NIST Special Publication 800-157

Guidelines for Derived Personal Identity Verification (PIV) Credentials

Hildegard Ferraiolo
David Cooper
Salvatore Francomacaro
Andrew Regenscheid
Jason Mohler
Sarbari Gupta
William Burr

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-157

INFORMATION SECURITY

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-157

Guidelines for Derived Personal Identity Verification (PIV) Credentials

Hildegard Ferraiolo
David Cooper
Salvatore Francomacaro
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

William Burr
Dakota Consulting, Inc.
Silver Spring, MD

Jason Mohler
Sarbari Gupta
Electrosoft Services, Inc.
Reston, VA

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-157

December 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. 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, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

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.

National Institute of Standards and Technology Special Publication 800-157
Natl. Inst. Stand. Technol. Spec. Publ. 800-157, 33 pages (December 2014)
http://dx.doi.org/10.6028/NIST.SP.800-157
CODEN: NSPUE2

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 NIST, 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. All NIST publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899-8930
Email: piv_derived@nist.gov

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, interoperable public key infrastructure (PKI) based identity credentials that are issued by Federal departments and agencies to individuals who possess and prove control over a valid PIV Card. The scope of this document includes requirements for initial issuance and maintenance of these credentials, certificate policies and cryptographic specifications, technical specifications for permitted cryptographic token types and the command interfaces for the removable implementations of such cryptographic tokens.

Keywords

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

Acknowledgments

The authors, David Cooper, Hildegard Ferraiolo, Salvatore Francomacaro and Andrew Regenscheid of the National Institute of Standards and Technology (NIST), William Burr of Dakota Consulting, Inc., and Sarbari Gupta and Jason Mohler of Electrosoft Services, Inc., wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content and development. Special thanks to the Federal Identity, Credential and Access Management (FICAM) Logical Access Working Group (LAWG) for the review and contributions to the document.

Trademark Information

All registered trademarks or trademarks belong to their respective organizations.

Executive Summary

The deployment of PIV Cards and their supporting infrastructure was initiated in 2004 by Homeland Security Presidential Directive-12 (HSPD-12) with a directive to eliminate the wide variations in the quality and security of authentication mechanisms used across Federal agencies. The mandate called for a common identification standard to promote interoperable authentication mechanisms at graduated levels of security based on the environment and the sensitivity of data. In response, the 2005 Federal Information Processing Standard (FIPS) 201 specified a common set of credentials in a smart card form factor, known as the Personal Identity Verification (PIV) Card, which is currently used government-wide, as intended, for both physical access to government facilities and logical access to Federal information systems.

At the time that FIPS 201 was first published, logical access was geared towards traditional computing devices (i.e., desktop and laptop computers) where the PIV Card provides common authentication mechanisms through integrated readers across the federal government. With the emergence of a newer generation of computing devices and in particular with mobile devices,[1] the use of PIV Cards has proved challenging. Mobile devices lack the integrated smart card readers found in laptop and desktop computers and require separate card readers attached to devices to provide authentication services from the device. For some departments and agencies, the use of PIV Cards and separate card readers is a practical solution for authentication from mobile devices. Other departments and agencies may plan to take advantage of Near Field Communication (NFC) to communicate with the PIV Card from NFC-enabled mobile devices. These solutions are summarized in Section 1.1, *Background*, and provide the complete picture of mobile device PIV-enablement.

NIST Special Publication (SP) 800-157 does not address use of the PIV Card with mobile devices, but instead provides an alternative to the PIV Card in cases in which it would be impractical to use the PIV Card. Instead of the PIV Card, SP 800-157 provides an alternative token, which can be implemented and deployed directly with mobile devices (such as smart phones and tablets). The PIV credential associated with this alternative token is called a Derived PIV Credential. The use of a different type of token greatly improves the usability of electronic authentication from mobile devices to remote IT resources.

Derived PIV Credentials are based on the general concept of derived credentials in SP 800-63-2, which leverages identity proofing and vetting results of current and valid credentials. When applied to PIV, identity proofing and vetting processes do not have to be repeated to issue a Derived PIV Credential. Instead, the user proves possession of a valid PIV Card to receive a Derived PIV Credential. To achieve interoperability with the PIV infrastructure and its applications, a Derived PIV Credential is a PKI credential.[2]

[1] A mobile device, for the purpose of this document is a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.

