NIST Special Publication
NIST SP 800-157r1 ipd

Guidelines for Derived Personal Identity Verification (PIV) Credentials

Initial 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.ipd

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

NIST Special Publication
NIST SP 800-157r1 ipd

Guidelines for Derived Personal Identity Verification (PIV) Credentials

Initial 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.ipd

January 2023

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 (2023) Guidelines for Derived Personal Identity Verification (PIV) Credentials. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-157r1 ipd. https://doi.org/10.6028/NIST.SP.800-157r1.ipd

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

January 10, 2023 - ~~March 24~~ April 21, 2023

Submit Comments

mailto:piv comments@nist.gov

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

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.

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

Note to Reviewers

Public draft SP 800-157r1 *Guidelines for Derived Personal Identity Verification (PIV) Credentials* expands the use of derived PIV credentials beyond mobile devices to include non-PKI-based phishing resistant multi-factor credentials. The draft details the expanded set of derived PIV credentials in a variety of form factors and authenticator types as envisioned in OMB Memoranda M-19-22, M-22-09, and subsequently outlined in FIPS 201-3. The cross-domain and interagency use of these credentials is provided by federation protocols outlined in public draft SP 800-217 Guidelines for PIV Federation. Both documents are closely aligned with draft release SP 800-63-4 *Digital Identity Guidelines*. NIST hopes that the draft document enables a close alignment with new

and emerging digital authentication and federation technologies employed in the federal government, while maintaining a strong security posture.

NIST is specifically interested in comments on and recommendations for the following topics:

1. Are the new controls for issuance, use, maintenance, and termination of non-PKI-based derived PIV credentials clear and practical to implement?
2. Are phishing-resistant authenticators available to meet agency use cases as well as the requirements for derived PIV authentication?
3. Are the new controls sufficient to provide comparable assurance to PIV Cards and other derived PIV credentials?

Reviewers are encouraged to comment on all or part of both SP 800-157r1 and SP 800-217. NIST requests that all comments be submitted by 11:59pm Eastern Time on March 24, 2023. Please submit your comments to piv_comments@nist.gov. NIST will review all comments and make them available at the NIST Computer Security Resource Center (CSRC) website. Commenters are encouraged to use the comment template provided on the NIST Computer Security Resource Center website.

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. 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, that are issued by a federal department or agency and may be used when the use of a PIV Card is not practical. 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 the use of the PIV Card for electronic authentication works well with many traditional desktop and laptop computers, it is not well-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 PKI Infrastructure 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.

In order 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. The technical details for the expanded set of derived PIV credentials is specified in this revision of SP 800-157 (SP 800-157, Revision 1) in a variety of form factors. Non-PKI-based derived PIV credentials are authenticators (as defined in [SP800-63B]) that 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 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 home agency — particularly when a non-PKI-based derived PIV credential is presented in authentication — federation allows connection across security domains as detailed in [SP800-217].

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 the use of PIV Cards is deemed impractical for authentication. This guideline specifies the use of authenticators with alternative form factors to the PIV Card that may be inserted into endpoints, such as USB authenticators, authenticators that are connected wirelessly to endpoints, or authenticators that are embedded in endpoints. Authenticators used as derived PIV credentials must meet the requirements for either hardware or software cryptographic authenticators. The use of 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 in order to authenticate the credential holder to remote systems.

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 as that used for authentication with a PIV Card.
2. Use of non-PKI-based authenticators. When non-PKI-based authenticators are used, derived PIV credentials are only used to authenticate with the home agency of the associated PIV Card. Interoperability with other agencies is achieved through the use of 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 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. While the PIV Card may be used as the basis for issuing other types of derived credentials, the issuance of these other credentials is outside of the scope of this document.

Derived PIV credentials are:

- Issued based on possession and control of the PIV Card,

- Represented in the PIV identity account at the home agency, and
- Issued in accordance with this document.

This document provides technical guidelines on:

- The primary lifecycle activities for the derived PIV credential — initial issuance, maintenance, and termination — and the requirements for each activity to ensure security and
- The derived PIV credential, including cryptographic specifications, types of implementation that are permitted, mechanisms for activation and use of the credential, and certificate policies if applicable.

This publication also includes an informative annex that provides recommendations for the inclusion of digital signature and key management keys on devices that host a derived PIV credential.

