COMMON Certificate Policy Change Proposal Number: 2024-07

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Trusted Agent and Key Recovery Role Clarifications
Date: October 10, 2024

Title: Trusted Agent and Key Recovery Role/Responsibility Clarifications

X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.8 May 3, 2024

Change Advocate's Contact Information: fpki@gsa.gov

Organization requesting change: CPWG

Change summary: Clarify the description of the trusted agent role in order to ensure that it is not confused with a standard trusted roles and thus does not require an equivalent background investigation.

Additionally, clarify seemingly conflicting policy language regarding Key Recovery Officials (KROs) and Third Party Key Recovery Requestors to include their responsibilities.

Background:

The CPWG was engaged by independent auditors regarding potential equivalence between RAs and trusted agents. This confusion may result in implementers making an incorrect assumption that trusted agents are officers and require background checks as described in Section 5.3.2, a distinction that has been more concrete in the FBCA CP.

The FPKIPA support team received questions from community members regarding seemingly contradictory policy language about KRO access to the KED as well as clarity regarding responsibilities of third-party key recovery requestors and their handling of recovered keying materials.

The proposed changes clarify TA requirements and the KRO role functions. Additionally, verbiage in Section 9.6.5 has been updated to specifically call out third-party key recovery requestors in alignment with the requirements of the entire section and to differentiate from requirements of subscribers themselves or their leadership when conducting key recovery.

Specific Changes:

Insertions are underlined, deletions are in ~~strikethrough~~:

1.3.3 Registration Authorities

A Registration Authority (RA) is an entity authorized by the CA to collect, verify, and submit information provided by potential Subscribers for the purpose of issuing public key certificates. The term RA refers to hardware, software, and individuals that may collectively perform this function. Individuals fulfilling the RA function are acting in a Trusted Role, and are considered Officers as defined in Section 5.2.1. The RA is responsible for:

- Control over the registration process.
- The identification and authentication process.

~~A Trusted Agent is a person who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA.~~ A Trusted Agent is authorized by a PKI to act on its behalf and may record~~s~~ information from and verify~~ies~~ biometrics (e.g., photographs) on presented credentials on behalf of an RA for Applicants who cannot appear before ~~in person at~~ an RA. Trusted Agents are not Trusted Roles; however, the PKI must document any Trusted Agent authorization requirements to include:

- trustworthiness vetting, and
- training or government appointment (e.g., notary public).

All identity proofing audit artifacts produced by a Trusted Agent must be traceable to an individual.

1.3.4 Key Recovery Authorities

For organizations that have implemented Key Recovery, the applicable requirements for physical, personnel, and procedural security controls, technical security controls, and Compliance Audit are applied as follows:

- CA requirements are applied to the KED and to the DDS
- RA requirements are applied to the Key Recovery Agent (KRA) and KRA automated systems
- ~~RA requirements are applied to the KRO and KRO automated systems, when the KRO has privileged access to the KED~~

1.3.4.3. Key Recovery Agent

A KRA is an individual who is authorized, as specified in the applicable Practice Statement (KRPS or CPS), to recover an escrowed key. ~~The KRAs send the recovered key to the KRO or directly to the Requestor.~~ The KRAs have high level, sensitive access to the KED and are considered Trusted Roles (see Section 5.2.1). KRAs can recover large numbers of keys, the number and location of KRAs should be closely controlled.

A KRA performs the following functions:

- Confirm validity and completeness of requests,
- Recover copies of escrowed keys; and
- Distribute copies of recovered keys to Requestor, with protection as described in Section 4.12.1.3.

KRAs may ~~additionally~~ conduct requestor identity verification and authorization validation when KROs are not used.

1.3.4.4. Key Recovery Official

Organizations may opt to appoint a Key Recovery Official (KRO) ~~may optionally be used~~ to support key recovery requestor identity verification and authorization validation tasks~~. KROs do not have privileged access to the KED.~~; however, a KRO is not a Trusted Role.

A KRO's responsibilities are to perform the following functions:

- Verify a Requestor's identity and authorization as stated by this policy;
- Assist authorized requestors in building key recovery requests;
- Utilize secure communication for key recovery requests to and responses from the KRA; and
- Participate in the distribution of escrowed keys to the Requestor, ensuring that it occurs as described by the associated practice statement (CPS or KRPS).

Practice Note: The responsibilities of the Key Recovery Official do not require access to the KED and as a result the KRO is not considered a Trusted Role. However, organizations may assign multiple responsibilities to one person due to resource constraints. In scenarios where Trusted Roles may also be assigned to perform the

duties of the KRO, the requirements for Separation of Duties per Section 5.2.4 must be enforced.

4.12.1.3 Key Recovery Through KRA

The KRA must provide access to a copy of an escrowed key only in response to a properly authenticated and authorized key recovery request. Such access requires the actions of at least two KRAs. All copies of escrowed keys must be protected using two-person control procedures during recovery and delivery to the authenticated and authorized Requestor. Split key or password procedures are considered adequate two-person controls, provided they comply with technical controls in Section 6.2.2.

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

The KRA is not required to notify subscribers of a third-party key recovery.