[2] 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 the scope of this document. Only derived credentials issued in accordance with this document are considered to be PIV credentials.

Table of Contents

Executive Summary .... **iv**

1. Introduction **1**

1.1 BACKGROUND 1
1.2 PURPOSE AND SCOPE 2
1.3 AUDIENCE: 3
1.4 DOCUMENT STRUCTURE 3
1.5 KEY TERMINOLOGY 4

2. Lifecycle Activities and Related Requirements **5**

2.1 DERIVED PIV CREDENTIAL LIFECYCLE ACTIVITIES 5
2.2 INITIAL ISSUANCE 6
2.3 MAINTENANCE 7
2.4 LINKAGE WITH PIV CARD 8

3. Technical Requirements **10**

3.1 CERTIFICATE POLICIES 10
3.2 CRYPTOGRAPHIC SPECIFICATIONS 10
3.3 CRYPTOGRAPHIC TOKEN TYPES 10
3.3.1 Removable (Non-Embedded) Hardware Cryptographic Tokens 11
3.3.2 Embedded Cryptographic Tokens 12
3.4 ACTIVATION DATA 13

List of Appendices

Appendix A— Digital Signature and Key Management Keys (Informative) **15**

Appendix B— Data Model and Interfaces for Removable (Non-Embedded) Hardware Cryptographic Tokens (Normative) **16**

B.1 DERIVED PIV APPLICATION DATA MODEL AND REPRESENTATION 16
B.1.1 Derived PIV Application Identifier 16
B.1.2 Derived PIV Application Data Model Elements 16
B.1.3 Derived PIV Application Data Objects Representation 18
B.1.4 Derived PIV Application Data Types and their Representation 18
B.1.5 Derived PIV Authentication Mechanisms 19
B.2 DERIVED PIV APPLICATION TOKEN COMMAND INTERFACE 20
B.2.1 Authentication of an Individual 21

Appendix C— Example Issuance Processes (Informative) **22**

C.1 EXAMPLE ISSUANCE OF DERIVED PIV CREDENTIALS AT LEVEL OF IDENTITY ASSURANCE 3 22
C.2 EXAMPLE ISSUANCE OF DERIVED PIV CREDENTIALS AT LEVEL OF IDENTITY ASSURANCE 4 22

Appendix D— Derived PIV Credentials in Relation to OMB Memoranda (Informative) **23**

Appendix E— Glossary (Informative) **24**

Appendix F— Acronyms and Abbreviations (Informative) **25**

Appendix G— References (Informative) **26**

List of Tables

Table B-1 Mapping of Data Objects 18
Table B-2 Mapping of Key Types 19
Table D-1 Token types and Relation to OMB's Electronic Authentication Guidelines 23

1. Introduction

FIPS 201 specifies a common set of identity credentials for the purpose 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 use of an additional common identity credential, a Derived PIV Credential, which is issued by a Federal department or agency and may be used with mobile devices where the use of a PIV Card is not practical. Consistent with the goals of HSPD-12, the Derived PIV Credential is designed to serve as a Federal government-wide standard for a secure and reliable identity credential that is interoperable across agencies.

1.1 Background

FIPS 201 originally required that all PIV credentials and associated keys be stored in a PIV Card. While the use of the PIV Card for electronic authentication works well with traditional desktop and laptop computers, it is not optimized for mobile devices. In response to the growing use of mobile devices within the Federal government, FIPS 201 was revised to permit the issuance of an additional credential, a Derived PIV Credential, for which the corresponding private key is stored in a cryptographic module with an alternative form factor to the PIV Card. Derived PIV Credentials leverage the current investment in the PIV infrastructure for electronic authentication and build upon the solid foundation of well-vetted and trusted identity of the PIV cardholder – achieving substantial cost savings by leveraging the identity-proofing results that were already performed to issue PIV cards. This document provides the technical guidelines for the implementation of Derived PIV Credentials.

The use of a Derived PIV Credential is one possible way to PIV-enable a mobile device. In other cases it may be practical to use the PIV Card itself with the mobile device, using either the PIV Card's contact or contactless interface, rather than issuing a Derived PIV Credential. Mobile devices are generally too small to integrate smart card readers into the device itself, requiring alternative approaches for communicating between the PIV Card and the mobile device. Some of these approaches are possible by today's set of available products. Other, newer technologies are addressed by new guidelines in the existing set of PIV Special Publications.

