review the audit records to identify whether escrowed keys may have been exposed. This would include a review and query of all keys recovered using the compromised KRO's or KRA's key through either a manual or automated search. Certificates associated with each of the potentially exposed escrowed keys will be revoked, according to procedures specified in the IdenTrust ECA CPS Section 4.9, and the Subscriber will be notified of the revocation.

If a KRO or the KRA Workstation is compromised, there is potential for Subscribers' escrowed keys to have been exposed. The Security Officer, for the KRA Workstation, or the Organization's internal auditor, for the KRO workstation, will stop the operation of the workstation and start an investigation of the extent of the compromise per established incident response procedures. Certificates associated with the potentially exposed escrowed keys will be revoked.

4.8.4 KRA or KRO Certificate Revocation

If the KRA or KRO Certificate is revoked for any reason, but the KRA or KRO remains authorized to perform his or her duties, then the KRA or KRO will request a new KRA or KRO Certificate from IdenTrust. IdenTrust will report the old KRA or KRO Certificate as revoked using IdenTrust's revocation notification policy. IdenTrust will follow its policy for Certificate issuance for the new KRA or KRO public key Certificate.

In cases that a KRO or KRA Certificate is revoked due to misuse by the holder, the KRO or KRA will be declared compromised and the procedures outlined in section 4.8.3 above will be used.

4.8.5 Administrative Private Key Compromise

If the administrative private key held in the Cryptographic Module is compromised, IdenTrust will notify the EPMA. The EPMA will be granted sufficient access to information necessary to determine the extent of the compromise and the EPMA will direct the appropriate action.

IdenTrust will take immediate actions that may include removal of the administrative Certificate and generation of a new one; decryption and re-encryption of the entire KED with the new Administrative Keys, as well as the potential revocation of any Subscribers' Certificates corresponding to Decryption Keys that may have been exposed. The compromised administrative Certificate and Administrative Keys will be zeroized upon completion of the re-encryption of the KED with the new Administrative Keys and a backup of the KED is created.

4.9 KRA Termination

Upon KRA termination, IdenTrust will archive all KRA records according to archive procedures outlined in the IdenTrust ECA CPS section 5.5.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

The KED will consist of a dedicated set of tables with encrypted material residing in the shared customer database hosted in equipment dedicated to PKI functions. The cryptographic token used for the KED houses the private key of the administrative Certificate, encrypting the Decryption Keys, and Administrative Keys for the cryptographic token itself. No other keys are present on the cryptographic token. The KRA Workstation used to host the applications that interact with the KED will not be used for any purpose other than Key Recovery.

Since the KED is part of the main customer database, the physical controls explained in the IdenTrust ECA CPS section 5.1 for the CA equipment apply to the KED.

Physical controls for the administrative cryptographic token and the KRA Workstation are explained in the following sections.

5.1.1 IdenTrust's Cryptographic Token and KRA Workstations Site

The cryptographic token and KRA Workstation are located in a building geographically separated from the KED and CA site. They are housed in an unmarked building; the site is not identified as housing IdenTrust equipment in a publicly visible way. The cryptographic token and KRA Workstation are located in an isolated and restricted-access room with no windows on the second floor of the building (the "KRA Room").

Multiple layers of security surround the KRA Workstations including external building and fourth floor doors with restricted access; tighter access control restrictions to the "KRA" room; and KRA Workstation room door with further restricted access. Additional layers of security surround the Cryptographic Module and the operator key. The cryptographic token and the operator key are kept within separate mini-vaults under two-person control from separate groups and those mini-vaults are kept within a larger safe.

5.1.2 Physical Access

The building entryways and the KRA Room are video-recorded 24 hours a day, 365 days a year. IdenTrust's security officers perform periodic checks and reviews of the security integrity of the facilities to ensure that alarms, access points, video cameras, storage containers, safes (containing the token and operator key), access logging, etc., are operational and functioning correctly. A record is kept that describes the type of checks performed, the time, and the person who performed them. Records are kept for no less than one year and reviewed with external auditors on an annual basis as part of the WebTrust for Certification Authorities audit.

IdenTrust personnel require two-person, two-factor controls to access the KRA room including pass cards and security codes. Pass cards for personnel working in IdenTrust's offices are granted upon authorization from IdenTrust security officers or Operations Management. Specific access to the KRA room is granted only to personnel with ECA Trusted Role status. The KRA Room is equipped with a motion-detection system that is armed when personnel are not in the room. When the motion-detection system is activated, a local alarm sounds and an external monitoring company is notified, who in turn contacts IdenTrust Security Officers or Operations Management. Arming and disarming the motion-detection system requires entering a security code.

Employees are prohibited from permitting unknown or unauthorized persons to gain access to the KRA room. Authorization to enter must be obtained in advance from Operations Management. Visitors must further properly identify themselves and the purpose for their visit. Visitors are not allowed to roam in IdenTrust-controlled areas without escorts. A Trusted Role employee will accompany any personnel or contractors into the KRA room when necessary.

All entry to and exit from the KRA Room is logged with the respective times and date of access.

Access to KRA Workstation requires individualized logon activation data that is memorized and never written down. Aside from the logon data, the KRA Workstation itself cannot provide software or Key Recovery functions unless it is connected to the Administrative Key, which is stored within the storage safes inside of the KRA room under two-person, two-factor control..

Access to storage safes containing the token and the operator key located inside the KRA Room is controlled through separation-of-duties/multi-party control. There are two mini safes located inside a larger safe. Each of the mini safes within the larger safe each holds either the token or the operator key. Each of the mini safes has a combination lock with a unique combination. No single employee has access to both mini safe combinations. Access to the combination of the first mini safe is restricted to a specific group of KRAs (i.e., RA Operators) that is different from the KRA group that has access to the combination of the second mini safe (i.e., Help Desk Representatives). All access to material inside the safes is documented through an access log and is signed for by (2) two KRAs.In order to communicate via secure email with KROs, KRAs use the same RA-client side equipment described in the IdenTrust ECA CPS section 5.1.1.2. This equipment is different than the KRA Workstation and the physical controls are already described in the IdenTrust ECA CPS 5.1.2.2.

5.1.3 Power and Air Conditioning

The facility that houses the IdenTrust KRA room is supplied with power and air conditioning sufficient to create a reliable operating environment.

