Check for updates

NIST Special Publication 800
NIST SP 800-157r1 fpd

Guidelines for Derived Personal Identity Verification (PIV) Credentials

Final Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-157r1.fpd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-157r1 fpd

Guidelines for Derived Personal Identity Verification (PIV) Credentials

Final Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

James L. Fenton
Altmode Networks

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-157r1.fpd

November 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Fair Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [will be added upon final publication]

How to Cite this NIST Technical Series Publication

Ferraiolo H, Regenscheid A, Fenton JL (2024) Guidelines for Derived Personal Identity Verification (PIV) Credentials. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-157r1 fpd. https://doi.org/10.6028/NIST.SP.800-157r1.fpd

Author ORCID iDs

Hildegard Ferraiolo: 0000-0002-7719-5999
Andrew Regenscheid: 0000-0002-3930-527X
James L. Fenton: 0000-0002-2344-4291

Public Comment Period

November 14, 2024 - January 10, 2025

Submit Comments

mailto:piv_comments@nist.gov

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/157/r1/fpd, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This recommendation provides technical guidelines for the implementation of standards-based, secure, reliable credentials that are issued by federal departments and agencies to individuals who possess and prove control of their valid PIV Card. These credentials can be either public key infrastructure (PKI)-based like the PIV Card or non PKI-based but verified by the individual's home agency. The scope of this document includes requirements for the initial issuance and maintenance of these credentials, certificate policies as applicable, cryptographic specifications, technical specifications for permitted authenticator types, and the command interfaces for removable implementations of such PKI-based credentials.

Keywords

authentication; credentials; derived PIV credentials; electronic authentication; electronic credentials; mobile devices; personal identity verification; PIV

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: mailto:piv_comments@nist.gov.

Table of Contents

List of Tables

List of Figures

Acknowledgments

The authors — Hildegard Ferraiolo and Andrew Regenscheid of the National Institute of Standards and Technology (NIST) and James Fenton of Altmode Networks — wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content and development. The authors would like to also acknowledge the past contributions of David Cooper, Salvatore Francomacaro, William Burr, Sarbari Gupta, and Jason Mohler. They give special thanks to Jonathan Gloster of HII-Mission Technologies for significant support in the revision of this document and to Isabel Van Wyk of NIST for much appreciated editing assistance.

1. Introduction

This section is informative.

[FIPS 201] specifies a common set of identity credentials to satisfy the requirements of [HSPD-12] in a smart card form factor known as the Personal Identity Verification (PIV) Card. This publication is a companion document to FIPS 201 that specifies the use of additional common identity credentials, known as derived PIV credentials, issued by a federal department or agency and may be used when using a PIV Card is impractical. Consistent with the goals of HSPD-12, derived PIV credentials are designed to serve as a Federal Government-wide standard for a secure and reliable identity credential that supports interoperability across agencies.

1.1. Background

FIPS 201 originally required that the PIV credential and associated keys be stored in a PIV Card. While using the PIV Card for electronic authentication works well with many traditional desktop and laptop computers, it needs to be better suited to other devices, such as mobile devices. In response to the growing use of mobile endpoints within the Federal Government, FIPS 201-2 permitted the issuance of additional PKI-based credentials, referred to as derived PIV credentials, for which the corresponding private key is stored in a cryptographic module within a mobile device, such as a smartphone. PKI-based derived PIV credentials use the Federal Public Key Infrastructure (FPKI) to securely establish the binding between the credential and the PIV identity account. PKI-based derived PIV credentials are typically integrated into user endpoints, such as mobile devices, although they are not limited to use in these devices.

To provide additional flexibility for federal departments and agencies, FIPS 201-3 expands the set of credentials beyond those that are PKI-based and broadens their use to other types of devices in addition to mobile devices. This document — NIST Special Publication (SP) 800-157r1 (Revision 1) — describes the expanded set of derived PIV credentials in a variety of form factors. Non-PKI-based derived PIV credentials are cryptographic authenticators (as defined in [SP800-63B]) that are phishing-resistant. They may be separate from the endpoint being authenticated and, if so, are connected to the endpoint for that purpose. Since there is no PKI infrastructure to validate and supply attributes for non-PKI-based derived PIV credentials, non-PKI-based derived PIV credentials are always used to authenticate to the home agency IdMS of the PIV cardholder from which the cardholder's PIV identity account is accessed. When access to the PIV identity account is needed outside of the cardholder's home agency — particularly when a non-PKI-based derived PIV credential is presented in authentication — federation allows for connection across security domains as detailed in [SP800-217]. In the case of non-PKI derived PIV credentials, attributes are obtained from the PIV identity account rather than from the derived PIV credential itself.

> Note: The PIV identity account is frequently implemented as multiple linked database records with potentially different access restrictions within the enterprise IDMS, which is the central repository for the cardholder's digital identities. References to the PIV identity account apply to the relevant linked record, the structure of which is determined by the issuing agency.

Derived PIV credentials leverage the current investment in the PIV infrastructure for electronic authentication and build upon the solid foundation of the well-vetted and trusted identity of the PIV cardholder as represented in the PIV identity account, achieving substantial cost savings by leveraging the identity proofing results that were already performed to issue PIV Cards. This document provides technical guidelines for the implementation of derived PIV credentials.

1.2. Purpose and Scope

This document provides guidelines for cases in which PIV Cards are deemed impractical for authentication and specifies the use of authenticators with alternative form factors to the PIV Card that may be inserted into endpoints (e.g., USB authenticators, authenticators that are connected wirelessly to endpoints, and authenticators that are embedded in endpoints). Authenticators used as derived PIV credentials must meet the requirements for cryptographic authenticators and must be phishing-resistant. Examples of suitable authentication processes include client-authenticated TLS and WebAuthn [WebAuthn]. Using alternative form factors greatly improves the usability of electronic authentication to remote IT resources while simultaneously maintaining the goals of HSPD-12 for common identification that is secure, reliable, and has government-wide interoperability.

The purpose of the derived PIV credential is to provide PIV-enabled authentication services on alternative endpoints to authenticate the credential holder to remote systems. As described in Appendix D, derived PIV credentials can also be used for physical access.

To achieve interoperability with the PIV infrastructure and its applications, two approaches to derived PIV credentials have been selected:

1. Use of public key infrastructure (PKI) technology. PKI-based derived PIV credentials rely on the same infrastructure used for authentication with a PIV Card. Cross-domain use of PKI-based derived PIV credentials is supported in the same manner as for PIV Cards.
2. Use of non-PKI-based authenticators. Non-PKI authenticators rely on IdAM infrastructure to allow for direct authentication by the home agency. Cross-domain use of non-PKI-based derived PIV credentials is supported through federation protocols, as specified in [SP800-217].

The derived PIV credentials specified in this document are issued at authentication assurance level (AAL) 2 or 3. Derived PIV credentials are issued at identity assurance level (IAL) 3, which is the identity proofing and issuance level associated with the PIV Card and bound to the PIV identity account, as per [FIPS201].

Derived PIV credentials are based on the general concept of post-enrollment authenticator binding in [SP800-63B], which leverages identity proofing and vetting associated with an existing subscriber account using current and valid authenticators to bind additional authenticators to that account. Identity proofing and vetting processes do not have to be repeated to issue a derived PIV credential. Instead, the user proves possession and control of a valid PIV Card to bind a derived PIV credential to their PIV identity account. The PIV Card may be used as the basis for issuing other types of derived credentials, but those credentials would not be bound to the PIV identity account and are therefore outside of this document's scope.

While non-PKI derived PIV credentials are different in nature from PIV Cards and PKI-based derived PIV credentials, they are nevertheless considered to be derived PIV credentials due to their binding to the cardholder's PIV identity account. Other authenticator requirements such as strength (AAL) and phishing resistance are additionally required for suitability as derived PIV credentials.

Derived PIV credentials are:

- Issued based on possession and control of the PIV Card,
- Represented in the PIV identity account at the home agency IdMS, and
- Issued in accordance with this document.

This document provides technical guidelines on:

- The primary life cycle activities for the derived PIV credential (i.e., initial issuance, maintenance, and termination) and the requirements for each activity to ensure security and
- The derived PIV credential, including cryptographic specifications, permitted implementation types, mechanisms for activation, use of the credential, and certificate policies, if applicable.

This publication includes an informative appendix that provides recommendations for including digital signature and key management keys on devices that host a derived PIV credential. It also includes an annex with guidelines for the issuance and use of derived PIV credentials for facility access.

1.3. Audience

This document is intended for stakeholders who are responsible for procuring, designing, implementing, and managing deployments of derived PIV credentials for mobile devices and other endpoints.

1.4. Requirements Notation and Conventions

This standard uses the following typographical conventions in text:

- Specific terms in **CAPITALS** represent normative requirements. When these same terms are not in **CAPITALS**, the term does not represent a normative requirement.
  - The terms "**SHALL**" and "**SHALL NOT**" indicate requirements to be strictly followed to conform to the publication and from which no deviation is permitted.
  - The terms "**SHOULD**" and "**SHOULD NOT**" indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.
  - The terms "**MAY**" and "**NEED NOT**" indicate a course of action permissible within the limits of the publication.
  - The terms "**CAN**" and "**CANNOT**" indicate a possibility and capability — whether material, physical, or causal — or, in the negative, the absence of that possibility or capability.

1.5. Document Structure

This document is organized as follows. Each section is labeled as either normative (i.e., mandatory for compliance) or informative (i.e., not mandatory).