Practice Note: Subscriber notification of key management key recovery is not necessary and may be prohibited in certain use cases (e.g., Counterintelligence or Law Enforcement investigations).

5.2.1 Trusted Roles

The requirements of this policy are defined in terms of four roles, implementing organizations may define additional roles provided the following separation of duties are enforced.

1. Administrator – authorized to install, configure, and maintain the CA, KED or DDS; establish and maintain system accounts; configure audit parameters; and generate PKI component keys.
2. Officer – authorized to request, ~~or~~ approve, or perform certificate issuance, revocations, or key recovery, as appropriate.
3. Auditor – authorized to review, maintain, and archive audit logs.
4. Operator – authorized to perform system backup and recovery.

~~5.2.1.1. Key Recovery Agent (KRA)~~

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

- ~~Authorized to authenticate requests and recover copies of escrowed keys; and~~
- ~~Authorized to distribute copies of recovered keys to Requestor, with protection as described in Section 4.12.1.2.1.~~

~~5.2.1.2. Key Recovery Official (KRO)~~

~~KROs are defined as Trusted Roles only if they have privileged access to the KED.~~

~~A KRO's responsibilities are to ensure that the following functions occur according to the stipulations of this policy:~~

- ~~Authorized to verify a Requestor's identity and authorization as stated by this policy;~~
- ~~Authorized to build key recovery requests on behalf of authorized Requestor;~~
- ~~Authorized to securely communicate key recovery requests to and responses from the KRA; and~~
- ~~Authorized to participate in distribution of escrowed keys to the Requestor, as described by the associated practice statement (CPS or KRPS).~~

5.5.1. Types of Events Archived

CA archive records must be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data must be recorded for archive:

…

- Record of an individual being added or removed from a trusted role, and who added or removed them from the role
- Evidence of qualification for Trusted Agents and the associated validity period(s) for which they are authorized to act as Trusted Agents

9.6.5. Representations and Warranties of Other Participants

Third-party key recovery Requestors must formally acknowledge and agree to the obligations described here, prior to receiving a recovered key:

- The Third-Party Requestor must protect Subscribers' recovered key(s) from compromise. The Third-Party Requestor must use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their keys and recovered Subscribers' keys.
- The Third-Party Requestor must destroy or surrender Subscribers' keys when no longer required (i.e., when the data has been recovered).

- The Third-Party Requestor must request and use the Subscriber's escrowed key(s) only to recover Subscriber's data they are authorized to access.
- The Third-Party Requestor must accurately represent themselves to all entities during any key recovery service.
- When the request is made, the Third-Party Requestor must provide accurate identification and authentication information at least to the same level required for issuing new PKI certificates at the level of the key being requested (e.g., the Third-Party Requestor sends a digitally signed request using the credential issued by the Entity PKI at the same or higher assurance level as the key being recovered).
- The Third-Party Requestor must protect information concerning each key recovery operation.
- ~~The Third-Party Requestor must communicate information concerning the recovery to the Subscriber when appropriate as determined by the reason for the recovery. The decision to notify the Subscriber must be based on the law and the Issuing Organization's policies and procedures for third party information access.~~
- ~~In the event that the Third-Party Requestor notifies the Subscriber of a key recovery, the Third-Party Requestor must consult with the Subscriber to determine whether or not the recovery circumstances warrant revoking the associated public key certificate.~~
- ~~As a condition of receiving a recovered key, a Third-Party Requestor must agree to follow the law and the Issuing Organization's policies relating to protection and release of the recovered key.~~
- Upon receipt of the recovered key(s), the Third-Party Requestor must sign an ~~attestation to the effect~~ acknowledgement of agreement to follow the law and the subscriber's organization policies relating to protection and release of the recovered key. Such agreement should include the following attestations:
    - Third Party Requestor has accurately represented their identity to all key recovery entities,
    - Third Party Requestor has truthfully described the reason(s) for the key recovery request,
    - Third Party Requestor has a legitimate and official need to obtain the requested key(s),
    - Third Party Requestor has received the recovered key(s),
    - Third Party Requestor will use the recovered key(s) only for the stated purpose(s),
    - Third Party Requestor will protect the recovered key(s) from unauthorized access. When no longer required, the Third Party Requestor shall either destroy the key(s) and inform the organization of destruction per agency requirements, or return any recovered key(s) stored on hardware to the organization,
    - Third Party Requestor is bound by applicable laws and regulations concerning the protection of the recovered key(s) and any data recovered using the key(s).

~~"I hereby state that I have legitimate and official need to recover this key in order to obtain (recover) the encrypted data that I have authorization to access. I acknowledge receipt of a recovered encryption key associated with the Subscriber identified here [Subscriber Name]. I certify that I have~~

~~accurately identified myself to the KRO, and truthfully described all reasons that I require access to data protected by the recovered key. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to the KRO when no longer needed. I understand that I am bound by [Issuing Organization] policies, applicable laws and Federal regulations concerning the protection of the recovered key and any data recovered using the key."~~

Estimated Cost: None

Implementation Date: Immediate upon publication

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	February 27, 2024
Date change released for comment:	March 20, 2024
Date comment adjudication published:	September 27, 2024