In case of public power failures, a full battery backup and a propane generator for secondary power redundancy are available. The uninterruptible power supply (UPS) provides temporary power for the facility and automatically activates the generator when a power failure is detected. The fuel tank can be refueled on the go for continuous service. This system is tested under load weekly.

5.1.4 Water Exposures

The KRA Workstation is installed such that it is not in danger of exposure to water, i.e., elevated above ground level and floor level.

The cryptographic token is stored in water-proof tamper-evident bags.

5.1.5 Fire Prevention and Protection

The automatic fire extinguishing system is installed in accordance with local fire policy and code. If fire or sprinkler system damage causes IdenTrust's KRA Workstation or the cryptographic token to become inoperative, IdenTrust will follow its disaster recovery plan referenced in section 4.8.

5.1.6 Media Storage

Backups of the cryptographic token, Key Recovery Requests in paper or electronic form, and any other material used during the Key Recovery process are kept in accordance with practices described in sections 5.1.6 and 5.5.3 of IdenTrust’s ECA CPS.

5.1.7 Waste Disposal

Media used to collect or transmit information discussed in section 2.8 will be destroyed in accordance with practices described in section 5.1.7 of IdenTrust’s ECA CPS.

5.1.8 Off-site Back-up

The KED is backed up in accordance to practices described in section 5.1.8 of IdenTrust's ECA CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Prior to assigning any IdenTrust employee to a Trusted Role that person must be identified to the IdenTrust Human Resource department as eligible and approved and authorized by Operations Management. IdenTrust maintains lists of all persons filling Trusted Roles. These lists include the following information: name of person, position they are serving in and their contact information. These lists will be available during compliance audit.

IdenTrust defines three Trusted Roles that execute functions related to Key Recovery. Two of those Trusted Roles perform KRA functions

- RA Operator (KRA role),
- Help Desk Representative (KRA role),
- Key Recovery Officer.

5.2.1.1 Key Recovery Agent

All RA Operators and Help Desk Representatives that operate under this Policy are subject to the stipulations of the ECA KRP and of this KRPS. The RA Operator and Help Desk Representatives are Trusted Roles defined by IdenTrust.

The IdenTrust RA Operator and Help Desk Representative common responsibilities and operating procedures, as they relate to the Key Recovery System Operations, are as follows:

- KRO functions as described in section 5.2.1.2, if no separate KRO is employed;
- Assemble and maintain a list of authorized KROs for each Subscribing Organization that will be used as the basis for verification of KROs' authority for the Subscribing Organization;
- Approve and initiate the recovery of escrowed keys; and
- Distribute the recovered keys (e.g., RSA PKCS#12 or Cryptographic Module) to Requestors, with protection as described in section 4.2.

The IdenTrust Help Desk Representative and the RA Operator have the responsibility to protect the information to access and activate the cryptographic token. RA Operators have access to the combination to one safe (i.e., cryptographic token), while Help Desk Representatives have access to the other safe's combination (i.e., operator key).

5.2.1.2 Key Recovery Official

All KROs that operate under this KRPS are also subject to the stipulations of the ECA KRP. The KRO is a Trusted Role defined by IdenTrust. The KRO role and corresponding procedures are defined below. A KRO's responsibilities are to ensure that the following functions are performed:

- Confirm Requestor's identity and authorization as stated by the ECA KRP and this KRPS;
- Build Key Recovery requests on behalf of authorized Requestors; and

- Securely communicate Key Recovery requests to and responses from the RA Operators and Help Desk Representatives.

5.2.1.3 Other Trusted Roles

Other Trusted Roles are IdenTrust's CA Administrator, System Administrator, Network Engineer, Security Officer, and Operations Management. These other Trusted Roles are defined in IdenTrust's ECA CPS. The responsible persons who are identified in these Trusted Roles are named and made available during compliance audits. The Key Recovery System responsibilities are divided among these roles and are performed in addition to the responsibilities defined in IdenTrust's ECA CPS for these roles. The division of responsibilities is as follows:

5.2.1.3.1 CA Administrator

CA administrators are responsible for the following:

- Generation, cloning, and destruction of the administrative key pair and corresponding Certificate; and
- Receipt, initialization, usage and management, including cloning, of the cryptographic tokens where the administrative private key is generated and held.

No person participating as IdenTrust CA Administrator will assume the Security Officer or Operations Management role. These roles maintain strict segregation of duties. Controls are in place to ensure this separation Physical management of the Administrative key pair and key material, as stated in the second bullet point, requires multiple controls to be satisfied including pre-approvals from Operations Management roles, scripted ceremonies that are video recorded and witnessed by the Security Officer and System Administrators, and handled within the secure room described in section 5.1 and under two-person control.

5.2.1.3.2 System Administrator

System Administrators are responsible for the following:

- Initial configuration of the system, including KED and KRA Workstation, including installation of applications, and initial setup of new accounts;
- Performance of system backups, software upgrades, patches, and system recoverability;
- Secure storage and distribution of backups and upgrades to an off-site location;
- Backup and archival of the security audit log (except for KRA Workstation logs) and other data as described in Sections 4.5 and 4.6 of this document;
- Performing the daily incremental KED backups; and
- Administrative functions such maintaining the KED.

A System Administrator will not assume the Security Officer or Operations Management role. These roles maintain strict segregation of duties. Controls are in place requiring the approval for root level access or other such access from the Security Officer or Operations Management prior to such access being granted.

Segregation of duties between System Administrators and CA administrators is further enforced separating the CA servers' root-level access and passwords for the CA. Without the cooperation of both administrators, IdenTrust software is inoperable for purposes including Generation, cloning, and destruction of the Administrative key pair as described in section 5.2.1.3.1.

5.2.1.3.3 Network Engineer

Network Engineers are responsible for:

- Initial installation and configuration of the network routers and switching equipment, configuration of initial host and network interface;
- Creation of devices to support recovery from catastrophic system loss; and
- Changing the host or network interface configuration.

The Network Engineer will not assume Security Officer or Operations Management role, as these roles maintain strict segregation of duties. Controls are in place, for example, approvals for changes to firewall rules are required by the Security Officer or Operations Management roles prior to implementation by a Network Engineer.

5.2.1.3.4 Security Officer

The Security officer is responsible for the following:

- Assignment of security privileges and access controls to Key Recovery System personnel;
- Backup and archival of the KRA Workstation security audit logs;
- Review of the audit logs; and
- Administrative functions such as compromise reporting.

The Security Officer may not serve in the roles of CA Administrator, Systems Administrator, or Network Engineer.