- Section 2 describes derived PIV credential life cycle activities and related requirements. This section is *normative*.
- Section 3 describes the technical requirements for implementing derived PIV credentials. This section is *normative*.
- Appendix A contains guidance on digital signature and key management keys. This appendix is *informative*.
- Appendix B provides detailed interface requirements for PKI-based removable (non-embedded) and PKI-based wireless implementations for logical access. This appendix is *normative* for implementing PKI-based derived PIV credentials on removable (non-embedded) or wireless cryptographic authenticators.
- Appendix C provides examples of issuance processes for derived PIV credentials. This appendix is *informative*.
- Appendix D provides detailed requirements for using derived PIV credentials in physical access control systems (PACS). This appendix is *normative* for derived PIV credentials used for physical access.

- Appendix E contains a glossary of selected terms used in this document. This appendix is *informative*.
- Appendix F defines acronyms and other abbreviations used in this document. This appendix is *informative*.
- Appendix G lists changes made to this document since its initial release. This appendix is *informative*.

1.6. Key Terminology

Certain key PIV terms have assigned meanings within the context of this document. The term *PIV cardholder* refers to a person who possesses a valid PIV Card, regardless of whether they have been issued a derived PIV credential. The term *applicant* refers to a PIV cardholder who has applied for but has yet to be issued a derived PIV credential, and the term *subscriber* refers to a PIV cardholder to whom a derived PIV credential has been issued.

2. Life Cycle Activities and Related Requirements

This section is normative.

The life cycle activities for a derived PIV credential are initial issuance, maintenance, and termination. At a more detailed level, the life cycle activities for PKI-based and non-PKI-based derived PIV credentials differ considerably. This section describes these life cycle activities and provides requirements and recommendations as appropriate.

Issuers of derived PIV credentials **SHALL** document the process for each life cycle activity described below. In accordance with [HSPD-12], the reliability of the derived PIV credential issuer **SHALL** be established through an official accreditation process, as described in [SP800-79].

2.1. Derived PIV Credential Life Cycle Activities

The derived PIV credential life cycle consists of the activities described above: initial issuance, maintenance, and termination. The activities at the manufacturer during fabrication and pre-personalization of the authenticator (as applicable) are not considered part of this life cycle model. Figure 1 presents the PKI-based derived PIV credential life cycle activities alongside the PIV Card life cycle activities. Figure 2 presents the corresponding life cycle activities for non-PKI-based derived PIV credentials.

The life cycle of a derived PIV credential begins with issuance on an approved device or authenticator associated with the applicant. This may be part of issuing a PIV Card or a subsequent process. Mobile devices with derived PIV credentials are managed, as described in [SP800-124].

The maintenance activities for a PKI-based derived PIV credential are the same as for other X.509 public key certificates. Certificate re-key is typically used to replace a certificate that is nearing expiration. Certificate modification replaces a certificate if information about the subscriber that appears on the certificate (e.g., their name) needs to be changed.

While non-PKI-based derived PIV credentials are not typically re-keyed and do not contain PII about the subscriber, they may require maintenance, such as replacing the activation secret or biometric factor used to activate the physical authenticator. Instead of re-keying, the current non-PKI-based derived PIV credential **SHALL** be invalidated and the initial issuance process (except for the device or authenticator approval process) repeated to bind a new derived PIV credential. When a non-PKI-based derived PIV credential is lost, stolen, or damaged, the issuer **SHALL** invalidate the credential to prevent its further use.

When an authenticator with the private key that corresponds to a PKI-based derived PIV credential is lost, stolen, or damaged, the issuer **SHALL** prevent further use of the affected credential by either collecting and destroying the associated private key or

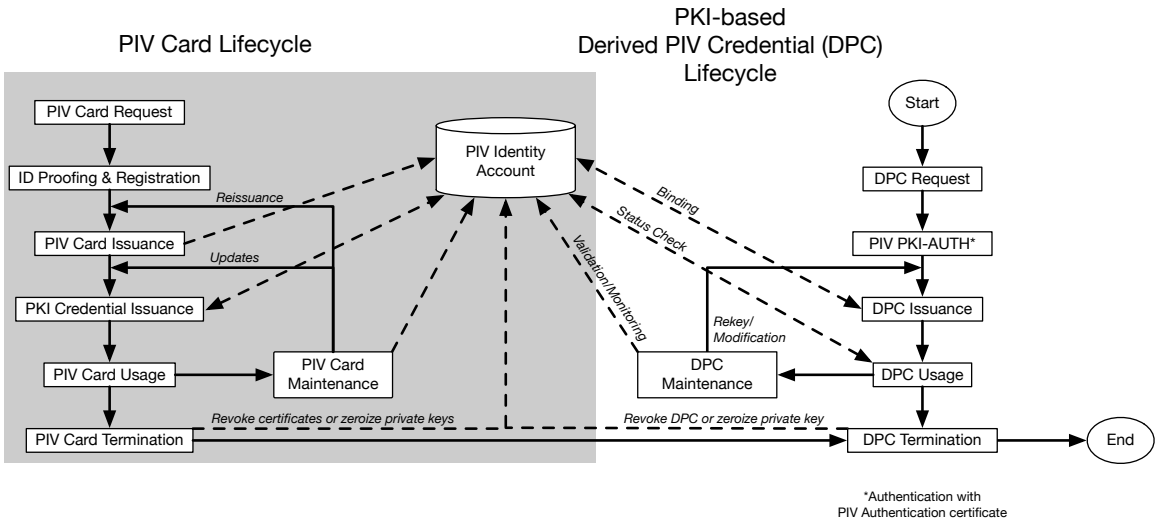

Fig. 1. PKI-based derived PIV credential life cycle activities

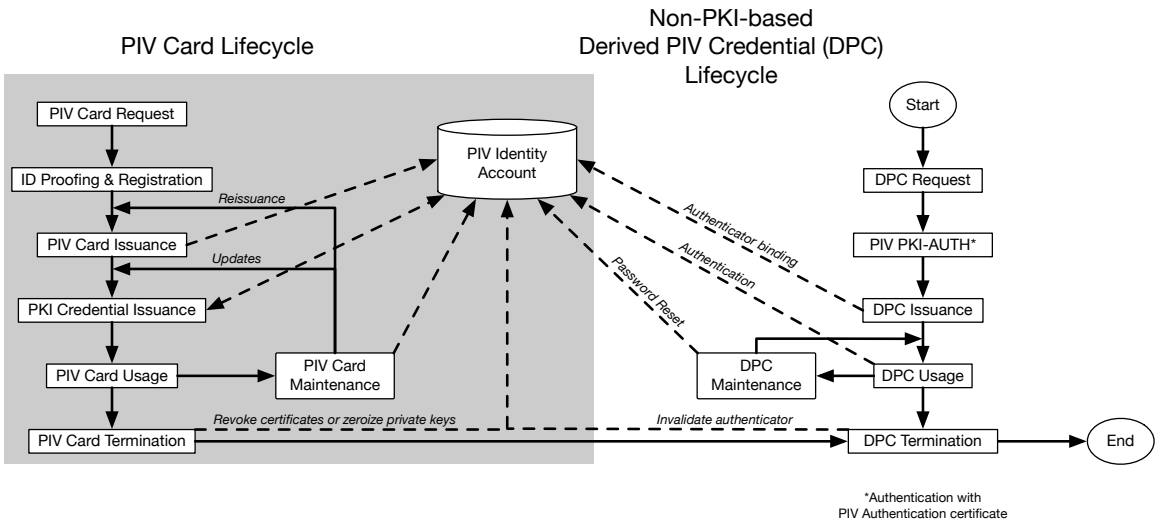

Fig. 2. Non-PKI-based derived PIV credential life cycle activities

revoking the associated certificate. These processes are described in Sec. 2.4. If the subscriber becomes ineligible to possess a PIV Card, all derived PIV credentials for that subscriber are revoked or otherwise invalidated.

2.2. Initial Issuance

Issuing a derived PIV credential is an instance of the post-enrollment binding of an authenticator described in [SP800-63B]. Issuance **SHALL** be performed in accordance with the requirements that apply to cryptographic authenticators and the requirements in this section. The term *issuance* is used when the device or authenticator is provided to the subscriber and when the device or authenticator is already in the subscriber's possession. Appendix C provides sample issuance processes for derived PIV credentials.

Derived PIV credentials **SHALL** only be issued by the home agency of the associated PIV identity account or by a third-party organization or service provider (e.g., USAccess) authorized by the home agency. Derived PIV credentials **SHALL** only be issued to devices (e.g., mobile devices) or authenticators that are approved by the home agency. Agencies **MAY** establish blanket approvals for particular device types or **MAY** individually authorize specific devices or authenticators for issuance and use by a cardholder. Each issuer **SHALL** document its authorization policies for issuance.

Binding a derived PIV credential to a PIV identity account can be accomplished through a connection to a PIV-authenticated endpoint, a direct connection to the PIV Card, or the use of the external authenticator binding procedure described in [SP800-63B] Sec. 4.1.2.2. Derived PIV credentials **MAY** be issued remotely or in person. Except for derived PIV credential issuance as described in Sec. 2.2.3, the binding **SHALL** require the cardholder to authenticate using their PIV Card with the PIV-AUTH authentication mechanism specified in [FIPS201] Sec. 6.2.3.1. In addition to authenticating the cardholder, performing the PKI-AUTH authentication mechanism verifies that the applicant is currently eligible to possess a PIV Card. All derived PIV credentials **SHALL** be issued in accordance with [SP800-63B] Sec. 6.1.2.1.

Issuing agencies **SHALL** have a documented policy or process for determining the capabilities and basis for trust of the credentials they issue and the devices on which they will reside. All AAL3 derived PIV credentials **SHALL** only be issued to devices that the home agency has determined to have been issued to the cardholder.

After the applicant has been authenticated, a derived PIV credential **MAY** be issued. The newly issued derived PIV credential **SHALL** be represented in the cardholder's PIV identity account. This implies that a third-party organization or service provider issuing derived PIV credentials needs to have access to the PIV identity account to meet this requirement.

