October 2022

From: Matt Arnold and Tim Baldridge
Federal PKI Policy Authority Co-Chairs

To: Federal Public Key Infrastructure Policy Authority Members

Subject: Clarifications Regarding Registration Authority Audits

This memorandum provides clarification of the responsibilities for Registration Authorities with regard to FPKI affiliate annual audits.

Common Terminology and Critical Definitions

The following definition is provided as context for this document:

- As defined in the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [COMMON]*, a Registration Authority (RA) is an entity authorized by the Certification Authority (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.
- *Special Publication 800-79-2, Guidelines for the Authorization of PIV Card Issuers and Derived PIV Credential* Issuers, defines an "Issuing Facility" as a physical site or location – including all equipment, staff, and documentation – that is responsible for carrying out one or more of the following PIV functions: (i) identity proofing/registration; (ii) card/token production; (iii) activation/issuance; and (iv) maintenance. An issuing facility operates under the auspices of a PIV Card or Derived PIV Credential Issuer, and implements the policies and executes procedures prescribed by the issuer for those functions sanctioned for the facility (e.g., an identity proofing/registration facility).
- The term "Registration Authority" is not used in NIST 800-79-2, but the RA functions described in [COMMON] incorporate the following functions defined in SP 800-79:
  - identity proofing/registration;
  - card/token production;
  - activation/issuance; and
  - PIV maintenance.

Background

CAs that participate in the FPKI community are required to receive an annual audit, and to share the results of that audit with the FPKI Policy Authority (FPKIPA), in order to remain in good standing with the FPKI community. The scope of the annual audit includes "[a]ll aspects of the CA/RA operation."

While CAs are ultimately responsible for submitting the review package, RAs are subject to the compliance audit requirements and must ensure that a compliance audit is performed and the results of the audit submitted to the FPKIPA along with the rest of the annual review package.

Within the context of PIV issuance, issuers are also subject to the requirements of NIST SP 800-79-2, and must obtain the appropriate Authority to Operate (ATO). As a condition of maintaining their ATO, PIV issuing agencies are further required to perform an annual lifecycle walkthrough and submit the results and any findings and recommendations to the Designated Authorizing Official (DAO). While the SP 800-79 ATO/annual walkthrough does not completely address the requirements for RAs defined in [COMMON], a management attestation (see Appendix A) based on the verification of appropriate controls from an agency authority will suffice to address the gaps between SP 800-79 and [COMMON] (see Appendix B).

Guidance for Registration Authorities

Every agency managing RAs that verify certificate contents and submit Certificate Signing Requests (CSRs) to a CA for the purpose of issuing certificates to agency personnel, must submit supporting audit documentation on an annual basis to their CAs, for inclusion in the CA's annual review package. The Registration Authority Agreement (RAA[1]) or other binding legal agreement between the CA and RA (e.g., established contracts) should specify the responsibilities for the audits that support the annual package, which should include at least the following elements.

The documentation provided by a RA may be either:

a) An audit of the RA's practices against the relevant CPS or RPS, or
b) A copy of an ATO letter provided under the requirements of SP 800-79, together with an attestation letter (see Appendix A) signed by an agency authority that the agency complies with the Key Recovery, if applicable, and audit and archive requirements of the relevant CPS.

Conclusions

- CAs are responsible for submitting audits for all elements of their PKI services, including RA functions
- Independently operated RAs are responsible for ensuring that their assigned services and responsibilities are documented, and any resulting audits are shared with their CA
- RAs that support issuance of PIV certificates (potentially in addition to other certificate types) may submit the following artifacts to their CAs for inclusion into the supporting FPKI annual review package:
    - RAs that complete the annual lifecycle walkthrough required by SP 800-79 for PIV and maintain an ATO may submit their ATO in lieu of a full audit package.
    - A letter from an agency authority attesting that they manage the elements not covered by the SP 800-79 ATO (Audit, Archive, Key Recovery) and, if applicable, that any additional certificates authorized by the RAs follow similar procedures
- All other RAs that **<u>do not</u>** issue PIV must submit a complete audit of their RA practices against the relevant CP/CPS.