1.3. Audience

This document is intended for stakeholders who will be 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 in order 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 lifecycle 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 hardware implementations. This appendix is *normative* for implementation of PKI-based derived PIV credentials on removable (non-embedded) or wireless hardware cryptographic tokens.
- Appendix C provides example issuance processes for derived PIV credentials. This appendix is *informative*.
- Appendix D contains a glossary of selected terms used in this document. This appendix is *informative*.
- Appendix E defines acronyms and other abbreviations used in this document. This appendix is *informative*.
- Appendix F provides a list of 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 not yet been issued a derived PIV credential, and the term *subscriber* refers to a PIV cardholder to whom a derived PIV credential has been issued.

2. Lifecycle Activities and Related Requirements

This section is normative.

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

Issuers of derived PIV credentials **SHALL** document the process for each of the lifecycle activities described below. In accordance with [HSPD-12], the reliability of the derived PIV credential issuer **SHALL** be established through an official accreditation process.

2.1. Derived PIV Credential Lifecycle Activities

The derived PIV credential lifecycle consists of the three classes of activities described above. The activities that take place at the manufacturer during fabrication and pre-personalization of the authenticator (as applicable) are not considered part of this lifecycle model. Figure 1 presents the PKI-based derived PIV credential activities alongside the PIV Card lifecycle activities. Figure 2 presents the corresponding lifecycle activities for non-PKI-based derived PIV credentials.

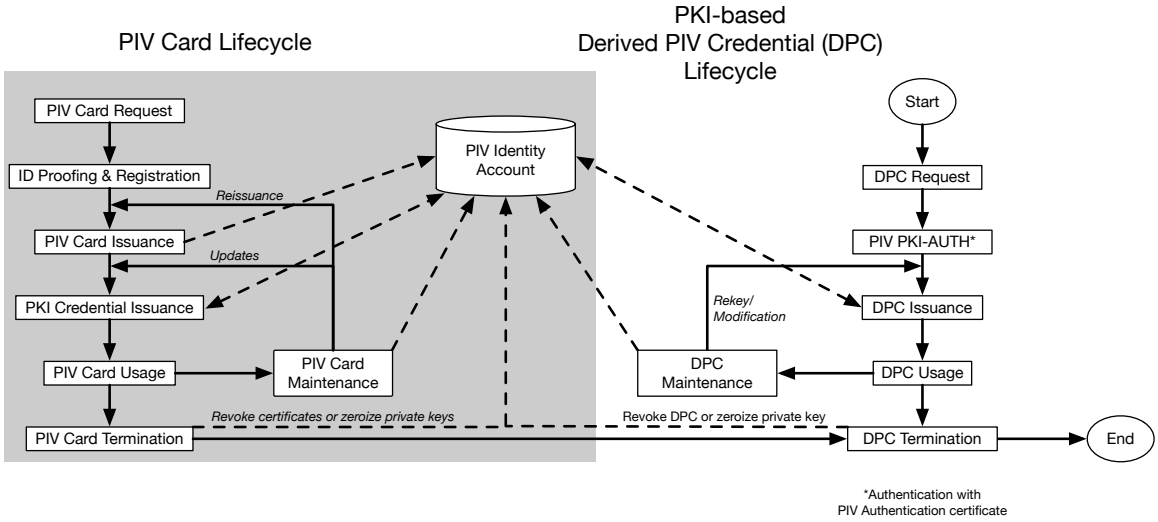

Figure 1. PKI-based derived PIV credential lifecycle activities

The lifecycle of a derived PIV credential begins with the issuance of a derived PIV credential on an approved device or authenticator associated with the applicant. This may be part of the process 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