When a new derived PIV credential is associated with a PIV identity account, the issuer **SHALL** promptly notify the PIV cardholder. Notification **SHALL** be to an address

associated with the cardholder's PIV identity account. More than one independent notification method **MAY** be used to ensure prompt receipt by the cardholder. Examples of these processes are given in Appendix C.

Derived PIV credentials **SHALL** meet the requirements for authentication assurance level (AAL) 2 or 3 specified in [SP800-63B]. Derived PIV credentials that meet AAL3 requirements also fulfill the requirements of AAL2 and can be used in circumstances that require authentication at AAL2. All derived PIV credentials at both AAL2 and AAL3 **SHALL** meet the requirements for phishing resistance defined in [SP800-63B] Sec. 3.2.5.

This guideline does not preclude issuing multiple derived PIV credentials to the same applicant based on the same PIV Card. However, this could increase the risk that one of the derived PIV credentials will be lost/stolen without the loss being reported or that the subscriber will inappropriately provide one to someone else. Accordingly, issuers **MAY** limit the number of active derived PIV credentials that a subscriber may have.

2.2.1. PKI-Based Derived PIV Credential Issuance

Issuing a PKI-based derived PIV credential requires the generation of a public/private key pair followed by the creation of a corresponding authentication certificate by the certificate authority (CA). For a derived PIV credential capable of being used at AAL3, all of the following requirements apply:

- The cardholder **SHALL** be authenticated using the PIV-AUTH authentication mechanism specified in [FIPS201].
- The key pair **SHALL** be generated in the device (authenticator or endpoint) that will house the derived PIV credential.
- The device **SHALL** send the certificate signing request containing the public key to the CA, which **SHALL** return an X.509 authentication certificate that **SHALL** be stored on the device (authenticator or endpoint).
- The CA **SHALL** retain a copy of the issued certificate for use should revocation be required.

For a derived PIV credential issued for use only at AAL2, the same procedure **MAY** be used, or the CA **SHALL** generate a key pair and corresponding certificate and send the certificate and private key to the device over an authenticated protected channel for installation. Following installation, the CA **SHALL** promptly and securely delete its copy of the private key.

The private key **SHALL** be stored on the device in a manner that makes it accessible only upon entry of the correct activation secret or presentation of a biometric factor that matches a stored biometric image or template. This **SHALL** be accomplished by using strong access controls for the stored private key or through decryption of the private key using an encryption key derived from the activation secret.

2.2.2. Non-PKI-Based Derived PIV Credential Issuance

The applicant **SHALL** be provided with or supply an approved physical authenticator for the highest AAL that the derived PIV credential will be used to authenticate. If the issuer does not directly provide the authenticator, the issuer **SHALL** verify that the authenticator's characteristics (e.g., single-factor or multi-factor) meet the requirements of [SP800-63B] for the highest authentication assurance level at which it will be used (AAL2 or AAL3), including [FIPS140] requirements.

The issuance process for a multi-factor authenticator **SHALL** prompt the applicant to establish an activation secret or a biometric activation factor (or both) for the authenticator if not previously established and successfully authenticate using that authenticator. The issuance process with a single-factor authenticator **SHALL** prompt the applicant to register a password that meets the requirements of [SP800-63B] Sec. 3.1.1 and will be verified along with the physical authenticator in the authentication process.

2.2.3. Derived PIV Issuance Without PIV Card

Some operational situations may motivate the issuance of a derived PIV credential when a PIV Card is unavailable. For example, it may be desirable to:

- Issue a derived PIV credential to a new subscriber in a field location where production facilities for PIV Cards are unavailable
- Issue a derived PIV credential to a cardholder who has forgotten to bring their PIV Card to work

In these and similar situations, one or more derived PIV credentials **MAY** be issued, subject to the following conditions.

The subscriber **SHALL** be issued a derived PIV credential only after all issuance requirements in [FIPS201] Sec. 2.8 and 2.8.3 have been met (substituting "derived PIV credential" for "PIV Card" in those sections) and the PIV identity account has been established. Issuance **SHALL** be performed in person or at a supervised remote identity proofing station.

Since only PIV Cards (and not derived PIV credentials) can be used to bind additional derived PIV credentials, all derived PIV credentials expected to be needed **SHOULD** be issued at the same time. For example, the subscriber may need a mobile device and also a separate hardware token as derived PIV credentials.

Derived PIV credentials issued in this manner **MAY** also be enabled for physical access, as described in Appendix D.

2.3. Maintenance

The maintenance activities required for derived PIV credentials depend on the type of derived PIV credential (PKI-based or non-PKI-based) used. Maintenance activities include rekeying, modifying certificates, and replacing an activation factor (biometric or activation secret) as appropriate.

Derived PIV credentials are unaffected when the subscriber replaces their PIV Card with a new one (reissuance) or when it is lost, stolen, or damaged. The ability for the subscriber to use a derived PIV credential is beneficial while waiting for a new PIV Card to be issued. In such circumstances, the subscriber continues to be able to use the derived PIV credential to gain logical access to remote federally controlled information systems from their endpoint.

Updating the activation factor (biometric or activation secret, such as a PIN) or resetting the activation retry count for a derived PIV credential **SHALL** be performed in accordance with Sec. 3.1.4 for PKI-based derived PIV credentials or Sec. 3.2.3 for non-PKI-based derived PIV credentials.

2.3.1. PKI-Based Derived PIV Credential Maintenance

PKI-based derived PIV credentials require typical maintenance activities applicable to asymmetric cryptographic credentials, including rekeying and modification. These activities **MAY** be performed either remotely or in person and **SHALL** be conducted in accordance with the certificate policy under which the derived PIV authentication certificate is issued. When certificate rekeying or modification is performed remotely for a derived PIV credential, communication between the issuer and the cryptographic module in which the derived PIV authentication private key is stored **SHALL** only occur over mutually authenticated secure sessions between tested and validated cryptographic modules.

Certain maintenance activities for the subscriber's PIV Card trigger corresponding maintenance activities for the derived PIV credential. PKI-based derived PIV credentials **SHALL** be reissued if any information about the subscriber that appears in the credential changes. For example, if the subscriber's PIV Card is reissued as a result of a change in the subscriber's name and the subscriber's name appears in the derived PIV authentication certificate, a new derived PIV authentication certificate with the new name **SHALL** be issued and the previous certificate invalidated. The subscriber then uses their current PIV authentication certificate to authenticate to the issuer, which then updates the certificate in the derived PIV credential module.

2.3.2. Non-PKI-Based Derived PIV Credential Maintenance

Maintenance activities for non-PKI-based derived PIV credentials are simpler than those for PKI-based derived PIV credentials since the former do not contain information about the cardholder nor carry a specific expiration date. Identity information **SHALL** be maintained in the PIV identity account and **SHALL** be updated when needed.

Updating a separate password used with a single-factor authenticator for use at AAL2 **SHALL** be performed in a mutually authenticated protected session with the home agency IdMS. The update **SHALL** require the entry of the current password. If resetting the password is required because the subscriber has forgotten the password or has reached the retry limit, it **SHALL** be done in accordance with Sec. 3.2.3.

2.4. Invalidation

When an authenticator associated with a derived PIV credential is compromised (e.g., lost, stolen, or damaged), that derived PIV credential **SHALL** be invalidated as described below.

All derived PIV credentials associated with a given PIV identity account **SHALL** be invalidated when that PIV identity account is terminated, typically due to the cardholder's loss of PIV credential eligibility. Issuers of derived PIV credentials **SHALL** continuously monitor the associated PIV identity account to determine its termination status. Meeting this requirement is simplified because the subject's PIV Card, credential eligibility, and all derived PIV credentials are maintained in one account — the PIV identity account — and maintained by the home agency IdMS.

If a PIV Card or derived PIV credential is invalidated due to loss or compromise, the home agency or issuer **SHOULD** check to see whether any derived PIV credentials have been recently (typically within the past seven days) bound to the PIV identity account and if so, determine whether they were appropriately issued to the subject. Termination of the PIV Card, which may occur due to loss or other compromise, does not usually require the invalidation of associated derived PIV credentials unless it is a result of termination of the associated PIV identity account.

The non-voluntary invalidation of a derived PIV credential **SHALL** be handled as specified in [CSP].

2.4.1. PKI-based Derived PIV Credential Invalidation

If the derived PIV authentication private key was created and stored on a hardware module that does not permit private key export and the token is collected and either zeroized or destroyed, then the derived PIV authentication certificate **SHOULD** be revoked. In all other cases, the derived PIV authentication certificate **SHALL** be revoked.

2.4.2. Non-PKI-Based Derived PIV Credential Invalidation

Non-PKI-based derived PIV credentials are always directly verified by the home agency IdMS of the associated PIV Card. Therefore, termination of a non-PKI-based derived PIV credential **SHALL** be accomplished by invalidating the reference to the associated authenticator in the PIV identity account so that the authenticator cannot be used to authenticate to the home agency IdMS. Separate authenticators **MAY** be collected from the subscriber, but this is not required.

3. Technical Requirements

This section is normative.

This section describes technical requirements for PKI-based and non-PKI-based derived PIV credentials and associated authenticators.

While the following sections focus on credential and authenticator requirements, the verifier is required to meet the corresponding verifier requirements in [SP800-63B] Sec. 3.1.

3.1. PKI-Based Derived PIV Credentials

A PKI-based derived PIV credential is a derived PIV authentication certificate, which is an X.509 public key certificate that has been issued in accordance with the requirements of this document and [COMMON]. All derived PIV credentials created under previous revisions of these guidelines are PKI-based and remain valid implementations under this SP 800-157 revision. Appendix B describes additional requirements for removable or wireless PKI-based derived PIV credentials that are used for logical access.

Authentication using PKI-based derived PIV credentials **SHALL** include a check to determine that the authentication certificate is valid and current (e.g., that the certificate is unexpired and not revoked).