[1] A generic RAA template is available at: https://www.idmanagement.gov/docs/fpki-ssp-raa.docx

Appendix A: Attestation Letter Checklist

The following elements must be contained in any Attestation Letter provided by agencies in lieu of an auditor's opinion letter:

Category	Requirement	Description
General	Signature	The attestation letter must be addressed to the Federal PKI PA and must be signed by an agency authority. Note - due to historical separation of oversight roles (e.g., key recovery officers vs RA officers) the agency must determine the appropriate authority for accepting the liability associated with this attestation.
Authority Information	Identity	Identity of the agency authority and the entities reviewing the controls.
Review Scope	Date Performed	The date the review was performed.
	Period of Performance	The period of performance the walkthrough covers.
	PKI Components in Scope	Which entity RA/Issuing Facility component(s) were audited (RAs).
	Documents Reviewed	Which documents were reviewed as a part of the audit, including document dates and version numbers. If portions of the PKI Policy are documented separately from the CP (e.g. a separate Key Recovery Policy & Practice Statement) these documents must also be reviewed as part of the audit.
Review Results	Statements concerning the Audit	A statement that the operations of the audited component(s) were evaluated for conformance to the requirements documented below.
	Findings	Report any and all findings related to the evaluation of the operational conformance of the audited component(s) to the requirements
	Closure of Previous Audit Cycle Findings	If applicable (always applicable if there were any findings reported the previous year), state that any findings from the previous audit were reviewed for closure.
	Opinion	Provide an opinion concerning the sufficiency of the RA/Issuing Facility operational compliance in relation to the SP 800-79/Common Policy or the applicable CPS/RPS.

Appendix B: Audit, Archive and Key Recovery controls not included in an 800-79 assessment or Annual Walkthroughs

Special Publication 800-79 identifies a set of controls against which a Federal organization's PIV issuance processes must be evaluated. Successful completion of this evaluation results in Authority to Operate and satisfies the requirement in HSPD-12 that a PIV credential *is issued only by providers whose reliability has been established by an official accreditation process.*

The Federal COMMON Policy Framework CP [COMMON], written in RFC 3647 format, establishes specific requirements for the identity proofing and issuance processes utilized in the issuance of digital certificates. [COMMON] bases its identity proofing and issuance requirements for PIV on FIPS 201 and established best practices for the issuance of digital certificates.

The FPKIPA requests NIST consider the following new language and controls to SP 800-79 certification the inclusion of which would obviate the requirement to conduct a COMMON-compliant PKI Third-party Audit Assessment of the Registration Authority for those organizations with SP 800-79 certification.

1. Audit and Archive Controls:
    a. Appendix D.1, Section X – Modify as follows:

PCI Issuance Information System (s) Description *<Provide a description of the technical aspects of the organization's PIV issuance system, including system architecture, network connectivity, connections to external system and information shared both internally and externally, the PKI provider as well as the information system authorization status. >*

a. Architecture
b. Interconnections and Information Sharing
c. Information System Inventory
d. Public Key Infrastructure
e. SP 800-37-1 A&A Information
f. Audit Record Review and Archive

    b. Appendix D.2, Section X – Modify as follows:

DPCI Issuance System (s) Description *<Provide a description of the technical aspects of the organization's PIV issuance system, including system architecture, network connectivity, connections to external system and information shared both internally and externally, the PKI provider as well as the information system authorization status. >*

a. Architecture
b. Interconnections and Information Sharing
c. Information System Inventory
d. Public Key Infrastructure
e. SP 800-37-1 A&A Information
f. Linkage between the PIV Card and the Derived PIV Credential
g. Audit Record Review and Archive

Appendix G, Table G.1, Preparation and Maintenance of Documentation (DO) add the following Control

Preparation and Maintenance of Documentation	DO-9	The organization has a written policy and procedure for archiving required audit logs and archive records according to a records retention schedule. **Assessment** *Determine that:* *(i) the organization has developed and documented a written policy and procedures for which audit logs are archived* *(ii) the organization has developed and documented a written policy and procedures for which archive records are destroyed* *(iii) the organization has developed and documented a records retention schedule*	FIPS 201-3 Section 2.6 – PIV Enrollment Records Federal Common Policy Framework Certificate Policy Section 5.4 (and subsections) – Audit Logging Procedures and Section 5.5 (and subsections) – Record Archival.