The current solution for PIV enablement directly uses PIV Cards with mobile devices through smart card readers. This has the advantage of avoiding the additional time and expense required to issue and manage Derived PIV Credentials. The approach requires smart card readers that are separate from, but attached to, the mobile device itself. These readers interface with the mobile device over a wired interface (e.g., USB) or wireless interface. The use of PIV Cards with mobile devices is functionally similar to their use with laptop and desktop computers. It does not involve new or different requirements to communicate with the PIV Card. Instead, the existing contact interface specifications of the PIV Card, as outlined in SP 800-73, form the basis for these types of readers to communicate with the PIV Card.

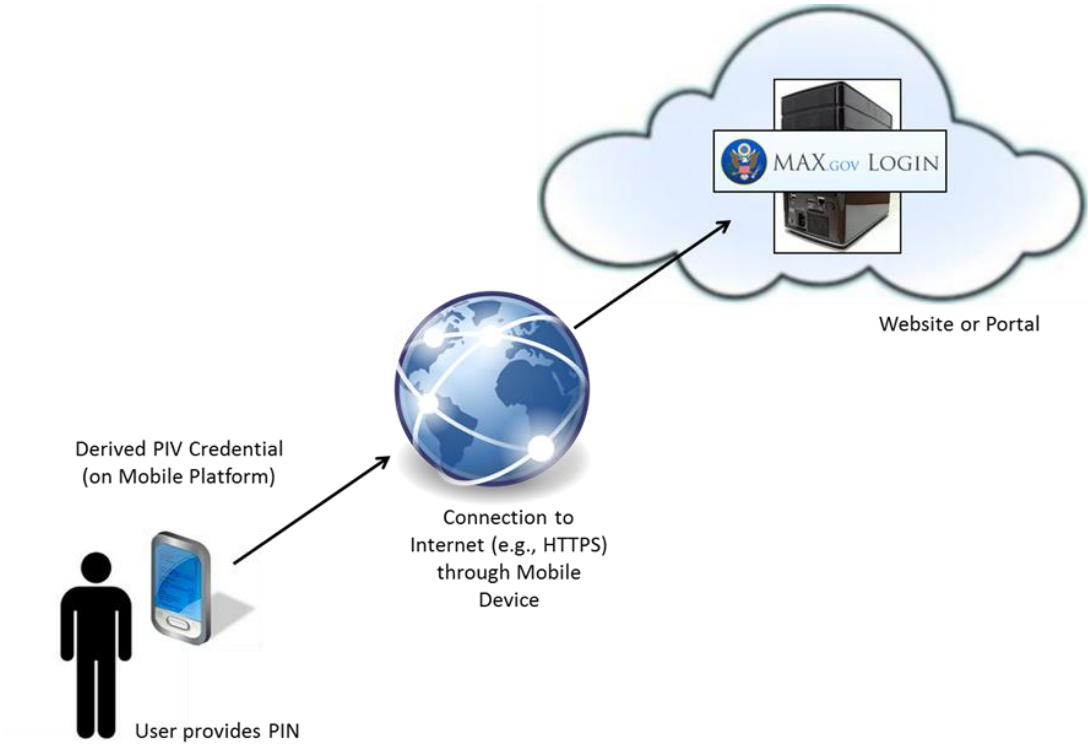
Newer technology on mobile devices can directly communicate with and use PIV Cards over a contactless interface using Near Field Communication (NFC). Similarly to the mobile devices and attached reader scenario, the use of NFC technology with PIV cards also avoids the additional time and expense required to issue and manage Derived PIV Credentials. NFC uses radio frequency to establish communication between NFC-enabled devices. An NFC-enabled mobile device can interact with a PIV Card over its contactless interface at a very close range, allowing the mobile device to use the keys on the PIV Card without a physical connection. The user would need to hold or place the card next to the mobile device. Earlier PIV specifications did not allow the use of certain keys over the contactless interface, as existing technologies and standards did not support a secure channel between the smart card and the mobile device over NFC. SP 800-73-4 will include a new capability to enable access to all non-card-management functionalities of the PIV Card over a secure wireless channel using the virtual contact interface.