3.1.1. Certificate Policies for PKI-Based Derived PIV Credentials

Derived PIV authentication certificates **SHALL** be issued under either the `id-fpki-common-derived-pivAuth-hardware` policy (satisfying [SP800-63B] AAL3) or the `id-fpki-common-derived-pivAuth` policy (satisfying AAL2) of [COMMON]. All derived PIV credentials **SHALL** be deemed to satisfy [SP800-63A] IAL3 since that is the identity proofing and issuance level associated with the PIV Card and bound to the PIV identity account.

Derived PIV authentication certificates **SHALL** comply with the *Derived PIV Authentication Certificate* profile in [PROF].

The expiration date of a derived PIV authentication certificate is based on the issuer's certificate policy and the certificate policy specified above. There is no requirement to align the expiration date of a derived PIV authentication certificate with the expiration date of the PIV authentication certificate or the expiration of the PIV Card. This allows a derived PIV credential to continue to act as an active credential while the cardholder's PIV Card is being renewed.

3.1.2. Cryptographic Specifications

The cryptographic algorithm and key size requirements for the derived PIV authentication certificates and private keys are the same as the requirements for the PIV authentication certificate and private key, as specified in [SP800-78].

For derived PIV authentication certificates issued under `id-fpki-common-pivAuth-derived-hardware` (AAL3), the derived PIV authentication key pair **SHALL** be generated within a cryptographic module that meets the requirements of [SP800-63B] Sec. 2.3.2, including being validated to [FIPS140] Level 2 or higher with Level 3 physical security to protect the derived PIV authentication private key while in storage and not permitting export of the private key.

For derived PIV authentication certificates issued under `id-fpki-common-pivAuth-derived` (AAL2), the derived PIV authentication key pair **SHALL** be generated within a cryptographic module that has been validated to [FIPS140] Level 1 or higher. If the key pair is generated outside of the authenticator itself, the private key **SHALL** be transferred via an authenticated protected channel as defined in [SP800-63B], and the authenticator **SHALL** meet the requirements of [SP800-63B] Sec. 2.2.2, including being validated to [FIPS140] Level 1 or higher.

3.1.3. Allowable Authenticator Types

A multi-factor cryptographic authenticator as specified in [SP800-63B] Sec. 3.1.7.1 **SHALL** be used for PKI-based derived PIV authentication. The authenticator **SHALL** be phishing-resistant, as described in [SP800-63B] Sec. 3.2.5. Authenticators used at AAL3 **SHALL** meet the additional requirements described in [SP800-63B] Sec. 2.3.

3.1.4. Activation Data

Activation of PKI-based derived PIV authenticators using an activation secret **SHALL** meet the requirements of [SP800-63B] Sec. 3.2.10. Activation using a biometric characteristic **SHALL** meet the requirements of [SP800-63B] Sec. 3.2.3.

If the activation secret or the biometric activation factor needs to be changed, entry of the current activation secret **SHALL** be required to change the value. The authenticator **MAY** support a PIN unblocking key (PUK) that can be used by the home agency IdMS to unblock or reset the activation secret or biometric activation factor if it has been forgotten or the permitted number of consecutive wrong attempts has been reached. If reset using PUK is unavailable and the authenticator cannot be successfully activated, the authenticator **SHALL** be invalidated as described in Sec. 2.4. A new derived PIV credential **MAY** then be issued.

3.2. Non-PKI-Based Derived PIV Credentials

Non-PKI-based credentials **SHALL** only be used to authenticate to verifiers that are authorized by the home agency of the associated PIV Card. All verifiers of non-PKI-based

derived PIV credentials **SHALL** access the home agency IdMS in order to determine the current validity of the associated PIV identity account. Non-PKI derived PIV credentials can be used elsewhere through federation with an IdP able to access the home agency IdMS, as described in [SP800-217].

3.2.1. Allowable Authenticator Types

Multi-factor or single-factor cryptographic authenticators as specified in [SP800-63B] Sec. 3.1.7.1 and Sec. 3.1.6.1, respectively, **SHALL** be used for non-PKI-based derived PIV authentication. Cryptographic authenticators **SHALL** be phishing-resistant as described in [SP800-63B] Sec. 3.2.5. Examples of suitable authentication processes include client-authenticated TLS and WebAuthn [WebAuthn]. Except for physical access applications specified in Appendix D, all single-factor authenticators **SHALL** be used in conjunction with a password that meets the requirements of [SP800-63B] Sec. 3.1.1. Authenticators used at AAL3 **SHALL** meet the additional requirements described in [SP800-63B] Sec. 2.3.

3.2.2. Cryptographic Specifications

Authenticators used as non-PKI-based derived PIV credentials **SHALL** meet the cryptographic requirements specified in [SP800-63B] Sec. 3.1 for the corresponding authenticator type.

3.2.3. Activation Data

Activation of the derived PIV credential using an activation secret **SHALL** meet the requirements of [SP800-63B] Sec. 3.2.10. Activation using a biometric characteristic **SHALL** meet the requirements of [SP800-63B] Sec. 3.2.3.

If the activation secret or the biometric activation factor needs to be changed, entry of the current activation secret **SHALL** be required to change the value. If the activation secret has been forgotten or the permitted number of consecutive wrong attempts has been reached, centralized management by the home agency IdMS **SHALL** be required to reset the activation secret and attempt counter. If centralized reset is unavailable, the authenticator **SHALL** be reset and will requires re-binding to the PIV identity account, as described in Sec. 2.2.

References

[COMMON] Federal Public Key Infrastructure Policy Authority (2024) X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. (Federal CIO Council), Version 2.8 [or as amended]. Available at https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf

[CSP] Rigas MJ (2020) Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials. (U.S. Offics of Personnel Management, Washington, DC). Available at https://www.opm.gov/suitability/suitability-executive-agent/policy/cred-standards.pdf

[FIPS140] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3 [or as amended]. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS201] National Institute of Standards and Technology (2022) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-3 [or as amended]. https://doi.org/10.6028/NIST.FIPS.201-3

[HSPD-12] Bush GW (2004) Policy for a Common Identification Standard for Federal Employees and Contractors. (The White House, Washington, DC), Homeland Security Presidential Directive HSPD-12. Available at https://www.dhs.gov/homeland-security-presidential-directive-12

[ISO7816] International Organization for Standardization/International Electrotechnical Commission (2004-2020) *ISO/IEC 7816 — Identification cards — Integrated circuit cards*. (multiple parts):

- International Organization for Standardization/International Electrotechnical Commission (2011) *ISO/IEC 7816-1:2011 — Identification cards — Integrated circuit cards — Part 1: Cards with Contacts — Physical characteristics*. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/54089.html
- International Organization for Standardization/International Electrotechnical Commission (2007) *ISO/IEC 7816-2:2007 — Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimensions and location of the contacts*. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/45989.html
- International Organization for Standardization/International Electrotechnical Commission (2006) *ISO/IEC 7816-3:2006 — Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission*

protocols. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/38770.html

- International Organization for Standardization/International Electrotechnical Commission (2020) *ISO/IEC 7816-4:2020 — Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/77180.html
- International Organization for Standardization/International Electrotechnical Commission (2004) *ISO/IEC 7816-5:2004 — Identification cards — Integrated circuit cards — Part 5: Registration of application providers*. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/34259.html
- International Organization for Standardization/International Electrotechnical Commission (2016) *ISO/IEC 7816-6:2016 — Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/64598.html

[ISO14443] International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 14443-1:2018 — Cards and security devices for personal identification — Contactless proximity objects Part 1: Physical characteristics*. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/73596.html

[PCSC] Personal Computer/Smart Card Workgroup (2020) *PC/SC Workgroup Specifications Overview*. Available at https://pcscworkgroup.com/specifications/

[PROF] Federal Public Key Infrastructure Policy Authority (2021) X.509 Certificate and Certificate Revocation List (CRL) Profiles. (Federal CIO Council), Version 2.1 [or as amended]. Available at https://www.idmanagement.gov/docs/fpki-x509-cert-profile-common.pdf

[SP800-63A] Temoshok D, Abruzzi C, Fenton JL, Galluzzo R, LaSalle C, Lefkovitz N, Regenscheid A (2024) Digital Identity Guidelines: Identity Proofing and Enrollment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63A-4 2pd [or as amended]. https://doi.org/10.6028/NIST.SP.800-63A-4.2pd

[SP800-63B] Temoshok D, Fenton JL, Choong YY, Lefkovitz N, Regenscheid A, Richer JP (2024) Digital Identity Guidelines: Authentication and Authenticator Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63B-4 2pd [or as amended]. https://doi.org/10.6028/NIST.SP.800-63B-4.2pd

[SP800-73pt1] Ferraiolo H, Mehta K, Francomacaro S, Chandramouli R, Gupta S (2024) Interfaces for Personal Identity Verification: Part 1 – PIV Card Application Namespace, Data Model, and Representation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-73pt1-5 [or as amended]. https://doi.org/10.6028/NIST.SP.800-73pt1-5

[SP800-73pt2] Ferraiolo H, Mehta K, Francomacaro S, Chandramouli R, Gupta S (2024) Interfaces for Personal Identity Verification: Part 2 – PIV Card Application Card Command Interface. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-73pt2-5 [or as amended]. https://doi.org/10.6028/NIST.SP.800-73pt2-5

[SP800-78] Ferraiolo H, Regenscheid A (2024) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-78-5 [or as amended]. https://doi.org/10.6028/NIST.SP.800-78-5

[SP800-79] Ferraiolo H, Regenscheid A, Gupta S, Ghadiali N (2023) Guidelines for the Authorization of PIV Card and Derived PIV Credential Issuers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-79r3 ipd [or as amended]. https://doi.org/10.6028/NIST.SP.800-79r3.ipd

[SP800-96] Dray JF, Giles A, Kelley M, Chandramouli R (2006) PIV Card to Reader Interoperability Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-96 [or as amended]. https://doi.org/10.6028/NIST.SP.800-96

[SP800-116] Ferraiolo H, Mehta KL, Ghadiali N, Mohler J, Johnson V, Brady S (2018) A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-116, Rev. 1 [or as amended]. https://doi.org/10.6028/NIST.SP.800-116r1

[SP800-124] Howell G, Franklin JM, Sritapan V, Souppaya MP, Scarfone KA (2023) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124r2 [or as amended]. https://doi.org/10.6028/NIST.SP.800-124r2

[SP800-166] Cooper D, Ferraiolo H, Chandramouli R, Ghadiali N, Mohler J, Brady S (2016) Derived PIV Application and Data Model Test Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-166 [or as amended]. https://doi.org/10.6028/NIST.SP.800-166

[SP 800-217] Ferraiolo H, Regenscheid A, Richer JP (2024) Guidelines for the Use of Personal Identity Verification (PIV) Credentials with Federation (National Institute of

Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-217 fpd [or as amended]. https://doi.org/10.6028/NIST.SP.800-217.fpd

[WebAuthn] Hodges J, Jones JC, Jones MB, Kumar A, Lundberg E (2021) Web Authentication: An API for accessing Public Key Credentials - Level 2. (World Wide Web Consortium, Cambridge, MA). Available at https://www.w3.org/TR/2021/REC-webauthn-2-20210408/

Appendix A. Digital Signature and Key Management Keys

This appendix is informative.