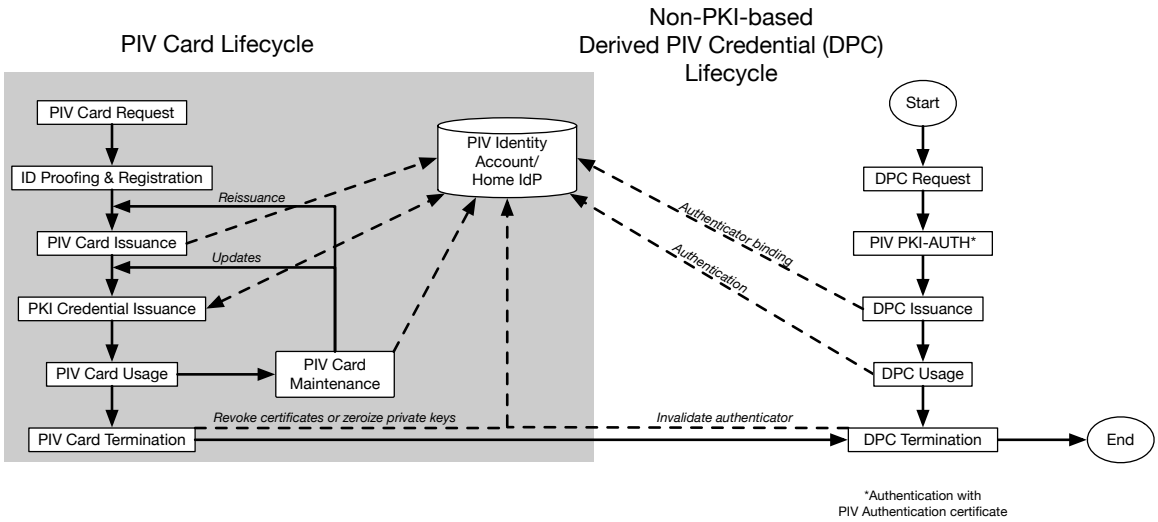

Figure 2. Non-PKI-based derived PIV credential lifecycle activities

a certificate that is nearing expiration. Certificate modification is used to replace a certificate if information about the subscriber that appears in the certificate, such as 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 that contains the private key corresponding 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 by 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

The issuance of 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 as well as the requirements in this section. The term *issuance* is used in cases where the device or authenticator is provided to the subscriber as well as 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** be issued only by the home agency of the associated PIV identity account. Derived PIV credentials **SHALL** be issued only to devices (such as 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. Authorization policies for issuance **SHALL** be documented by each issuer.

Derived PIV credentials **MAY** be issued remotely or in person. At the time of issuance, the applicant **SHALL** authenticate to the derived PIV credential issuer using their PIV Card. This authentication **SHALL** be performed using the PKI-AUTH authentication mechanism described in Sec. 6.2.3.1 of [FIPS201]. This authentication **MAY** be performed remotely. 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.

All derived PIV credentials for use at AAL3 **SHALL** be issued in accordance with the following additional requirements. The applicant **SHALL** identify themself using a biometric sample that can be verified against their PIV Card or against the biometric information in their enrollment record. If the issuance process consists of two or more transactions, the applicant **SHALL** identify themself using a biometric sample that can be verified against either their PIV Card or against a biometric that was recorded in a previous transaction. The issuer **SHALL** retain the biometric sample used to verify the applicant for future reference.

After the applicant has been authenticated, a derived PIV credential **MAY** be issued and associated with the cardholder's PIV identity account. The newly issued derived PIV credential **SHALL** be represented in the cardholder's PIV identity account.

When a new derived PIV credential is associated with a PIV identity account, the issuer **SHALL** promptly notify the PIV cardholder of the binding of a derived PIV credential through an independent means that would not afford an attacker the opportunity to interfere with the notification. More than one independent notification method **MAY** be used to ensure prompt receipt by the cardholder.

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. 5.2.5.

This guideline does not preclude the issuance of multiple derived PIV credentials to the same applicant on the basis of the same PIV Card. 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 of them to someone else. Accordingly, issuers **MAY** place a limit on the number of active derived PIV credentials that a subscriber may have.

2.2.1. PKI-based Derived PIV Credential Issuance

Issuance of a PKI-based derived PIV credential requires the generation of a public/private keypair followed by the creation of a corresponding authentication certificate by the CSP. For a derived PIV credential capable of being used at AAL3, the keypair **SHALL** be generated in the device (authenticator or endpoint) that will house the derived PIV credential. The device **SHALL** send the certificate signing request that contains the public key to the CSP, which **SHALL** return an X.509 authentication certificate that **SHALL** be stored on the credential. The CSP **SHALL** retain a copy of the issued certificate for use should revocation be required. For a derived PIV credential that is issued for use only at AAL2, the same procedure **MAY** be used, or the CSP **MAY** generate a keypair and corresponding certificate and send the certificate and private key to the device over an authenticated protected channel for installation. The CSP **SHALL** immediately 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 either through the use of strong access controls for the stored private key or through decryption of the private key using an encryption key that is 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 authenticator is not directly provided by the issuer (i.e., the home agency), 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 a memorized secret or biometric activation factor (or both) for the authenticator and successfully authenticate using that authenticator. The issuance process with a single-factor authenticator **SHALL** prompt the applicant to register a memorized secret that meets the requirements of [SP800-63B] Sec. 5.1.1 and that will be verified along with the physical authenticator in the authentication process.