Appendix G, Table G.1, Maintenance Process (MP) add the following Control

Maintenance Process	MP-16	Audit records must be generated for all identity proofing, verification and issuance activities. Where possible, audit records must be automatically generated. Records should be reviewed on a monthly basis by a qualified IT security specialist. Such reviews should look for anomalous behavior in the identity proofing and enrollment systems. Audit records are archived for as long as required by policy (NARA GRS 5.6). **Assessment** *Determine that:* *(iv) audit records are available for all identity proofing, verification and issuance activities* *(v) audit records have been reviewed as required and all anomalous events identified and investigated.* ***(vi)*** *audit records are archived per NARA GRS 5.6, and maintained according to an established records retention schedule.*	FIPS 201-3 Section 2.6 – PIV Enrollment Records Federal Common Policy Framework Certificate Policy Section 5.4 (and subsections) – Audit Logging Procedures and Section 5.5 (and subsections) – Record Archival.

c. Appendix G, Table G.2, Maintenance Process (MP) add the following Control

Maintenance Process	MP(DC)-19	Audit records must be generated for all Derived PIV issuance activities. Where possible, audit records must be automatically generated. Records should be reviewed on a monthly basis by a qualified IT security specialist. Such reviews should look for anomalous behavior in the Derived PIV issuance systems. Audit records are archived for as long as required by policy (NARA GRS 5.6). **Assessment** *Determine that:* *(i) audit records are available for all issuance activities* *(ii) audit records have been reviewed as required and all anomalous events identified and investigated.* *(iii) audit records are archived per NARA GRS 5.6.*	FIPS 201-3 Section 2.6 – PIV Enrollment Records Federal Common Policy Framework Certificate Policy Section 5.4 (and subsections) – Audit Logging Procedures and Section 5.5 (and subsections) – Record Archival.

2. Key Escrow and Recovery Controls
   a. Appendix D.1, Section VII - Modify as follows:

Issuing Facility Details

<Identify all the issuing facilities that are included and are part of the authorization boundary. Provide details such as the location, PIV Card Process performed (e.g. registration) at the facility and the approximate number of PIV Cards personalized at each facility. Indicate whether the issuing facility also manages a key escrow and recovery system for the key management keys associated with the PIV Card. >

b. Appendix D.1, Section IX - Modify as follows:

PCI Policies and Procedures

<Describe in this section the various policies and procedures that apply for (i) sponsorship, (ii) identity proofing / registration, (iii)adjudication, (iv) card production, (v) activation and issuance and (vi) maintenance for PIV Cards. Where applicable, discuss the procedures for key escrow and recovery. Also discuss the procedures for temporary badges, as well as for non-PIV badges employed by the organization. >

a. Sponsorship

b. Identity Proofing and Registration

c. Adjudication

d. Card Production

e. Activation/Issuance

f. Key Escrow (if applicable)

~~f~~. g. Maintenance

  i. Re-issuance

  ii. Post-issuance updates

  iii. Key recovery (if applicable)

  ~~iii~~. iv Termination

b. Temporary/Non-PIV Badges

c. Appendix D.2. Section VII – Modify as follows:

Issuing Facility Details

<If applicable, identify all the Issuing facilities that are included and are part of the authorization boundary. Provide details such as the location, Derived PIV Credential functions performed at the facility and the types and approximate number of Derived PIV Credentials personalized at each facility. If issuance is conducted entirely remotely, indicate this within VI. Indicate whether the issuing facility also manages a key escrow and recovery system for key management keys associated with the DPIV credential. >

d. Appendix D.2. Section IX – Modify as follows:

DPCI Policies and Procedures

<Describe in this section the various policies and procedures that apply for (i) sponsorship, (ii) token production and (ii) activation and issuance, and (iv) maintenance for Derived PIV Credentials.

  a. Sponsorship

  b. Token Production

  c. Activation/Issuance

  d. Key Escrow (if applicable)

  ~~d~~.e. Maintenance

    i. Re-issuance

    ii. Post-issuance updates

    iii Key Recovery (if applicable)