In addition to the PIV authentication keys, [FIPS201] also requires each PIV Card to have a digital signature key and a key management key unless the cardholder does not have a government-issued email account at the time of credential issuance. A subscriber who has been issued a derived PIV credential may also need a digital signature and key management key.

To decrypt data that was previously encrypted using one of the older key management public keys, it would be necessary to store a copy of the PIV Card's key management private key and certificate in the keystore that hosts the derived PIV credential. Neither [FIPS201] nor [COMMON] precludes a key management private key from being used on more than one device (e.g., the PIV Card and a derived PIV credential keystore) as long as all of the requirements of the policy under which the key management certificate was issued are satisfied. This means that to use a copy of a key management private key in a [FIPS140] Level 1 software cryptographic module, the corresponding certificate would have to be issued under a certificate policy, such as `id-fpki-common-policy`, that does not require the use of a [FIPS140] Level 2 hardware cryptographic module. This should be considered when issuing the key management certificate placed on the PIV Card. Key recovery mechanisms are encouraged for key management keys used on derived PIV credential keystores.

As the digital signature key on a PIV Card cannot be copied, a new digital signature private key will need to be generated and a corresponding certificate will need to be issued for the derived PIV credential keystore. The issuance of this private key and certificate is independent of the issuance of the PIV Card. As the certificate policies associated with digital signature certificates in [COMMON] (`id-fpki-common-policy`, `id-fpki-common-hardware`, and `id-fpki-common-High`) are not limited to use with PIV Cards, a digital signature certificate for a derived PIV credential keystore may be issued under one of these policies as long as all of the policy requirements are satisfied.

Appendix B. Data Model and Interfaces for Removable or Wireless PKI-Based Cryptographic Authenticators

This appendix is normative.

This appendix provides data model and interface requirements for PKI-based derived PIV applications implemented on removable or wireless cryptographic authenticators. Use of wireless cryptographic authenticators in this appendix is applicable to logical access. Wireless authenticators for physical access (e.g., facility access) are specified in Appendix D.

B.1. Derived PIV Application Data Model and Representation

The data model and representation requirements for derived PIV applications are based on the requirements for PIV Card applications, as described in [SP800-73pt1]. Test requirements and test assertions for testing the derived PIV application and associated derived PIV data objects implemented on removable hardware tokens are specified in [SP800-166], *Derived PIV Application and Data Model Test Guidelines*. The specifications for the mandatory and optional data objects listed below are the same as the specifications for the corresponding data objects on a PIV Card application, as described in [SP800-73pt1].

B.1.1. Derived PIV Application Identifier

The PIV application ID (AID) **SHOULD** be used to maximize interoperability with PIV Cards. For reference, that application ID is (in hexadecimal):

```
A0 00 00 03 08 00 00 10 00 01 00
```

Alternatively, the derived PIV application identifier defined in the previous edition of this guideline **MAY** be used. This application ID is deprecated and may not be included in future editions of this guideline. That application ID is (in hexadecimal):

```
A0 00 00 03 08 00 00 20 00 01 00
```

No other application ID **SHALL** be used.

The PIV or derived PIV application can be selected as the current application on the removable cryptographic token by providing the full AID listed above or the right-truncated version, as follows (hexadecimal):

```
A0 00 00 03 08 00 00 x0 00
```

where ‘x’ is either 1 for the PIV application or 2 for the derived PIV application.

B.1.2. Derived PIV Application Data Model Elements

The derived PIV application **SHALL** contain the following mandatory interoperable data object:

X.509 Certificate for Derived PIV Authentication

The read access control rule for the X.509 certificate for derived PIV authentication and the PKI cryptographic function access rule for the corresponding private key are as described for the X.509 certificate for PIV authentication in Sec. 3.1.3 of [SP800-73pt1].

The following data objects **MAY** also be present:

X.509 Certificate for Digital Signature

The read access control rule for the X.509 certificate for digital signature and the PKI cryptographic function access rule for the corresponding private key are as described in Sec. 3.2.1 of [SP800-73pt1].

X.509 Certificate for Key Management

The read access control rule for the X.509 certificate for key management and the PKI cryptographic function access rule for the corresponding private key are as described in Sec. 3.2.2 of [SP800-73pt1].

Discovery Object

The requirements for the discovery object are as described in Sec. 3.3.2 of [SP800-73pt1], except for the following:

- References to “PIV card application AID” are replaced by “derived PIV application AID.”
- References to “PIV card application PIN” are replaced by “derived PIV activation secret.”
- The first byte of the PIN usage policy **SHALL** be set to `0x40` to indicate that the virtual contact interface (VCI) is not implemented, `0x48` to indicate that a pairing code is required to establish a VCI, or `0x4C` to indicate that no pairing code is required to establish a VCI. This also means that neither the global PIN nor the on-card biometric comparison (OCC) satisfies the access control rules for command execution and data object access within the derived PIV application.

Key History Object

Up to 20 retired key management private keys **MAY** be stored in the derived PIV application. The Key History Object **SHALL** be present in the derived PIV application if the derived PIV application contains any retired key management private keys but **MAY** be present even if no such keys are present in the derived PIV application.

The requirements for the key history object are as described in Sec. 3.3.3 of [SP800-73pt1], except for the following:

- References to *keysWithOnCardCerts* **SHOULD** be interpreted as keys for which the corresponding certificate is populated within the derived PIV application.
- References to *keysWithOffCardCerts* **SHOULD** be interpreted as keys for which the corresponding certificate is not populated within the derived PIV application.
- References to *offCardCertURL* **SHOULD** be interpreted as a URL that points to a file containing the certificates that correspond to all of the retired key management private keys within the derived PIV application, including those for which the corresponding certificate is stored within the derived PIV application.

Retired X.509 Certificates for Key Management

The read access control rules for the retired X.509 certificates for key management and the PKI cryptographic function access rules for corresponding private keys are as described in Sec. 3.3.4 of [SP800-73pt1].

Security Object

The security object **SHALL** be present in the derived PIV application if the discovery object, the key history object, or the optional pairing code reference data container is present. The requirements for the security object are as described in Sec. 3.1.7 of [SP800-73pt1], except for the following:

- The security object for a derived PIV application is signed using a private key whose corresponding public key is contained in a PIV content signing certificate that satisfies the requirements for certificates used to verify signatures on cardholder unique identifiers (CHUID), as specified in Sec. 4.2.1 of [FIPS201].
- The signature field of the Security Object, tag `0xBB`, **SHALL** include the derived PIV credential issuer's certificate.
- The security object **SHALL** include all unsigned data objects (i.e., the discovery object, the key history object, and the pairing code reference data container) within the derived PIV application.

Secure Messaging Certificate Signer

Derived PIV credential applications that support the virtual contact interface (VCI) capability **SHALL** include the secure messaging certificate signer object described in Sec. 3.3.7 of [SP800-73pt1].

Pairing Code Reference Data Container

Derived PIV credential applications that support the virtual contact interface (VCI) using a pairing code **SHALL** include the pairing code reference data container described in Sec. 3.3.8 of [SP800-73pt1].

B.1.2.1. Derived PIV Application Data Object Containers and Associated Access Rules

Section 3.5 of [SP800-73pt1] provides the container IDs and access rules for the mandatory and optional data objects for a derived PIV application with the following mappings:

Table 1. Mapping of Data Objects

Derived PIV Application Data Object	PIV Card Application Data Object
X.509 Certificate for Derived PIV Authentication	X.509 Certificate for PIV Authentication
Security Object	Security Object
X.509 Certificate for Digital Signature	X.509 Certificate for Digital Signature
X.509 Certificate for Key Management	X.509 Certificate for Key Management
Discovery Object	Discovery Object
Key History Object	Key History Object
Retired X.509 Certificate for Key Management [1:20]	Retired X.509 Certificate for Key Management [1:20]
Secure Messaging Certificate Signer	Secure Messaging Certificate Signer
Pairing Code Reference Data Container	Pairing Code Reference Data Container

The detailed data model specifications for each of the data objects of the derived PIV application are the same as the specifications for the corresponding data objects (mapped per Table 1) of the PIV Card application as described in Appendix A of [SP800-73pt1], except for the following:

- The security object for the derived PIV application is optional. It is required if the optional discovery object, the optional key history object, or the optional pairing code reference data container is present.
- The minimum capacity for the security object container **SHALL** be 3000 bytes to allow space for the derived PIV credential issuer's certificate.