5.2.1.3.5 Operations Management

Operations Management as Risk Management Committee members perform the following duties:

- Review of special compliance audits in cases where a KRO or KRA is relieved of that responsibility due to a failure to comply with the ECA KRP or this KRPS; and
- Review of security incidents reported by the Security Officer.
- Risk Management Committee members will not serve in external auditor roles.

5.2.2 Separation of Roles

Under no circumstances will a KRA or KRO perform a Trusted Role for a KED facility as defined in Section 5.2.1.3.

Under no circumstances will a KRA or KRO perform his or her own compliance audit function.

Separation of responsibilities among Trusted Roles for the KED is described in each subsection of section 5.2.1.3 of this KRPS.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

Persons selected for KRA roles for operation of the KRS will meet the requirements specified in IdenTrust's ECA CPS section 5.3.1 for CMA roles.

Persons selected for KRO will meet the requirements specified in IdenTrust's ECA CPS for individuals in the role of Trusted Correspondents specified in IdenTrust's ECA CPS Section 5.3.1.

5.3.2 Background check procedures

Background check procedures are as specified in Section 5.3.2 of IdenTrust's ECA CPS.

5.3.3 Training requirements

IdenTrust requires mandatory periodic training in multiple areas of computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of the ECA computer system. This training is described in section 5.3.3 of IdenTrust's ECA CPS. In addition to that training, all personnel involved in the Key Recovery System operation are appropriately trained in topics related to this specific system.

IdenTrust maintains a file that contains signed and dated records from IdenTrust personnel listing their names, roles, training received, and date that training was completed.

Specific topics for every role will include:

RA Operator and Help Desk Representatives

Any employee serving in the RA Operator and Help Desk Representative role will be trained in the following areas:

- All the KRO functions;
- Processes related to the approval and initiation the Key Recovery;
- Secure distribution of recovered keys to Requestors;
- Techniques to monitor and detect potentially anomalous activity; and
- Operation of the KRA Workstation.

Key Recovery Officer

- Confirmation of Requestor's identity and authority in accordance with IdenTrust procedures;
- Verification of Requestor's Key Recovery request forms correctness and completion;
- Security around recovered keys; and
- Secure communication of Key Recovery requests to and responses from RA Operators and Help Desk Representatives.

CA Administrator

- Generation and Certificate lifecycle details for Administrative Key pairs and its associated Certificate.

System Administrators

- Installation and maintenance of KRA Workstation application.

Security Officer

- Techniques to monitor and detect potentially anomalous activity related to Key Recovery processes.

Operations Management Personnel

- Audit procedures and investigation procedures for when a RA Operator or Help Desk Representative is relieved of his or her responsibility due to a failure to comply with the ECA KRP or this KRPS.

IdenTrust maintains a file that contains signed and dated records from IdenTrust personnel listing their names, roles, training received, and date that training was completed including the items outlined above.

5.3.4 Retraining frequency and requirements

In the event that significant changes to Key Recovery System operation occur, IdenTrust will document those changes and implement a training (awareness) plan that includes any retraining required for Key Recovery System operation staff, KRA or KRO personnel as appropriate.

As explained in section 5.3.4 of the IdenTrust ECA CPS, Trusted Role employees undergo retraining every twelve (12) months. This training will also include relevant information about the practices in this KRPS and its ruling KRP.

5.3.5 Job rotation frequency and sequence

Job rotation frequency and sequence is specified in IdenTrust's ECA CPS.

5.3.6 Sanctions for unauthorized actions

Appropriate administrative and disciplinary actions will commence against personnel who violate this KRPS. Sanctions will be applied in accordance with section 5.3.6 of the IdenTrust ECA CPS.

Subscribing Organizations are obligated by contract and the ECA KRP and this KRPS to commence administrative and disciplinary action against personnel who violate the Subscribing Organization's policy relating to Key Recovery.

5.3.7 Contracting personnel requirements

All IdenTrust subcontractors providing services for the ECA Program are required to perform in accordance with the ECA KRP and this KRPS. All subcontractor personnel are subject to all personnel requirements of this KRPS, including the ones described in section 5.3 and subsections thereof. IdenTrust supplies its contracting personnel with documentation sufficient to define duties and procedures for each role will be provided to the personnel filling that role.

Failure of any employee or agent of IdenTrust to comply with the provisions of the ECA KRP or this KRPS, whether through negligence or with malicious intent, will subject such individuals to appropriate administrative and disciplinary actions, which may include termination as an agent or employee of IdenTrust and possible civil and criminal sanctions.

IdenTrust personnel performing KRO and KRA functions are Trusted Roles and any potential unauthorized or inappropriate action in relationship to the ECA KRP and this KRPS will be treated as explained in the IdenTrust CPS section 5.3.7.

5.3.8 Documentation supplied to personnel

Personnel filling the roles of RA Operator, Help Desk Representative, KRO, CA Administrator, System Administrator, Network Engineer, Security Officer, and Operations Management will be provided (have in their possession or have access to) documentation defining the duties and procedures of such roles in what relates to the Key Recovery System's installation, operation, administrative functions, and security. The information will be available in print or on-line.

At a minimum the following information is provided:

RA Operator and Help Desk Representative

Procedures related to:

- Confirmation of Requestor's identity and authority;
- Verification of digital signatures:
- The approval and initiation the Key Recovery;

- Secure communication with KROs; and
- Manuals for operation of the KRA Workstation including:
    - Operation of software to extract escrowed keys;
    - Secure use of the administrative private key associated Certificate and the cryptographic token;
    - Secure distribution of recovered keys to Requestors;
    - Deletion of key recovered material;
    - Procedures on how to monitor and detect potentially anomalous activity; and
    - Key Recovery Forms Information.

Key Recovery Officer

Procedures related to:

- Confirmation of Requestor's identity and authority;
- Verification of digital signatures;
- Secure communication with RA Operators and Help Desk Representative; and
- Key Recovery Request Forms Information.

CA Administrator

- Procedures and scripts for generation and other Certificate lifecycle events for administrative Certificates.

System Administrators

- Technical manuals for KRS including:
- Installation and maintenance of KED; and
- Installation and maintenance of KRA Workstation software.

Security Officer

- Technical manuals for audit tools including messaging that indicates anomalous behavior; and
- Information that enables understanding of audit logs.