    ~~iii~~. iv. Termination

e. Appendix G, Table G.1, Preparation and Maintenance of Documentation (DO) add the following Control

Preparation and Maintenance of Documentation	DO-9	For organizations that maintain a key escrow and recovery system in conjunction with the PIV Issuance system, the organization has a written policy and procedures for key escrow and recovery that are approved by the head or deputy secretary (or equivalent) of the Federal department or agency. **Assessment** *Determine that:* *(i) The organization has developed and documented written policy and procedures for key escrow and recovery for key management keys associated with PIV Cards. (review)* *(ii) The policy is consistent with the organizations mission and functions, and applicable laws, directives, policies, regulations, standards and guidance (review).* ***(iii)** The policy and procedures have been signed off by the head or deputy secretary (or equivalent) of the Federal department or agency (review).* ***(iv)** The organization will periodically review and update the policy and procedures as required (review, interview).*	FIPS 201-3 Section 5.2 – PKI Certificate Federal Common Policy Framework Certificate Policy Section 4.12 (and subsections) – Key Escrow and Recovery

f. Appendix G, Table G.1, Assignment of Roles and Responsibilities (RR) add the following Control

Assignment of Roles and Responsibilities	RR-7	For organizations that maintain a key escrow and recovery system in conjunction with the PIV Issuance system, the organization has appointed the role of Third-Party Key Recovery Request Approver. **Assessment** *Determine that:* *(i) The organization has defined the role of Third-Party Key Recovery Request Approver and its responsibilities (review)* *(ii) The organization has assigned the role of Third-Party Key Recovery Request Approver (review).*	FIPS 201-3 Section 5.2 – PKI Certificate Federal Common Policy Framework Certificate Policy Section 4.12.1.8 Requestor Authorization Validation

g. Appendix G, Table G.1, Facility and Personnel Readiness (FP), add the following:

Facility and Personnel Readiness	FP-10	For organizations that maintain a key escrow and recovery system in conjunction with the PIV Issuance system, all operators who perform duties associated with key escrow and recovery are allowed access to the Key Escrow Database only when authenticated through a PIV Card. At least two operators are required to recover an escrowed key management key. **Assessment** *Determine that:* *(i) The requirement that all operators who perform roles within the key escrow and recovery system are allowed logical access to escrowed keys only when authenticated through a PIV Card has been documented in the issuing facility's standard operating procedures. (review)* *(ii) Operators use PIV cards to access key recovery systems in the course of performing*	FIPS 201-3 Section 5.2 – PKI Certificate Federal Common Policy Framework Certificate Policy Section 4.12 (and subsections) – Key Escrow and Recovery

		their roles within the Key escrow and Recovery Systems (review). *(iii) All operators who perform roles within the key escrow and recovery system are allowed access to escrowed keys only after completing a training course specific to their duties (interview, review).* *(iv) Records showing that the appropriate training course has been completed by key recovery personnel are stored y the facility for audit purposes (interview, review).*	

h. Appendix G, Table G.1, Implementation of Credentialing Infrastructures (CI), add the following control:

Implementation of Credentialing Infrastructures	CI-	For organizations that maintain a key escrow and recovery system in conjunction with the PIV Issuance system, all key management private keys are escrowed. **Assessment** *Determine that:* *(i) The key escrow database is operational and copies of key management private keys are automatically stored when key management certificates are generated (review, test).*	FIPS 201-3 Section 5.2 – PKI Certificate Federal Common Policy Framework Certificate Policy Section 4.12 1 – Key Escrow and Recovery Policy and Practices

i. Appendix G, Table G.1 Sponsorship Process (SP), add the following:

Sponsorship Process	SP-3	For organizations that maintain a key escrow and recovery system in conjunction with the PIV Issuance system, keys are recovered only upon request by proper authority. **Assessment** *Determine that:* *(i) The process for making a request is documented (review)* *(ii) A request from a valid authority is required to recover an escrowed private key management key.*	FIPS 201-3 Section 5.2 – PKI Certificate Federal Common Policy Framework Certificate Policy Section 4.12.1.8 – Requestor Authorization Validation

j. Appendix G, Table G.2, Preparation and Maintenance of Documentation (DO(DC)) add the following Control