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) being used. Maintenance activities include rekeying, modification of certificates, and replacement of an activation factor (biometric or memorized secret) as appropriate.

Derived PIV credentials are unaffected when the subscriber replaces their PIV Card with a new one (reissuance) or when the PIV Card is lost, stolen, or damaged. The ability for the subscriber to use a derived PIV credential is especially useful 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 data (biometric or memorized 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 performed 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.

Some maintenance activities for the subscriber's PIV Card may trigger corresponding maintenance activities for the derived PIV credential since the derived PIV credential will need to 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.

2.3.2. Non-PKI-based Derived PIV Credential Maintenance

The maintenance activities for non-PKI-based derived PIV credentials are somewhat simpler than for PKI-based derived PIV credentials since the former do not contain information about the cardholder and do not carry a specific expiration date. Identity information **SHALL** be maintained in the PIV identity account and **SHALL** be updated when needed.

Updating a separate memorized secret used with a single-factor authenticator for use at AAL2 **SHALL** be performed in a mutually authenticated protected session with the home agency. The update **SHALL** require the entry of the current memorized secret used for activation. If resetting the memorized secret is required because the subscriber has forgotten the memorized secret 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 Card **SHALL** be invalidated when the associated PIV identity account is terminated, typically due to the cardholder's loss of PIV Card 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, cardholder eligibility, and all derived PIV credentials are maintained in one account — the PIV identity account — and maintained by the home agency.

The issuer of the derived PIV credential **SHALL NOT** solely rely on tracking the revocation status of the PIV authentication certificate as a means of tracking the termination status of the PIV Card. This is because there are situations in which the PIV authentication certificate is not revoked even though the PIV Card has been terminated and subsequently replaced with a new card. This may happen, for example, when a terminated PIV Card is collected and either zeroized or destroyed by an agency. In this case and in accordance with [FIPS201], the corresponding PIV authentication certificate does not need to be revoked.

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 export of the private key 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 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. Separate hardware-based 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 both 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. 5.1.

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 revision of SP 800-157. Additional requirements for PKI-based derived PIV credentials that are removable or wireless are found in Appendix B.

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 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 certificate policy of the issuer. 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. However, in many cases, aligning the expiration dates will simplify lifecycle management.

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 hardware cryptographic module that meets the requirements of [SP800-63B] Sec. 4.2.2, 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. 4.2.2, including being validated to [FIPS140] Level 1 or higher.

3.1.3. Allowable Authenticator Types

Phishing-resistant multi-factor cryptographic authenticators **SHALL** be used for PKI-based derived PIV authentication. A multi-factor cryptographic device authenticator as specified in [SP800-63B] Sec. 5.1.9.1 **SHALL** be used for derived PIV authentication at AAL3. Either a multi-factor cryptographic device authenticator or a multi-factor cryptographic software authenticator as specified in [SP800-63B] Sec. 5.1.8.1 **SHALL** be used for derived PIV authentication at AAL2.

3.1.4. Activation Data

Activation of the derived PIV authenticator using a memorized secret **SHALL** meet the requirements of [SP800-63B] Sec. 5.2.11. Activation using a biometric characteristic **SHALL** meet the requirements of [SP800-63B] Sec. 5.2.3. Unlocking the device that houses a derived PIV authenticator (e.g., mobile phone) **SHALL NOT** be considered activation of the authenticator. Separate entry of the activation secret or presentation of a biometric factor **SHALL** be performed to use the authenticator. The same secret or biometric factor used to unlock the device **MAY** be used to activate the authenticator.

If the memorized secret used for activation or the biometric activation factor needs to be changed, entry of the current memorized 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, the home agency **SHALL** be required to input the PIN unblocking key (PUK). If the PUK is not implemented by the authenticator or cannot be provided, either the authenticator certificates **SHALL** be revoked or the associated private keys **SHALL** be destroyed or zeroized. A new derived PIV credential MAY then be obtained.