B.1.3. Derived PIV Application Data Objects Representation

The ASN.1 object identifiers (OID) and "basic encoding rules – tag length value" (BER-TLV) tags for the mandatory and optional data objects within the derived PIV application are the same as for the corresponding data objects (mapped per Table 1) of the PIV Card application, as described in Sec. 4 of [SP800-73pt1].

B.1.4. Derived PIV Application Data Types and Their Representation

This appendix describes the data types used in the derived PIV application command interface.

B.1.4.1. Derived PIV Application Key References and Security Conditions of Use

Key references are assigned to keys and secrets of the derived PIV application. Table 8 of [SP800-78] and Table 4 of [SP800-73pt1] define the key reference values that **SHALL** be used on the derived PIV application interfaces with the following mappings:

Table 2. Mapping of Key Types

Derived PIV Key Type	PIV Key Type
Derived PIV Activation Secret	PIV Card Application PIN
Activation Secret Unblocking Key	PIN Unblocking Key
Derived PIV Authentication Key	PIV Authentication Key
Derived PIV Token Management Key	Card Management Key
Digital Signature Key	Digital Signature Key
Key Management Key	Key Management Key
Retired Key Management Key	Retired Key Management Key
Derived PIV Secure Messaging Key	PIV Secure Messaging Key

The key reference specifications in Sec. 5.1 of [SP800-73pt1] apply to the corresponding keys included in the derived PIV application (mapped per Table 2), except for the following:

- References to “PIV Card application” are replaced with “derived PIV application.”
- References in the “Security Condition for Use” column to “PIN or OCC” are replaced with “derived PIV activation secret.”

B.1.4.2. Derived PIV Application Cryptographic Algorithm and Mechanism Identifiers

The algorithm identifiers for the cryptographic algorithms that **MAY** be recognized on the derived PIV application interfaces are the symmetric and asymmetric identifiers specified in Table 9 and Table 10 of [SP800-78]. The cryptographic mechanism identifiers that **MAY** be recognized on the derived PIV application interfaces are those specified in Table 5 of [SP800-73pt1].

B.1.4.3. Derived PIV Application Status Words

The status words that **MAY** be returned on the derived PIV application command interface are as specified in Sec. 5.6 of [SP800-73pt1].

B.1.5. Derived PIV Authentication Mechanisms

The derived PIV application supports the following validation steps:

- Credential validation (CredV) is established by verifying the certificates retrieved from the derived PIV application and checking the validity and revocation status of these certificates.
- Derived PIV application holder validation (HolderV) is established when the authenticator holder proves knowledge of the derived PIV activation secret associated with the derived PIV credential that contains valid and unrevoked certificates.

The derived PIV application facilitates a single authentication mechanism, which is a cryptographic challenge and response authentication protocol that uses the derived PIV authentication private key as described in Appendix B.1.2 of [SP800-73pt1] with the following translations:

- References to “PIV application” are replaced with “derived PIV application.”
- References to “PIV auth certificate” are replaced with “derived PIV authentication certificate.”
- References to “PIV Card app ID” are replaced with “derived PIV application ID.”

Authentication can also be performed wirelessly over a virtual contact interface (VCI) if a VCI has been established with the derived PIV application.

B.2. Derived PIV Application Token Command Interface

This appendix contains the technical specifications for the command interface to the derived PIV application surfaced by the card edge of the integrated circuit card (ICC) that represents the removable cryptographic authenticator. The command interface for the derived PIV application **SHALL** implement all of the card commands supported by the PIV Card application as described in [SP800-73pt2], which include:

- SELECT
- GET DATA
- VERIFY
- CHANGE REFERENCE DATA
- RESET RETRY COUNTER
- GENERAL AUTHENTICATE
- PUT DATA
- GENERATE ASYMMETRIC KEY PAIR

The specifications for the token command interface **SHALL** be the same as the specifications for the corresponding card edge commands for a PIV Card as described in [SP800-73pt2], except for the following deviations:

- References to “PIV Card application” are replaced with “derived PIV application.”
- References to “PIV data objects” are replaced with “derived PIV data objects.”
- References to “PIV authentication key” are replaced with “derived PIV authentication key.”
- The derived PIV activation secret **SHALL** satisfy the criteria specified in Appendix B.2.1 of this document rather than Sec. 2.4.3 of [SP800-73pt2].
- In Appendix A:
  - References to “PIV Card application administrator” are replaced with “derived PIV application administrator.”
  - References to “card management key” are replaced with “derived PIV token management key.”

The token platform **SHALL** support a default selected application, which is the application chosen following a cold or warm reset. This default application may be the derived PIV application or another application.

B.2.1. Authentication of an Individual

Knowledge of a secret (specifically the derived PIV activation secret) is how an individual can be authenticated to the derived PIV application.

The derived PIV activation secret **SHALL** be between 6 and 8 bytes in length. If the actual length of the derived PIV activation secret is less than 8 bytes, it **SHALL** be padded to 8 bytes with `0xFF` when presented to the token command interface. The `0xFF` padding bytes **SHALL** be appended to the actual value of the secret. The bytes that comprise the derived PIV activation secret **SHALL** be limited to values `0x30` – `0x39`, `0x41` – `0x5A`, and `0x61` – `0x7A`: the ASCII values for the decimal digits ‘0’ – ‘9’; upper case characters ‘A’ – ‘Z’; and lower case characters ‘a’ – ‘z’. For example,

- Actual derived PIV activation secret: “Part21” or (hexadecimal) `50 61 72 74 32 31`
- Padded derived PIV activation secret presented to the card command interface (hexadecimal): `50 61 72 74 32 31 FF FF`

The derived PIV application **SHALL** enforce the minimum length requirement of 6 bytes for the derived PIV activation secret (i.e., **SHALL** verify that at least the first 6 bytes of the value presented to the card command interface are in the range `0x30` – `0x39`, `0x41` – `0x5A`, or `0x61` – `0x7A`) as well as the other formatting requirements specified in this section.

Appendix C. Example Issuance Processes

This appendix is informative.

The issuance process for a derived PIV credential varies depending on whether it is being issued for use at AAL2 or AAL3. Section 2.2 specifies the requirements for initial issuance. This appendix provides example issuance processes that satisfy those requirements at AAL2 and at AAL3. These examples assume the PKI-AUTH authentication mechanism will be used with a valid PIV Card to enable the issuance process.

C.1. Example Issuance of a PKI-Based Derived PIV Credential at AAL3

An employee requires a derived PIV credential to access a relying party application that requires authentication at AAL3. Their endpoint does not easily accommodate their PIV Card, and the application resides at a different agency that does not support federation, so a PKI-based credential is needed. A request to issue a derived PIV credential is submitted to the agency's approval authority and is approved.

The employee visits their security office or other issuing authority. If the issuance of a derived PIV credential has been approved, they are provided with a USB authenticator capable of supporting the derived PIV application and meeting AAL3 requirements. After authenticating with their PIV Card using the PKI-AUTH authentication mechanism, the USB authenticator is provisioned, which involves the generation of a key pair for the derived PIV authentication certificate within the device's cryptographic module and export of the public key to the IDMS, which generates the certificate and loads it onto the authenticator. The employee is also prompted to establish an activation secret for the credential. The issuer enters information about the new derived PIV credential into the subscriber's PIV identity account. The employee is notified of the binding of the new derived PIV credential by email or postal notification to their address in the PIV identity account.

Additional data elements described in Appendix B.1.2 may also be provisioned on the device.

C.2. Example Issuance of a PKI-Based Derived PIV Credential at AAL2

An employee requires a mobile device for work. The mobile device is ordered, and a request to issue a derived PIV credential is submitted to the agency's approval authority.

Following receipt of the device and approval, the employee starts the binding process remotely — such as from their home — by visiting a derived PIV credential website operated by or on behalf of their PIV Card's home agency IDMS. The website requires TLS client authentication using the PKI-AUTH authentication method with the employee's PIV Card. The employee performs this step from a desktop computer since they cannot use their PIV Card on a mobile device. Having authenticated the employee, the server verifies PIV credential eligibility in the employee's PIV identity account. Once the

employee has successfully authenticated to the server, the issuer generates and displays a binding secret to the employee.

The employee then runs a provisioning application on the mobile device. The application asks the employee to identify themselves and enter the binding secret previously provided from the desktop website to create an activation secret, which will subsequently be used to authenticate to the cryptographic module. The application generates a key pair within the device's cryptographic module and submits the binding secret and newly generated public key to the PIV issuer as part of a certificate request. The PIV issuer authenticates the employee by verifying that the certificate request's binding secret matches the one it previously issued and forwards the public key to the CA, which signs and issues the derived PIV credential (i.e., the derived PIV authentication certificate). The provisioning application loads the derived PIV authentication certificate on the mobile device. The PIV Card issuer enters information about the new derived PIV credential into the subscriber's PIV identity account. The cardholder is notified of the binding of the new derived PIV credential by email or postal notification to their address in the PIV identity account.

Normative requirements for this process are given in [SP800-63B] Sec. 4.1.2.2 and in Sec. 2.2 of this document.

C.3. Example Binding of a Non-PKI-Based Derived PIV Credential at AAL3

An employee requires a derived PIV credential to access a relying party using one or more endpoints that do not accommodate the direct use of a PIV Card. The employee requests a non-PKI-based authenticator capable of authentication at AAL3 and approval to use that authenticator as a derived PIV credential. The agency's approval authority approves the request.