Preparation and Maintenance of Documentation	DO(DC)-7	For organizations that maintain a key escrow and recovery system in conjunction with the DPIV Issuance system, the organization has a written policy and procedures for key escrow and recovery that are approved by the head or deputy secretary (or equivalent) of the Federal department or agency. **Assessment** *Determine that:* *(i) The organization has developed and documented written policy and procedures for key escrow and recovery for key management keys associated with DPIV credentials. (review)* *(ii) The policy is consistent with the organization's mission and functions, and applicable laws, directives, policies, regulations, standards and guidance (review).* *(iii) The policy and procedures have been signed off by the head or deputy secretary (or equivalent) of the Federal*	FIPS 201-3 Section 5.2 – PKI Certificate Federal Common Policy Framework Certificate Policy Section 4.12 (and subsections) – Key Escrow and Recovery

		department or agency (review). **(iv)** *The organization will periodically review and update the policy and procedures as required (review, interview).*	

k. Appendix G, Table G.2, Assignment of Roles and Responsibilities (RR(DC)) add the following Control

Assignment of Roles and Responsibilities	RR(DC)-6	For organizations that maintain a key escrow and recovery system in conjunction with the DPIV Issuance system, the organization has appointed the role of Third-Party Key Recovery Request Approver. **Assessment** *Determine that:* *(i) The organization has defined the role of Third-Party Key Recovery Request Approver and its responsibilities (review)* *(ii) The organization has assigned the role of Third-Party Key Recovery Request Approver (review).*	FIPS 201-3 Section 5.2 – PKI Certificate Federal Common Policy Framework Certificate Policy Section 4.12.1.8 Requestor Authorization Validation

l. Appendix G, Table G.2, Facility and Personnel Readiness (FP(DC)), add the following:

Facility and Personnel Readiness	FP(DC)-10	For organizations that maintain a key escrow and recovery system in conjunction with the DPIV Issuance system, all operators who perform duties associated with key escrow and recovery are allowed access to the Key Escrow Database only when authenticated through a PIV Card. At least two operators are required to recover an escrowed key management key. **Assessment** *Determine that:* *(i) The requirement that all operators who perform roles within the key escrow and recovery system are allowed logical access to escrowed*	FIPS 201-3 Section 5.2 – PKI Certificate Federal Common Policy Framework Certificate Policy Section 4.12 (and subsections) – Key Escrow and Recovery

		keys only when authenticated through a PIV Card has been documented in the issuing facility's standard operating procedures. (review) *(ii) Operators use PIV cards to access key recovery systems in the course of performing their roles within the Key escrow and Recovery Systems (review).* *(iii) All operators who perform roles within the key escrow and recovery system are allowed access to escrowed keys only after completing a training course specific to their duties (interview, review).* *(iv) Records showing that the appropriate training course has been completed by key recovery personnel are stored y the facility for audit purposes (interview, review).*	

m. Appendix G, Table G.2, Implementation of Credentialing Infrastructures (CI(DC)), add the following control:

Implementation of Credentialing Infrastructures	CI(DC)-15	For organizations that maintain a key escrow and recovery system in conjunction with the DPIV Issuance system, all key management private keys are escrowed. **Assessment** *Determine that:* *(i) The key escrow database is operational, and copies of key management private keys are automatically stored when key management certificates are generated (review, test).*	FIPS 201-3 Section 5.2 – PKI Certificate Federal Common Policy Framework Certificate Policy Section 4.12 1 – Key Escrow and Recovery Policy and Practices

n. Appendix G, Table G.2 Sponsorship Process (SP(DC)), add the following:

Sponsorship Process	SP-3	For organizations that maintain a key escrow and recovery system in conjunction with the DPIV Issuance system, keys are recovered only upon request by proper authority. **Assessment** *Determine that:* *(i) The process for making a request is documented (review)* *(ii) A request from a valid authority is required to recover an escrowed private key management key.*	FIPS 201-3 Section 5.2 – PKI Certificate Federal Common Policy Framework Certificate Policy Section 4.12.1.8 – Requestor Authorization Validation