3.2. Non-PKI-based Derived PIV Credentials

When used, non-PKI-based credentials **SHALL** be used to authenticate only to the home agency of the associated PIV Card.

3.2.1. Allowable Authenticator Types

Phishing-resistant multi-factor or single-factor cryptographic authenticators **SHALL** be used for non-PKI-based derived PIV authentication. A multi-factor cryptographic device authenticator as specified in [SP800-63B] Sec. 5.1.9.1 or a single-factor cryptographic device authenticator as specified in [SP800-63B] Sec. 5.1.7.1 **SHALL** be used for derived PIV authentication at AAL3. Either a cryptographic device authenticator or a multi-factor cryptographic software authenticator as specified in [SP800-63B] Sec. 5.1.8.1 or a single-factor cryptographic software authenticator as specified in [SP800-63B] Sec. 5.1.6.1 **SHALL** be used for derived PIV authentication at AAL2. All single-factor authenticators **SHALL** be used in conjunction with a memorized secret that meets the requirements of [SP800-63B] Sec. 5.1.1.1.

3.2.2. Cryptographic Specifications

Authenticators used as non-PKI-based derived PIV credentials **SHALL** meet the cryptographic requirements specified in [SP800-63B] Sec. 5.1 for the corresponding authenticator type.

3.2.3. Activation Data

Activation of a multi-factor authenticator being used as a derived PIV credential using a memorized secret **SHALL** meet the requirements of [SP800-63B] Sec. 5.2.11. Activation using a biometric characteristic **SHALL** meet the requirements of [SP800-63B] Sec. 5.2.3. Unlocking the device that houses the authenticator (e.g., mobile phone) **SHALL NOT** be considered activation of the authenticator. Separate entry of the activation secret or presentation of a biometric factor **SHALL** be performed to use the authenticator. The same activation secret or biometric factor used to unlock the device **MAY** be used to activate the authenticator.

If the memorized secret used for activation 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, the activation secret and attempt counter MAY be reset by centralized management by the home agency. If centralized reset is not available, the authenticator **SHALL** be reset and require re-binding to the PIV identity account, as described in Sec. 3.3.

3.3. Binding Derived PIV Credentials

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, as described in [SP800-63B] Sec. 6.1.2.4. In all cases, binding **SHALL** require the use of the PIV-AUTH authentication mechanism specified in [FIPS201].

References

[COMMON] Federal Public Key Infrastructure Policy Authority (2021) X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. (Federal CIO Council), Version 2.2 [or as amended]. Available at https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.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

[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 (2022) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63A-4 ipd [or as amended]. https://doi.org/10.6028/NIST.SP.800-63a-4.ipd

[SP800-63B] Temoshok D, Fenton JL, Choong YY, Lefkovitz N, Regenscheid A, Richer JP (2022) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63B-4 ipd [or as amended]. https://doi.org/10.6028/NIST.SP.800-63b-4.ipd

[SP800-73] Cooper DA, Ferraiolo H, Mehta K, Francomacaro S, Chandramouli R, Mohler J (2015) Interfaces for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-73-4 [or as amended]. https://doi.org/10.6028/NIST.SP.800-73-4

[SP800-78] Polk WT, Dodson DF, Burr WE, Ferraiolo H, Cooper DA (2015) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (National

Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-78-4 [or as amended]. https://doi.org/10.6028/NIST.SP.800-78-4

[SP800-79] Ferraiolo H, Chandramouli R, Ghadiali N, Mohler J, Shorter S (2015) Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-79-2 [or as amended]. https://doi.org/10.6028/NIST.SP.800-79-2

[SP800-124] Souppaya M, Scarfone K (2013) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124r1 [or as amended]. https://doi.org/10.6028/NIST.SP.800-124r1

[SP 800-217] Ferraiolo H, Regenscheid A, Richer JP (2023) 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 ipd [or as amended]. https://doi.org/10.6028/NIST.SP.800-217.ipd

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.

For most subscribers, it will 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. Similarly, copies of some or all of the PIV Card's retired key management private keys and certificates should be stored in the derived PIV credential keystore. 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 in order 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 taken into account at the time that the key management certificate that will be placed on the PIV Card is issued. Key recovery mechanisms are encouraged for key management keys that will be 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 Hardware Cryptographic Devices

This appendix is normative.