Operations Management Personnel

- Procedures for completing audits and investigation for when an RA Operator or Help Desk Representative is relieved of his or her responsibility due to a failure to comply with the ECA KRP or this KRPS.

6 TECHNICAL SECURITY CONTROLS

6.1 Protocol Security

When recovered by the KRAs, all copies of escrowed keys will be protected continuously by two-person controls. Delivery mechanisms have been designed to minimize the risk of exposure to every part of the recovered key and to ensure the authenticated and authorized Requestor receives all components of the key. Both KRAs work in unison, maintaining two-person control, to securely store the key(s) and corresponding recovered Certificates(s) into the appropriate Cryptographic Module.

Furthermore, the delivery mechanism for copies of escrowed keys will provide protection against disclosure with assurance equal to or greater than the level of the Certificates associated with the escrowed keys. Recovered keys always remain within a PKCS#12 file or within a Cryptographic Module validated in accordance to FIPS requirements appropriate to the assurance level. IdenTrust implements a process that separates parts necessary to reconstruct the recovered key until it is delivered via mail as explained in later sections.

6.1.1 KED Protocol Security

Communication between the KRA Workstation and the KED is protected by an AES-256 IPSEC VPN. The VPN is established through a hardware device that encrypts all traffic from the KRA Workstation to the network segment where the KED application is located. Traffic is decrypted with the associated VPN hardware device. The VPN is set up with vendor-recommended authorization requirements. The KED and firewall are locked to allow KRA communication only by IP address and required port numbers. Only Trusted Role employees with authorization to use the KRA know the VPN password. The KRA is housed in a room secured using two-factor authentication, and the VPN device is removed from the KRA and placed in a dual-control safe when the workstation is not in use.

The KED is protected in order to prevent unauthorized use as described here and in section 6.6. Firewall rules are applied that allow only the authorized KRA Workstation access to the KED. KRA Workstation-to-KED communication requires authentication to the KED. The KED user ID and password are kept encrypted in the KRA Workstation. The public key of the administrative Certificate is used to encrypt this information. The administrative private key is used to decrypt the user ID and password. This private key is kept under separation-of-duties/multi-party control as explained in Section 5.1.2.

6.1.2 KRA - KRO Protocol Security

Communications between an IdenTrust KRA and a KRO will be through digitally signed electronic mail. Every KRA and KRO will be required to obtain a digital Certificate(s) that will enable him or her to communicate via signed and encrypted S/MIME. Digital Certificates for all KRAs are IdenTrust's ECA Medium Assurance Hardware Certificates that will provide the appropriate degree of assurance to any communication. Certificate for KROs are commensurate to the level of assurance of the population they are serving but at a minimum, they will be provided with IdenTrust's ECA Medium Token Assurance Certificates.

KRAs and KROs will be instructed to configure their email clients to use SHA-1 hash algorithm or an equivalent algorithm, as well as 3DES for the encryption algorithm or another FIPS algorithm (i.e., AES) that provides equivalent strength.

Non-electronic communication of recovered keys will be through mail or courier channels that provide tracking of the package, and receipt-signature verification. No single package will contain all of the information needed to obtain the recovered key. Envelopes and packaging used in distribution of any key material will be tamper-evident.

6.1.3 Escrowed Key Distribution Security

IdenTrust has opted for not involving KROs in the distribution of recovered keys.

6.1.3.1 Distribution of Recovered Keys Requested by Subscriber through Automated Self-Recovery

Self-Recovery services are not implemented at this time.

6.1.3.2 Distribution of Recovered Keys Requested by Requestor through KRO/KRA

As illustrated in Figure 1, IdenTrust uses two similar processes to deliver recovered keys to Requestors--for Medium Assurance Certificates--an RSA PKCS#12 and P12 password; and for medium token or medium hardware assurance Certificates--a token/smart card and its protecting password

Direct Delivery to Requestor - Medium Assurance Certificate. After the KRAs have extracted the escrowed material into the KRA Workstation, the workstation will reconstitute the Certificate chain and transform it into a PKCS#12 file format. The password that protects the file will be generated by the workstation in accordance with the IdenTrust ECA CPS section 4.1.2.6 Delivery of Activation Code and Retrieval Kit. For every Decryption Key recovered, the system will generate one PKCS#12 file. The PKCS#12 file(s) will be burned into a CD-ROM. The CD-ROM burning process will prevent subsequent alteration. The corresponding password will be printed and/or protected in a way that any tampering is evident. The creation of the CD-ROM and printing the passwords will be controlled procedurally and performed by KRAs following two-person controls.

Then, the package with the CD-ROM and the envelope with the password will be mailed to the mailing address that is provided by the Requestor on the key recovery forms. The packages will be mailed through different courier/mail services offset by one business day. The envelope that is not mailed immediately will be stored in a safe in the KRA Room until the next business day's mail batch is processed.

The courier and mail services provide delivery confirmation as part of the service. Packaging for the cryptographic material is tamper evident.

Direct Delivery to Requestor – Medium Token / Medium Hardware Assurance Certificate. This process follows the same sequence until the keys have been extracted and decrypted. From that point, the following events occur: the recovered material is reconstituted into a Certificate chain, then the KRA Workstation will generate a random 8-character token password that will be used by the KRA to change the default token password. The token passcode is an 8 character value where each character has 6 bits of entropy. Entropy is gathered from the token itself using the C_GenerateRandom PKCS#11 function. After the token password is changed, the KRA Workstation will insert the Decryption Key and Certificate chain into the token, thereby confirming the token password. The token password will be printed and sealed in an envelope.

Then, the package with the cryptographic token and drivers, and the envelope with the token password are mailed to the mailing address on the key recovery request forms. The packages will be mailed through two different courier/mail services offset by one business day. The envelope that is not mailed immediately will be stored in a safe in the KRA Room until the next business day's mail batch is processed.

The courier and mail services provide delivery confirmation as part of the service. Packaging for the cryptographic material is tamper evident.

6.2 KED, KRA and KRO Private Key Protection

6.2.1 Standards for Cryptographic Modules

Cryptographic Modules will be validated to the FIPS 140-1 or FIPS 140-2 (as appropriate) level identified in this section, or validated, certified, or verified via one of the standards published by the EPMA.

KRAs and KROs will use hardware Cryptographic Modules that are validated to meet or exceed the criteria specified for FIPS 140-1/140-2 Level 2.