After receiving the approval and authenticator, the employee starts the binding process by authenticating with their PIV Card using PKI-AUTH at a derived PIV credential website operated by or on behalf of the employee's home agency IdMS. The website requires TLS client authentication with the PKI-AUTH authentication method using the employee's PIV Card. Having authenticated the employee, the server verifies eligibility to possess a PIV Card. The employee then inserts (connects) the authenticator to be used as a derived PIV credential and registers (binds) that credential, including establishing a second authentication factor (activation secret or biometric characteristic) if that has not already been done. The website determines whether the authenticator meets AAL3 requirements. Upon successful registration, the home agency's endpoint stores the subscriber's key and appropriate metadata for non-PKI-based PIV authentication. The PIV Card issuer enters information about the new derived PIV credential into the subscriber's PIV identity account. The employee is notified of the binding of the new derived PIV credential by email or postal notification to their address in the PIV identity account.

If the authenticator uses verifier name binding as described in [SP800-63B] Sec. 3.2.5.2, the website used to register the authenticator has to share the same domain name as will be used by the home agency IdMS to authenticate the subscriber so that the same keys are used for registration and authentication.

C.4. Example Binding of a Non-PKI-Based Derived PIV Credential at AAL2

The binding of a non-PKI-based derived PIV credential at AAL2 is identical to that at AAL3, except that the authenticator needs only to meet the requirements of AAL2.

C.5. Example Binding of PACS Credential

To enable a derived PIV credential to be used for physical access as described in Appendix D, the applicant first authenticates using their PIV Card and the PKI-AUTH authentication method. Having authenticated the employee, the server verifies PIV credential eligibility in the applicant's PIV identity account. The issuer generates a new CHUID data object, derived card authentication key, and derived card authentication certificate. If the SM-AUTH authentication method is supported, a key pair is generated. The issuer creates a corresponding derived card verifiable certificate and secure messaging certificate signer object. The issuer transfers the created objects to the derived PIV credential module using a TLS or similar authenticated protected channel. Because the PACS credential is a single authentication factor, it is not necessary to establish an activation factor.

The PIV Card issuer enters information about the new derived PIV credential into the subscriber's PIV identity account. The cardholder is notified of the binding of the new derived PIV credential.

Appendix D. Physical Access

This appendix is normative.

Credentials on PIV cards are commonly used to identify and authenticate individuals accessing government facilities. Agencies **MAY** issue derived PIV credentials for use with physical access control systems. This appendix provides data model and interface requirements for derived PIV applications for physical access. To facilitate compatibility with PIV readers, these requirements reference the requirements for the PIV card and PIV card application specified in [SP800-73pt2].

Authentication to physical access control systems (PACS) using derived PIV credentials **MAY** use the PKI-CAK or SM-AUTH authentication mechanisms described in [SP800-73pt2] and [SP800-116]. Derived PIV credential modules that support PACS **SHALL** support the PKI-CAK authentication mechanism. Physical access **SHALL** be supported by contactless readers that conform to [ISO14443] for the card-to-reader interface and conform to [ISO7816] for data transmitted over the [ISO14443] link. If readers are connected to general-purpose desktop computing systems, they **SHALL** conform to [PCSC] for the reader-to-host system interface and the requirements specified in [SP800-96]. This standard does not specify the reader-to-host system interface in systems where the readers are not connected to general-purpose desktop computing systems.

Since the PKI-CAK and SM-AUTH authentication mechanisms are single-factor, there is no need to establish an activation factor for these physical access methods.

Issuance of derived PIV credentials that support PACS **SHALL** be done in accordance with the post-enrollment binding described in Sec. 2.2 and the PKI-based PIV credential issuance procedures described in Sec. 2.2.1. Issuance of derived PIV credentials in support of PACS without a PIV card **SHALL** follow Sec. 2.2.3.

D.1. PACS Derived PIV Application Data Model and Representation

The data model and representation requirements for the derived PIV application are based on the requirements for the PIV Card application, as described in [SP800-73pt1]. Test requirements and test assertions for testing the derived PIV application and associated derived PIV data objects implemented on removable hardware tokens are specified in [SP800-166], *Derived PIV Application and Data Model Test Guidelines*. The specifications for the mandatory and optional data objects listed below are the same as the specifications for the corresponding data objects on a PIV Card application, as described in [SP800-73pt1], with exceptions as noted.

D.1.1. Derived PIV Application Identifier

Either the PIV card application identifier (AID) defined in Sec. 2.2 of [SP800-73pt1] or the derived PIV application AID, defined in Appendix B, **SHALL** be used. To maximize

compatibility with existing PACS readers, the AID of the PIV card application **SHOULD** be used unless the use of the derived PIV AID for logical access makes this infeasible.

For reference, the AID of the PIV card application is (in hexadecimal):

```
A0 00 00 03 08 00 00 10 00 01 00
```

The AID of the derived PIV application is (in hexadecimal):

```
A0 00 00 03 08 00 00 20 00 01 00
```

The desired application can be selected by providing the full AID listed above or a truncated version that omits the last two bytes '01 00'.

D.1.2. PACS Derived PIV Application Data Model Elements

The derived PIV application **SHALL** contain the following data objects when used for PACS:

Derived CHUID Data Object

The read access control rule for the derived CHUID data object is as described for the CHUID data object specified in Sec. 3.1.2 of [SP800-73pt1] except that it **SHALL** be accessible only via the contactless interface. The FASC-N and card UUID contained within the derived CHUID data object **SHALL** be distinct from the corresponding values on the PIV card and any other derived PIV credential module.[1] This data object is required for access control systems that use the FASC-N or the card UUID in the CHUID to look up authorization information rapidly. The derived CHUID **SHALL NOT** be used for authentication since that authentication method has been withdrawn. If the optional cardholder UUID is included in the derived CHUID data object, it **SHALL** contain the same value as the cardholder's PIV card.

The FASC-N, card UUID, expiration date, and, if present, cardholder UUID **SHALL NOT** be modified post-issuance.

The expiration date included in the derived CHUID data object **SHALL** be the same as the expiration date of the derived card authentication certificate. It **SHALL** be no later than the expiration date of the content signing certificate. There is no requirement to align the expiration date included in the derived CHUID data object with the expiration date of the CHUID data object on the cardholder's PIV Card or with other certificates on the derived PIV credential.

X.509 Certificate for Derived Card Authentication

This data object is required for the PKI-CAK authentication mechanism. The read access control rule for the X.509 certificate for derived card authentication and

[1] This will generally require multiple entries for the cardholder on the access control list — one for each of their derived PIV credential modules and the PIV card.

the PKI cryptographic function access rule for the corresponding private key are as described for the X.509 certificate for card authentication in Sec. 3.1.4 of [SP800-73pt1] with the exception that they **SHALL** only be accessible via the contactless interface. The card UUID value **SHALL** be the same as the one in the derived CHUID data object.

The derived PIV application **MAY** contain the following data objects:

Derived PIV Secure Messaging Key and Derived Card Verifiable Certificate
The PKI cryptographic function access rule for the derived PIV secure messaging key and the read access control rule for the derived card verifiable certificate (DCVC) are as described for the secure messaging key specified in Sec. 5.1.2 of [SP800-73pt1] and Sec. 4.1.5 of [SP800-73pt2], respectively, except that they **SHALL** only be accessible via the contactless interface. These data objects are required for the SM-AUTH authentication mechanism. The card UUID in the derived card verifiable certificate **SHALL** be the same as that in the derived CHUID data object.

Secure Messaging Certificate Signer Object
The read access control rule for the secure messaging certificate signer object is as described in Sec. 3.3.7 of [SP800-73pt1]. This data object is required for the SM-AUTH authentication mechanism.

D.1.2.1. PACS Derived PIV Application Data Object Containers and Associated Access Rules

Section 3.5 of [SP800-73pt1] provides the container IDs and access rules for the PACS data objects for a derived PIV application with the mappings in Table 3.

Table 3. Mapping of Data Objects

Derived PIV Application Data Object	PIV Card Application Data Object	Specification
X.509 Certificate for Derived Card Authentication	X.509 Certificate for Card Authentication	[SP800-73pt1] Appendix A Table 18
Derived CHUID Data Object	CHUID Data Object	[SP800-73pt1] Appendix A Table 10
Derived Card Verifiable Certificate	Card Verifiable Certificate	[SP800-73pt2] Sec. 4.1.5
Secure Messaging Certificate Signer	Secure Messaging Certificate Signer	[SP800-73pt1] Appendix A Table 43

The detailed data model specifications for each of the PACS data objects are the same as the specifications for the corresponding data objects of the PIV Card application cited in

Table 3 above with the exception that, as specified in Sec. D.1.2, they are accessible only over the contactless interface, except for the Secure Messaging Certificate Signer.

Derived card authentication certificates **SHALL** be issued under the `id-fpki-common-devices` or the `id-fpki-common-devicesHardware` policy of [COMMON]. The certificate **SHALL** also include an extended key usage (extKeyUsage) extension asserting `id-PIV-cardAuth`. Derived card authentication certificates **SHALL** comply with the *Alternative PACS Authenticator Certificate* profile in [PROF].

The expiration date of a derived card authentication certificate is based on the issuer's certificate policy and the certificate policy specified above. There is no requirement to align the expiration date of a derived card authentication certificate with the expiration date of the card authentication certificate or the expiration of the PIV Card. This allows a derived PIV credential to continue to act as an active credential while the cardholder's PIV Card is being renewed.

For derived card authentication certificates issued under `id-fpki-common-devices`, the derived card authentication key pair **SHALL** be generated within a cryptographic module that has been validated to [FIPS140] Level 1 or higher. If the key pair is generated outside of the authenticator itself, the private key **SHALL** be transferred via an authenticated protected channel as defined in [SP800-63B], and the authenticator **SHALL** meet the requirements of [SP800-63B] Sec. 2.2.2, including being validated to [FIPS140] Level 1 or higher.

For derived card authentication certificates issued under `id-fpki-common-devicesHardware`, the derived card authentication key pair **SHALL** be generated within a cryptographic module that has been validated to [FIPS140] Level 2 or higher. If the key pair is generated outside of the authenticator itself, the private key **SHALL** be transferred via an authenticated protected channel as defined in [SP800-63B], and the authenticator **SHALL** meet the requirements of [SP800-63B] Sec. 2.3.2, including being validated to [FIPS140] Level 2 or higher.