This appendix provides data model and interface requirements for PKI-based derived PIV applications that are implemented on removable or wireless hardware cryptographic tokens.

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 [SP800-73] Part 1. 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 [SP800-73] Part 1.

B.1.1. Derived PIV Application Identifier

The application identifier (AID) of the derived PIV application **SHALL** be (in hexadecimal):

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

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

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

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 [SP800-73] Part 1.

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 [SP800-73] Part 1.

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 [SP800-73] Part 1.

Discovery Object

The requirements for the discovery object are as described in Sec. 3.3.2 of [SP800-73] Part 1, 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 [SP800-73] Part 1, 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 [SP800-73] Part 1.

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 [SP800-73] Part 1, 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.
- 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 **SHALL** be included in the security object.

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 [SP800-73] Part 1.

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 [SP800-73] Part 1.

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

Section 3.5 of [SP800-73] Part 1 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 [SP800-73] Part 1, 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 in order 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 [SP800-73] Part 1.

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

This appendix provides a description of 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 6-1 of [SP800-78] and Table 4 of [SP800-73] Part 1 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 [SP800-73] Part 1 are applicable 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 6-2 and Table 6-3 of [SP800-78]. The cryptographic mechanism identifiers that **MAY** be recognized on the derived PIV application interfaces are those specified in Table 5 of [SP800-73] Part 1.

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 [SP800-73] Part 1.

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 [SP800-73] Part 1 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."

The 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 hardware cryptographic token. The command interface for the derived PIV application **SHALL** implement all of the card commands supported by the PIV Card application as described in [SP800-73] Part 2, 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 [SP800-73] Part 2, 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 [SP800-73] Part 2.
- 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 selected application that immediately 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 memorized secret (specifically the derived PIV activation secret) is the means by which 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 the derived PIV credential is being issued at AAL2 or AAL3. Section 2.2 specifies the requirements for initial issuance. This appendix provides two example issuance processes that satisfy those requirements: one at AAL2 and another at AAL3.

C.1. Example Issuance of a Derived PIV Credential at AAL2

The following is an example of a PKI-based derived PIV credential.

An employee requires a mobile device for work. The mobile device is ordered, and a request for the issuance of 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. The website requires TLS client authentication using the PIV authentication certificate on 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. By requiring and validating a PIV Authentication certificate when connecting to the website, the server authenticates the employee and verifies that the employee is still eligible to possess a PIV Card. If the employee successfully authenticates 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 themself and enter the binding secret that was 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 binding secret in the certificate request matches the one that 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.

Normative requirements for this process are given in [SP800-63B] Sec. 6.1.2.4 and in Sec. 2.2 of this document.

C.2. Example Binding of a 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 request is approved by the agency's approval authority.

After receiving the approval and authenticator, the employee starts the binding process by authenticating with their PIV Card at a derived PIV credential website operated by or on behalf of the PIV cardholder's home agency. The employee additionally provides a biometric sample that can be verified against their PIV Card. The website requires TLS client authentication using the PIV authentication certificate on the employee's 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 subscriber's key and appropriate metadata are stored for use by the home agency's endpoint 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 cardholder is notified of the binding of the new derived PIV credential.

If the authenticator uses verifier name binding as described in [SP800-63B] Sec. 5.2.5.2, the website used to register the authenticator has to share the same domain name as will be used by the home agency to authenticate the subscriber so that the same keys are used for registration and authentication.

Appendix D. Glossary

This appendix is informative.

Selected terms used in the 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], and [SP800-73].

applicant
A PIV cardholder who has applied for but has not yet been 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 hardware cryptographic token. It hosts a PKI-based derived PIV credential and associated mandatory and optional elements.

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

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 the PIV authentication certificate on the applicant's PIV Card serves as the original credential. The derived PIV credential is an additional common identity credential under HSPD-12 and FIPS 201 that is issued by a federal department or agency.

non-PKI-based derived PIV credential
An authenticator that has been bound to a PIV identity account at a subscriber's home agency and that can be used for federated authentication to applications as an alternative to the subscriber's PIV Card.

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 binding of the authenticators with the subscriber account and check that the subscriber account is active.

Appendix E. 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

CSP
Cetificate Service Provider

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 F. 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 lifecycle 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