The cryptographic token holding the administrative private key is validated to meet the criteria specified for FIPS 140-1 level 3. These modules do not allow output of the private asymmetric key to plaintext.

6.2.2 Private Key Control

The private components of IdenTrust's KRA and KRO Signature Key pairs and the Decryption Key are under single person control to ensure non-repudiation of the KRA and KRO.

The administrative private key, associated to the administrative Certificate, used to decrypt escrowed keys in the KRA Workstation is under separation-of-duties/multi-party control. The names of all the individuals with control over the keys are maintained on a list that is made available for compliance audits.

When not in use, the cryptographic token containing the administrative private key is stored in a secure container within a safe in the KRA Room as explained in section 5.1.2 of this KRPS.

6.2.3 KED Key Backup

The IdenTrust's administrative private key is backed up to provide secure continuity of Key Recovery operations. The administrative private key is generated on a FIPS 140-1 level 3 Cryptographic Module that allows a "cloning" process to create a copy of the private key, which IdenTrust uses for purposes of business continuity. Cloning of the Administrative Key is done under two-person control and the process is documented in writing, approved by management, witnessed, and video-recorded.

Two cloned copies of the Administrative Key are created. One of the copies is held under two-person control in the offsite location described in the section 5.1.6 of the IdenTrust ECA CPS. The second copy is held in the primary facility's Secure Room under two-person control explained section 5.1.2.1.1 of the IdenTrust ECA CPS.

In case of need to restore a backup administrative key, a security officer and a second Trusted Role individual will, using two-person controls, attempt to restore the copy held in the primary facility's Secure Room. If this attempt fails, the Security Officer will request the delivery by the offsite-facility personnel of the second copy. In any case, two Trusted Roles from IdenTrust will take custody of the backup token, test it in the KRA Workstation and, with the assistance of at least one KRA, store it in the safe in the KRA Room.

6.2.4 Private Key Generation and Transport

KRA and KRO Certificates are IdenTrust-issued ECA Medium Hardware Assurance Certificates. Private keys for administrative Certificates are generated only within the Cryptographic Module. IdenTrust uses FIPS 140-1 level 3 Cryptographic Modules for its administrative Certificates. Generation of these keys is done under two-person control and the process is documented in writing, approved by management, witnessed, and video- recorded. Backup of the administrative private key is performed as explained above in section 6.2.3, and keys are never in plaintext outside of the tokens.

6.2.5 Method of Activating Private Key

Activation of the KRO and KRA private keys is accomplished as explained for Subscribers in the IdenTrust ECA CPS section 6.2.8.

Administrative private keys reside within a FIPS 140-1 Level 3 validated Cryptographic Module. Activation of the private key requires an operator key to be connected to the module. The administrative private key is activated by use of the operator key. The operator key that activates the module is stored securely and separately from the Cryptographic Module and is retrieved always under two-person control. This two-person control is achieved by the physical controls described in section 5.1.2 when retrieving the operator key and the Cryptographic Module. Two separate KRAs are present when the Cryptographic Module and the operator key are used to activate the administrative private keys: one KRA retrieves the Cryptographic Module and another one the operator key.

6.2.6 Method of Deactivating Private Key

The private component of the KRO and KRA key pairs is deactivated as described for Subscribers' private keys in section 6.2.9 of the IdenTrust ECA CPS.

The administrative private key is used by the KRA Workstation to decrypt the encrypted escrow material. Deactivation information is explained in the section 6.2.7 below.

6.2.7 Method of Deactivating Storage Key

The cryptographic token holding administrative private keys used for Key Escrow Database operations is not left unattended or otherwise open to unauthorized access while it is connected to the KRA Workstation and is in use. This token, when outside of its storage vaults, is under two-person controls and is kept within the KRA Room under the physical controls described in section 5.1.2.

If not in operation, the token is deactivated via a manual logout procedure and stored within its storage vaults as described in section 5.1.2. All storage procedures and mechanisms for the token require two-person or multi-party control.

6.3 Private Key Activation Data

Generation, change, and management of private key activation data is in accordance with FIPS 140-1/2.

Individuals performing functions as a KRA (i.e., an RA Operator) or KRO use Cryptographic Modules and will be required to self-select the activation data in accordance with section 6.4.1 of the IdenTrust ECA CPS.

The Administrative Key token's activation data is contained within an operator key. The operator key and the Cryptographic Module containing the Administrative Key are kept under different KRA control in the KRA room as described in section 6.2.5. When not in use, the operator key and the Cryptographic Module remain stored in separate safes in the same room.

6.4 Computer Security Controls

6.4.1 KED

The IdenTrust's KED is hosted on the same hardware and operating system as the customer database that holds the ECA information. Therefore, section 6.5 and the ECA Technical Specification of the IdenTrust ECA CPS provides a description of the computer security controls in place.

The KRA Workstation performs the KED Key Recovery function as defined in the ECA KRP; remote login to the KRA Workstation is not permitted. Remote login is disabled using the KRA Workstation operating system configuration.

6.4.2 KRA and KRO Workstation

KRA Workstation will use a Windows 7based operating system, with current appropriate security patches maintained, configured in a manner that:

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

When KRA Workstation equipment is hosted on an evaluated platform in support of computer security assurance requirements, then the system (hardware, software, operating system) will be operating in the evaluated configuration. The KRA Workstation will be configured in accordance with the Common Criteria Evaluation and Validation Scheme for Microsoft Windows 2003 Server and Windows 7Workstation and applicable Security Target configuration documentation. During this configuration, the swap space capability is disabled to prevent Decryption Keys from recovery requests from being written to disk.

Reasonable care is taken to prevent malicious software from being loaded on KRA Workstation equipment. Network access is isolated and locked down to only KRA-to-KED functions and host-based intrusion detection. Only applications required for IdenTrust to perform and provide certification services are loaded on the KRA Workstation, and all such software will be obtained from sources authorized by local policy. Data on KRA Workstation equipment will be scanned for malicious code in real time. Since this workstation is not connected to the Internet, the data on the virus definitions files will be updated manually every month or after any major threat is identified. Malicious-code-scanning industry standard antivirus software, is used to scan the KRA Workstation. This software is selected from a list of industry-leading providers and offers frequent updates. For email communication with KROs, KRAs use the same equipment used for the RA client-side function, which is different than the KRA Workstation. KRAs are required to take reasonable care to prevent malicious software from being loaded on their computers through user education coupled with the use of malicious-code-scanning programs, and adhering to the software manufacturer's recommended patches applicable to the installed software. Only applications required to perform the organization's mission will be loaded on the computer, and all such software will be obtained from sources authorized by local policy. Data on the computer is scanned for malicious code on first use and periodically afterward. Equipment updates are purchased or developed in the same manner as original equipment, and are installed by Trusted Role employees and trained personnel in a defined manner. Firewalls are configured to allow access only by the address, ports, protocols, and commands required for the provision of services required by the KRA Workstation. Unused Input/Output ports are locked down.