If present, the derived PIV secure messaging key pair **SHALL** be generated on the authenticator itself. Its private key **SHALL NOT** be exportable. The authenticator **SHALL** be validated to [FIPS140] Level 1 or higher.

The issuer **SHALL** generate the derived PIV card verifiable certificate, the derived CHUID data object, and the secure messaging certificate signer object (if required) and transfer them to the authenticator.

D.1.3. Derived PIV PACS Application Data Objects Representation

The ASN.1 object identifiers (OID) and *basic encoding rules – tag length value* (BER-TLV) tags for the PACS data objects within the derived PIV application are the same as for the corresponding data objects of the PIV Card application (mapped per Table 3), as described in Sec. 4 of [SP800-73pt1].

D.1.4. Derived PIV Application PACS Data Types and Representation

This section describes the data types used in the derived PIV application PACS command interface.

D.1.4.1. Derived PIV Application PACS Key References and Security Conditions

Key references are assigned to keys and secrets of the derived PIV application. Table 8 of [SP800-78] and Table 4 of [SP800-73pt1] define the key reference values that **SHALL** be used on the derived PIV application interfaces with the mappings in Table 4.

Table 4. Mapping of PACS Key Types

Derived PIV PACS Key Type	PIV Key Type
Derived Card Authentication Key	Card Authentication Key
Derived PIV Secure Messaging Key	PIV Secure Messaging Key

The key reference specifications in Sec. 5.1 of [SP800-73pt1] apply to the corresponding keys included in the derived PIV application (mapped per Table 4) except that references to "PIV Card application" are replaced with "derived PIV application."

D.1.4.2. Derived PIV Application PACS Cryptographic Algorithm and Mechanism Identifiers

The algorithm identifiers for the cryptographic algorithms that **MAY** be recognized for PACS use on the derived PIV application interfaces are the asymmetric identifiers specified in Table 9 and Table 10 of [SP800-78]. The cryptographic mechanism identifiers that **MAY** be recognized on the derived PIV application interfaces are those specified in Table 5 of [SP800-73pt1].

D.1.4.3. Derived PIV Application Status Words

The status words that **MAY** be returned for PACS use on the derived PIV application command interface are as specified in Sec. 5.6 of [SP800-73pt1].

D.1.5. Derived PIV PACS Authentication Mechanisms

The derived PIV application supports the following validation steps for PACS use:

- Credential validation (CredV) is established by verifying the certificates retrieved from the derived PIV application and checking the validity and revocation status of these certificates.

- As with the PKI-CAK and SM-AUTH authentication mechanisms for the PIV card, derived PIV holder validation (HolderV) for PACS is only established by possession of the derived PIV credential (i.e., these are single-factor authentication mechanisms).

Derived PIV applications that support PACS **SHALL** support PKI-CAK, a cryptographic challenge and response authentication protocol that uses the derived card authentication key as described in Appendix B.1.3 of [SP800-73pt1]. Derived PIV applications **MAY** also support SM-AUTH — a key establishment protocol that uses the derived PIV secure messaging key, as described in Appendix B.1.7 of [SP800-73pt1]. The following translations apply to the use of these protocols by a derived PIV credential:

- References to “PIV application” are replaced with “derived PIV application.”
- References to “Card auth certificate” are replaced with “derived card authentication certificate.”
- References to “SM parameters” are replaced with “derived SM parameters”
- References to “PIV Card app ID” are replaced with “derived PIV application ID.”

D.2. Derived PIV Application Token Command Interface

This appendix contains the technical specifications for the command interface to the derived PIV application surfaced by the wireless interface to the derived PIV credential for PACS. The command interface for the derived PIV application **SHALL** implement a subset of the card commands supported by the PIV Card application, as described in [SP800-73pt2], which include:

- SELECT
- GET DATA
- GENERAL AUTHENTICATE
- PUT DATA
- GENERATE ASYMMETRIC KEY PAIR

The specifications for the token command interface **SHALL** be the same as the specifications for the corresponding card edge commands for a PIV Card, as described in [SP800-73pt2], except for the following deviations:

- References to “PIV Card application” are replaced with “derived PIV application.”
- References to “PIV data objects” are replaced with “derived PIV data objects.”
- References to “card authentication key” are replaced with “derived card authentication key.”
- In Appendix A:

- References to “PIV Card application administrator” are replaced with “derived PIV application administrator.”
- References to “card management key” are replaced with “derived PIV token management key.”

The token platform **SHALL** support a default selected application, which is the application chosen immediately following a cold or warm reset. This default application **MAY** be the derived PIV application or another application.

D.2.1. Authentication of an Individual for PACS

The two authentication mechanisms for PACS are PKI-CAK and SM-AUTH, which rely only on possession of the derived PIV credential for holder validation (HolderV). Therefore, an activation secret is not used for enhanced holder validation.

D.3. Invalidation of PACS Derived PIV

A derived PIV credential that is used for physical access **SHALL** be invalidated when the associated PIV identity account is terminated or when the PACS credential or the device on which it resides has been lost or compromised. The IdMS **SHALL** revoke the card authentication certificate associated with the lost or compromised device or all such certificates associated with the terminated PIV identity account. The home agency IdMS **SHOULD** direct all physical access control systems known to use the credential to remove it from their access control lists.

Appendix E. Glossary

This appendix is informative.

Selected terms used in this guideline are defined below. All other significant technical terms used within this document are defined in other key documents, including [FIPS201], [SP800-63A], [SP800-63B], [SP800-73pt1], and [SP800-73pt2].

applicant
A PIV cardholder who has applied for but has yet to be issued a derived PIV credential.

derived PIV application
A standardized application based on the PIV Card's PIV application that resides on a removable or wireless cryptographic token. It hosts PKI-based derived PIV credentials and associated mandatory and optional elements.

derived PIV credential module
A collection of objects (e.g., certificates, keys, etc.) that provide derived PIV functionality in a derived PIV application or other device.

home agency
The government agency responsible for maintaining the PIV identity account and issuing a PIV Card. While another agency may sometimes perform the enrollment and identity proofing process, the home agency is responsible for monitoring ongoing eligibility and initiating termination if appropriate.

home agency IdMS
An identity management system operated by the home agency or on their behalf by an authorized third party or shared service provider that houses the PIV identity accounts of cardholders.

PIV identity account
The logical record that contains credentialing information for a given PIV cardholder. This is stored within the *home agency IdMS* and includes PIV enrollment data, cardholder identity attributes, information regarding the cardholder's PIV card, and any derived PIV credentials bound to the account.

PKI-based derived PIV credential
An X.509 derived PIV authentication certificate, which is issued in accordance with the requirements specified in this document, where one or more X.509 certificates on the applicant's PIV Card serve as the original credential. The derived PIV credential is an additional common identity credential under HSPD-12 and FIPS 201 that a federal department or agency issues.

non-PKI-based derived PIV credential
An authenticator (as defined in [SP800-63B]) that has been bound to a PIV identity account at a subscriber's home agency that does not use the PKI-based authentication mechanisms described in [FIPS201]. A non-PKI-based derived PIV credential bound to the subscriber's PIV identity account can be used for federated authentication via the cardholder's home agency IdMS.

subscriber
A PIV cardholder to whom a derived PIV credential has been issued.

verifier
An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or more authenticators using an authentication protocol. To do this, the verifier needs to confirm the authenticators' binding with the subscriber account and check that the subscriber account is active.

Appendix F. Acronyms and Abbreviations

This appendix is informative.

Selected abbreviations used in this guideline are defined below.

AAL
Authentication Assurance Level

AID
Application Identifier

ASCII
American Standard Code for Information Interchange

CA
Certificate Authority

CHUID
Cardholder Unique Identifier

ICC
Integrated Circuit Card

FIPS
Federal Information Processing Standard

OCC
On-Card (biometric) Comparison

PIN
Personal Identification Number

PIV
Personal Identity Verification

PKI
Public Key Infrastructure

TLS
Transport Layer Security

VCI
Virtual Contact Interface

Appendix G. Change Log

This appendix is informative. It provides an overview of the changes to SP 800-157 since its initial release.

- Throughout — Removed restrictions to only use derived PIV credentials on mobile devices
- Sections 1.1, 1.2 — Allowed binding of non-PKI-based derived PIV credentials at AAL2 and AAL3
- Sections 1.2, 2.1, 2.2, 3.1, 3.2, C — Changed assurance levels from LOA to AAL
- Sections 1.4, 2.2 — Removed relationship to obsolete OMB memoranda
- Section 2.1 — Added life cycle of non-PKI-based derived PIV credentials
- Sections 2.2.1, 2.2.2 — Added detail on issuance for PKI and non-PKI-based derived PIV credentials
- Sections 2.3.1, 2.3.2 — Added detail on maintenance for PKI and non-PKI-based derived PIV credentials
- Sections 2.4, 2.4.1, 2.4.2 — Added invalidation detail, replacing linkage with PIV Card
- Section 3.1, 3.2 — Reorganized sections into PKI and non-PKI-based derived PIV credential requirements
- Section 3.1.3 — Removed specific physical details for authenticators
- Sections 3.1.4, 3.2.3 — Referenced SP 800-63B for activation requirements
- Section 3.3 — Added reference to binding requirements in SP 800-63B
- Appendix B.1.2, B.1.3 — Added secure messaging and VCI capabilities for removable and wireless authenticators
- Appendix C.1 — Added reference to issuance requirements in SP 800-63B
- Appendix C.2 — Updated existing PIV credential issuance example and added example of issuance of non-PKI-based derived PIV credentials
- Appendix D — New appendix on the use of derived PIV credentials with physical access control systems