IdenTrust and Subscribing Organizations are obligated by contract, the ECA KRP, and this KRPS to maintain a KRO workstation that uses an operating system that complies with the five bullet points in the beginning of this section. In addition, the KRO workstation shall make use of strong passwords, secure email, and a personal firewall. The KRO workstation's users and/or administrators shall take reasonable steps to scan for malicious code in real time, maintain malicious-code-scanning data files up-to-date, load only applications required to perform the Organization mission and obtain such software from authorized sources.

6.4.3 Anomaly Detection

Key Recovery (in particular automated Key Recovery) must be carried out with extreme caution, as the chance for compromise can be very high. Further, the risk of compromise and the scope of any potential compromise are highly dependent upon the implementation. IdenTrust will monitor all Key Recovery events and will establish a baseline for each Key Recovery event. All events and behaviors that fall outside the baseline will be reported to IdenTrust's Security Officer and

investigated. A written disposition of the findings will be filed and reported to IdenTrust's Risk Management and Audit Committees. Therefore, the Key Recovery infrastructure will be capable of detecting anomalous Key Recovery activities and behavior and reporting them to IdenTrust's Security Officer for further disposition.

IdenTrust's Security Officer and System Administrators will check the KED, KRA, and application server (i.e., CMC) audit logs referred to in section 4.5.1 for anomalies in support of any suspected violations, and KED, KRA and application server audit logs will be reviewed for events such as repeated failed actions, requests for privileged information, attempted access of system files and unauthenticated responses. IdenTrust Security auditors will check for continuity of the security audit data.

6.5 Life Cycle Technical Controls

Individuals with Trusted Roles in the facility where the KED is kept (e.g., CA administrators, System Administrators, Network Engineers, Security Officers, etc.) will use security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements. These tools and procedures check the integrity of the system data, software, discretionary access controls, audit profile, firmware, and hardware to ensure secure operation. These controls are the same as for the customer database which are described in the ECA Technical Specification and Section 6.6 of the IdenTrust ECA CPS.

IdenTrust hardens the KED and KRA Workstation utilizing industry best practices and IdenTrust-developed checklists prior to deployment. For the KED those controls are explained in the context of the main database in CPS section 6.5. In accordance with IdenTrust's configuration guidelines, in the KRA Workstation, all unused ports, protocols, and services, are disabled. In addition, only the minimum user and system accounts necessary for the functioning of the services provided through the KRA Workstation are enabled.

Trusted Role employees, including the IdenTrust Security Officer and internal IdenTrust security auditors are responsible for securing the KRS in accordance with this KRPS.

6.6 Network Security Controls

Since the KED is integral part of the customer database, network access to the KED is protected as specified in section 6.7 of IdenTrust's CPS.

Network access to the dedicated KRA Workstation is secured by allocating a network segment within the inner tier of the network to service only the KRA Workstation, which inherits the network security controls outlined in Section 6.7 of the IdenTrust's CPS. The KRA Workstation accesses the KED for specified business transactions via encrypted VPN. The encrypted VPN is the only network connection on the KRA Workstation. Logical access will be limited to a "need to have" access basis. Firewalls are configured to allow access only by the addresses, ports, protocols, and commands required for the provision of services required by the workstation. All unused network ports will be turned off. Services are limited to needed business functions only. Any network software present on the workstation will be necessary for performing KRA functions.

6.7 Cryptographic Module Engineering Controls

Requirements for Cryptographic Modules are stated in section 6.2.1.

7 POLICY ADMINISTRATION

7.1 Policy Change Procedures

Changes to this KRPS will be made following the CPS change procedures outlined in IdenTrust's ECA CPS Section 9.12. Modifications to this KRPS will be communicated to the EPMA for approval.

7.2 Publication and Notification Policies

IdenTrust will notify the EPMA of any changes to this KRPS. IdenTrust will also notify the relevant community of participants in the ECA PKI of any changes or modifications to this KRPS by e-mail or other equally-reliable means.

7.3 Policy Approval Procedures

The EPMA may accept, accept with modification, or reject any changes to this KRPS.

Appendix A: Acronyms and Abbreviations

CA: Certification Authority
CMA: Certificate Management Authority
CP: Certificate Policy
CPS: Certification Practices Statement
DES: Data Encryption Standard
ECA: External Certification Authority
EPMA: ECA Policy Management Authority
FIPS: Federal Information Processing Standard
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
PIN: Personal Identification Number
PKCS: Public Key Cryptography Standard
PKI: Public Key Infrastructure
RA: Registration Authority
SHA-1: Secure Hash Algorithm
S/MIME: Secure Multipurpose Internet Mail Extensions
SSL: Secure Sockets Layer

Appendix B: Glossary

The definitions in the ECA CP, IdenTrust ECA CPS, and ECA KRP are incorporated into this KRPS unless the KRPS provides a different definition.

Administrative Keys: The public and private keys are associated to an administrative Certificate. These keys are used to encrypt and decrypt escrowed private keys stored in the KED.

Decryption Key: The private component of an encryption key pair associated with the Encryption Certificate.

Requestor: Individual who are authorized, under the ECA Key Recovery Policy (KRP), to request recovery of Subscriber's escrowed Decryption Keys. These individuals may be: (1) Subscribers that can always request recovery of their own keys. (2) Other employees within the Subscribing Organization, who are authorized based on their internal policies, to request Key Recovery of any Subscriber. (3) Law enforcement personnel who may request Key Recovery by service of a subpoena upon a Subscribing Organization or IdenTrust.

Signature or Signing Key: Private key associated with a Subscriber's Signing Certificate

Subscriber: See IdenTrust ECA CPS section 1.3.3. This term is used in this KRPS to distinguish between the Individual Subscriber and the Subscribing Organization with which the Individual Subscriber is affiliated.

Subscribing Organization: See IdenTrust ECA CPS section 1.3.4.

Appendix C: Letter Agreement: Key Recovery Request

[REQUESTING ORGANIZATION'S LETTERHEAD]

[DATE]

ATTN: ECA KEY RECOVERY REQUESTS
IDENTRUST SERVICES, LLC
5225 WILEY POST WAY
SUITE #450
SALT LAKE CITY, UT 84116

SUBJECT: ECA KEY RECOVERY REQUEST AND ACKNOWLEDGEMENT OF AGREEMENT

TO WHOM IT MAY CONCERN:

I, <Requestor's Name>, declare under penalty of perjury punishable under the provisions 18 U.S.C. § 1621 that I have a legitimate and official need to recover the Decryption Key of the Subscriber identified below in order to obtain (recover) the encrypted data that I have authorization to access. I certify that I have accurately identified myself to [the KRO], and truthfully described all reasons for which I require access to data protected by the key to be recovered, identified below. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to [the KRO] when no longer needed. I understand that I am bound by Subscribing Organization's policies, applicable laws and Federal regulations concerning disclosure of key recovery to the Subscriber and the protection of the recovered key and any data recovered using the key.

REQUESTOR'S IDENTITY INFORMATION (Requestor's Use)

First Name: _____ **Middle Initials:**

Last Name: _____

Address: _____

Telephone (Ext): _____ **E-mail:** _____

Job Title: _____

Organization: _____

REQUESTOR'S IDENTITY INFORMATION (Key Recovery Officer's Use)

NOTE: *Process this section in person if Requestor cannot submit digitally signed request*

(1) ONE FEDERALLY-issued photo ID:

_____ _____ _____ _____
Exact Name Listed on Photo ID | Identification Number | Expiration Date | Identification Type

_____ _____
Date of Issuance | Issuing Authority

(2) If photo ID (1) does not have a serial number, a STATE-issued photo ID with serial number is required:

_____

Exact Name Listed on Photo ID	Identification Number	Expiration Date	Identification Type

Date of Issuance	Issuing Authority

Requestor's Signature and Date: _____ _____

(Sign only in the presence of the Key Recovery Officer) (Date)

CERTIFICATE AND SUBSCRIBER'S INFORMATION (Requestor's Use)

Subscriber Full Name:
NOTE: Leave blank if Requestor is the Subscriber _____

Email:
NOTE: Leave blank if Requestor is the Subscriber _____

Subscribing Organization Name
NOTE: Leave blank if Requestor is the Subscriber _____

Certificate's Use Date and Serial Number _____

Reason for Key Recovery Request:

- ☐ Private Key Lost, Damaged or Inaccessible
- ☐ Need to Decrypt Information
- ☐ Subscriber is unavailable (no longer working for or affiliated with OPDIV)
- ☐ Other: _____

REQUEST APPROVAL INFORMATION (Key Recovery Officer's Use)

Service Request is:

☐ Approved

☐ Rejected (Provide Reason): _____

Key Recovery Officer Performed Identity and Authority Verification

☐ Yes ☐ No

Key Recovery Officer's Name	Signature	Date

Sincerely,

Authorized Requestor for Key Recovery

Appendix D: Key Recovery Officer Addendum to Subscribing Organization Authorization Agreement

Subscribing Organization hereby recommends that the Candidate identified below ("Candidate") be appointed to the role of Key Recovery Officer in the Department of Defense External Certification Authority program conducted by IdenTrust Services, LLC. ("IdenTrust") and, by signing where indicated below, Candidate pledges to fulfill the responsibilities of that role, as summarized below. If approved by IdenTrust, Candidate will assist IdenTrust in performing such identity verification tasks as may be required by the terms of the Key Recovery Policy for External Certification Authorities ("KRP") published by the United States Department of Defense ("DoD") and IdenTrust's Key Recovery Practices Statement ("KRPS").

Candidate confirms that he or she has read the relevant provisions of the ECA KRP and KRPS, and applicable provisions of the Certification Practices Statement understands, and will fully and faithfully discharge, his or her obligations as described in those documents and summarized below.

As a Key Recovery Officer, I, Candidate, will be performing a key role in the identification and authentication of Requestors for ECA Decryption Keys. In the capacity as a Key Recovery Officer, I agree to do the following:

1. Conform to the ECA KRP and KRPS in providing services as a Key Recovery Officer under the IdenTrust ECA Program.
2. Follow IdenTrust's instructions relative to the services I perform for IdenTrust.
3. Inform myself of my responsibilities as a Key Recovery Officer by reading and following all written instructions and any training materials provided by IdenTrust.
4. Ensure that each Requestor receives and signs an acknowledgment of agreement for key recovery, i.e. a Letter Agreement: Key Recovery Request. This form contains statements by the Requestor acknowledging the responsibility to follow policies of IdenTrust and Subscribing Organization governing recovered DecryptionKeys.
5. Ensure that each Requestor provides all required evidence of identity and authorization and presents the required identification credentials to me for inspection.
6. Contact IdenTrust at ecaservices@identrust.com or 1-888-882-1104 (U.S.) or 1-801-924-8141 (International) with any questions I may have.

_____ _____ _____

Key Recovery Officer Candidate Signature: Print Name: Date:

Telephone Number: (_____)_____ E-Mail Address: _____

Agreement by Subscribing Organization

1. Subscribing Organization hereby confirms that Candidate named above is an employee of Subscribing Organization and appoints and authorizes Candidate to fulfill all the responsibilities of a Key Recovery Officer on behalf of Subscribing Organization, as prescribed above and in the ECA KRP and KRPS.
2. Subscribing Organization warrants that, in the event it ever concludes that Candidate has breached Subscribing Organization's own key recovery policies, any term of this Agreement, or any applicable requirement of the ECA KRP or KRPS, Subscribing Organization will immediately revoke Candidate's authorization to act as a Key Recovery Officer, notify IdenTrust, and commence any other administrative or disciplinary actions that it deems appropriate considering the circumstances.
3. Subscribing Organization undertakes to manage its key recovery operations in accordance with the ECA KRP and KRPS, to maintain and protect key recovery records, and to supervise Candidate in connection with his or her responsibilities in the role of Key Recovery Officer and ensure that there will be no conflict between Candidate's duties as an employee of Subscribing Organization and duties as a Key Recovery Officer (KRO). Subscribing Organization agrees to maintain the security of the KRO workstation by requiring the use of strong passwords, taking reasonable steps to scan for malicious code in real time, using secure email, maintaining a software firewall on the workstation, keeping antivirus data files and other software up-to-date, loading only applications required to perform the Organization mission and obtaining such software from authorized sources. If Subscribing Organization becomes aware of a compromise in the security of KRO's workstation adversely

affecting key recovery activities, Subscribing Organization agrees to stop the operation of the workstation and start an investigation into the extent of the compromise per established incident response procedures. Subscribing Organization agrees that, if requested by IdenTrust at any time, it will immediately revoke the authorization of Candidate to act as a Key Recovery Officer, and promptly appoint a new individual to serve as a Key Recovery Officer.

4. Subscribing Organization agrees to notify IdenTrust in the event that a Key Recovery Officer is no longer authorized to act as a Key Recovery Officer.

5. Subscribing Organization acknowledges that it has an obligation to include the KRO Workstation and Key Recovery operations in its periodic internal security audits, which shall occur on at least an annual basis. Subscribing Organization shall report the results of the annual, key-recovery security audit to an individual within the Organization designated to receive such reports and to IdenTrust on an annual basis. In the event that Candidate is relieved of that responsibility due to failure to comply with the ECA KRP or KRPS, then IdenTrust may direct that a special audit be conducted to determine whether any activities of the Candidate have been improper or adversely affected the integrity of the Key Recovery System and IdenTrust may report the results of such audit to the DOD ECA Policy Management Authority.

6. In the event that IdenTrust may determine, in its reasonable sole discretion, that the Candidate has breached any of the applicable terms of his or her agreement above, the KRP, or the KRPS, or that Subscribing Organization has breached any of the applicable terms of this Agreement or the KRP or the KRPS, then IdenTrust may revoke any or all of Subscribing Organization's ECA Certificates.

7. In consideration of IdenTrust's appointment, Subscribing Organization hereby agrees to indemnify and hold IdenTrust, its parent company, and the officers, directors, employees and agents of either of them harmless from and against any loss, cost, damage, liability or expense any of the foregoing may incur or be liable for, including reasonable attorneys' fees and expenses, arising out of this appointment; any act or omission of Candidate in the capacity as a Key Recovery Officer; or any act or omission of Subscribing Organization in connection with the ECA Program or any key recovered as a result of Key Recovery Officer's actions. If Subscribing Organization is the U.S. Government, this provision may not apply.

Organization Officer Sign Here: _____

Print Name: _____

Telephone Number: (_____)_____

E-Mail Address: _____

_____ _____ _____

Organization Officer Signature: Print Name: Date:

Telephone Number: (_____)_____ E-Mail Address: _____

Appointment by IdenTrust: The individual named above is hereby appointed to serve as a Key Recovery Officer.

IdenTrust Services, LLC, by:

_____ _____ _____

IdenTrust Officer Signature: Print Name: Date:

Note: The above nomination by the Subscribing Organization of the individual named above to serve as a Key Recovery Officer in the IdenTrust ECA program must be accepted in writing by IdenTrust within thirty (30) days after the later of the date of signature by the individual or the Subscribing Organization shown above, or such nomination shall be deemed rejected, and the Subscribing Organization must nominate another individual to the role, or may renominate the original individual, provided that any circumstance which prevented IdenTrust from accepting the original nomination shall have been remedied to the satisfaction of IdenTrust.

Appendix E: Subscriber Agreement

See IdenTrust ECA CPS

Appendix F: Key Recovery Agent Authorization Agreement

The Candidate identified below ("Candidate") will be appointed to the role of Key Recovery Agent ("KRA") in the Department of Defense External Certification Authority ("ECA") program conducted by IdenTrust Services, LLC. ("IdenTrust") and, by signing where indicated below, Candidate pledges to fulfill the responsibilities of that role, as summarized below. If approved by IdenTrust, Candidate will assist IdenTrust in performing such key recovery tasks as may be required by the terms of the Key Recovery Policy for ECAs ("KRP") and IdenTrust's ECA Key Recovery Practices Statement ("KRPS").

Candidate confirms that he or she has been given and has read a copy of the KRP and KRPS, and applicable provisions of the CPS and understands, and will fully and faithfully discharge, his or her obligations as described in those documents and summarized below.

As a Key Recovery Agent, I, Candidate, will be performing a key role in the key recovery process for ECA Decryption Keys. In the capacity as a Key Recovery Agent, I agree to do the following:

1. Inform myself of my responsibilities as a KRA by reading and following all written instructions and any training materials provided to me by IdenTrust.
2. Follow IdenTrust's instructions and conform to the ECA KRP and KRPS in providing KRA services.
3. Protect all information regarding all occurrences of key recovery.
4. Maintain and observe multi-person control over the administrative private key used to perform key recoveries.
5. Ensure that each request for key recovery includes a signed acknowledgment of agreement for key recovery, i.e. a Letter Agreement: Key Recovery Request.
6. Authenticate the identity of the Requestor when the Requestor makes an electronic request that is digitally signed.
7. Ensure that any Key Recovery Officer (KRO) submitting a request is an authorized KRO for the Subscriber whose key has been requested to be recovered.
8. Request additional information or confirmation from the KRO if deemed necessary.
9. Ensure that all required documentation has been submitted and is complete.
10. Release Subscriber's escrowed keys only for properly authenticated and authorized requests from Requestors.
11. Protect Subscribers' recovered private keys from unauthorized disclosure, including the encrypted files and associated DecryptionKkeys, including protecting the RSA PKCS#12 files, P12 passwords, cryptographic tokens and protecting passwords and send them securely only to authorized Requestors.
12. Communicate knowledge of a recovery process only to the KRO and Requestor involved in the key recovery, and not communicate any information concerning a key recovery to the Subscriber except when the Subscriber is the Requestor.
13. Report anomalous activity or breaches of proper key recovery protocols.
14. Discuss with my supervisor any questions I may have.

KRA Candidate Signature:	Print Name:	Date:

Appointment by IdenTrust: The individual named above is hereby appointed to serve as a Key Recovery Agent.

IdenTrust Services, LLC, by:

IdenTrust Officer Signature:	Print Name:	Date:

Appendix G: ECA Technical Specification Document

[Redacted]

Appendix H: References

[ECA KRP]: United States Department of Defense Key Recovery Policy for External Certification Authorities, Version 1.0 (dated 06/04/2003). Available online

[IdenTrust ECA CPS]: IdenTrust Certification Practice Statement, Version 1.1 (dated 08/27/2008). Available online