1.2 Purpose and Scope

This document provides guidelines for cases in which the use of PIV Cards with mobile devices, using either contact card readers or NFC, is deemed impractical. This guideline specifies the use of tokens with alternative form factors to the PIV Card that may be inserted into mobile devices, such as Secure Digital (SD) cards, USB tokens, Universal Integrated Circuit Cards (UICC, the new generation of SIM cards), or that are embedded in the mobile device. The embedded tokens may be either hardware or software cryptographic modules. The use of tokens with alternative form factors greatly improves the usability of electronic authentication from mobile devices to remote IT resources, while at the same time maintaining the goals of HSPD-12 for common identification that is secure, reliable and interoperable government-wide.

The scope of the Derived PIV Credential is to provide PIV-enabled authentication services on the mobile device to authenticate the credential holder to remote systems as illustrated in Figure 1-1. This publication also includes an informative annex that provides recommendations for the inclusion of digital signature and key management keys on mobile devices.

To achieve interoperability with the PIV infrastructure and its applications, public key infrastructure (PKI) technology has been selected as the basis for the Derived PIV Credential. The PKI-based Derived PIV Credentials specified in this document are issued at levels of assurance (LOA) 3 and 4.[3]



[3] [M0404] provides a foundation for four levels of assurance (LOA) for electronic authentication. [SP800-63] provides guidance and technical requirements for electronic authentication solutions at each of the four levels of assurance.

Figure 1-1 Use of Derived PIV Credential

Derived PIV Credentials are based on the general concept of derived credential in [SP800-63], which leverages identity proofing and vetting results of current and valid credentials. When applied to PIV, identity proofing and vetting processes do not have to be repeated to issue a Derived PIV Credential. Instead, the user proves possession of a valid PIV Card to receive a Derived PIV Credential. The 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 the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* [COMMON]. 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 the scope of this document. Only derived credentials issued based on the PIV Card and in accordance with this document are considered to be Derived PIV credentials.

This document provides the technical guidelines on:

- The primary lifecycle activities for the Derived PIV Credential – initial issuance and maintenance – and the requirements for each activity to ensure security; and

- Technical requirements for the Derived PIV Credential including certificate policies, cryptographic specifications, types of cryptographic implementation that are permitted and mechanisms for activation and use of the credential.

The publication also includes an informative annex that provides recommendations for the inclusion of digital signature and key management keys on mobile devices.

1.3 Audience:

This document is targeted at stakeholders who will be responsible for procuring, designing, implementing, and managing deployments of Derived PIV Credentials for mobile devices.

1.4 Document Structure

The structure of the rest of this document is as follows. Each section is labeled as either normative (i.e., mandatory for compliance) or informative (i.e., non-mandatory).

- Section 2 describes Derived PIV Credential lifecycle activities and related requirements. This section is *normative,* with the exception of Section 2.1, which is *informative*.

- 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 the removable hardware implementations. This appendix is *normative* for implementation of Derived PIV Credentials on removable (non-embedded) hardware cryptographic tokens.

- Appendix C provides example issuance processes for Derived PIV Credentials. This appendix is *informative*.

- Appendix D summarizes the association of the Derived PIV Credentials' token types with the electronic authentication policies in OMB memoranda M-06-16 and M-07-16. This appendix is *informative*.

- Appendix E contains a glossary defining selected terms from this document. This appendix is *informative*.

- Appendix F defines acronyms and other abbreviations used in this document. This appendix is *informative*.

- Appendix G provides a list of references for this document. This appendix is *informative*.

1.5 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 is pending issuance of a Derived PIV Credential, and the term "Subscriber" refers to a PIV cardholder who has already been issued a Derived PIV Credential.

2. Lifecycle Activities and Related Requirements

The lifecycle activities (phases) for a Derived PIV Credential are initial issuance and maintenance. This section describes these lifecycle activities and provides requirements and recommendations as appropriate.

Issuers of Derived PIV Credentials must 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. The process, as outlined in [SP800-79], shall include an independent (third-party) assessment.

2.1 Derived PIV Credential Lifecycle Activities

The Derived PIV Credential lifecycle consists of five activities. The activities that take place at the manufacturer during fabrication and pre-personalization of the cryptographic token are not considered part of this lifecycle model. **Figure 2-1** presents these Derived PIV Credential activities alongside the PIV Card lifecycle activities.

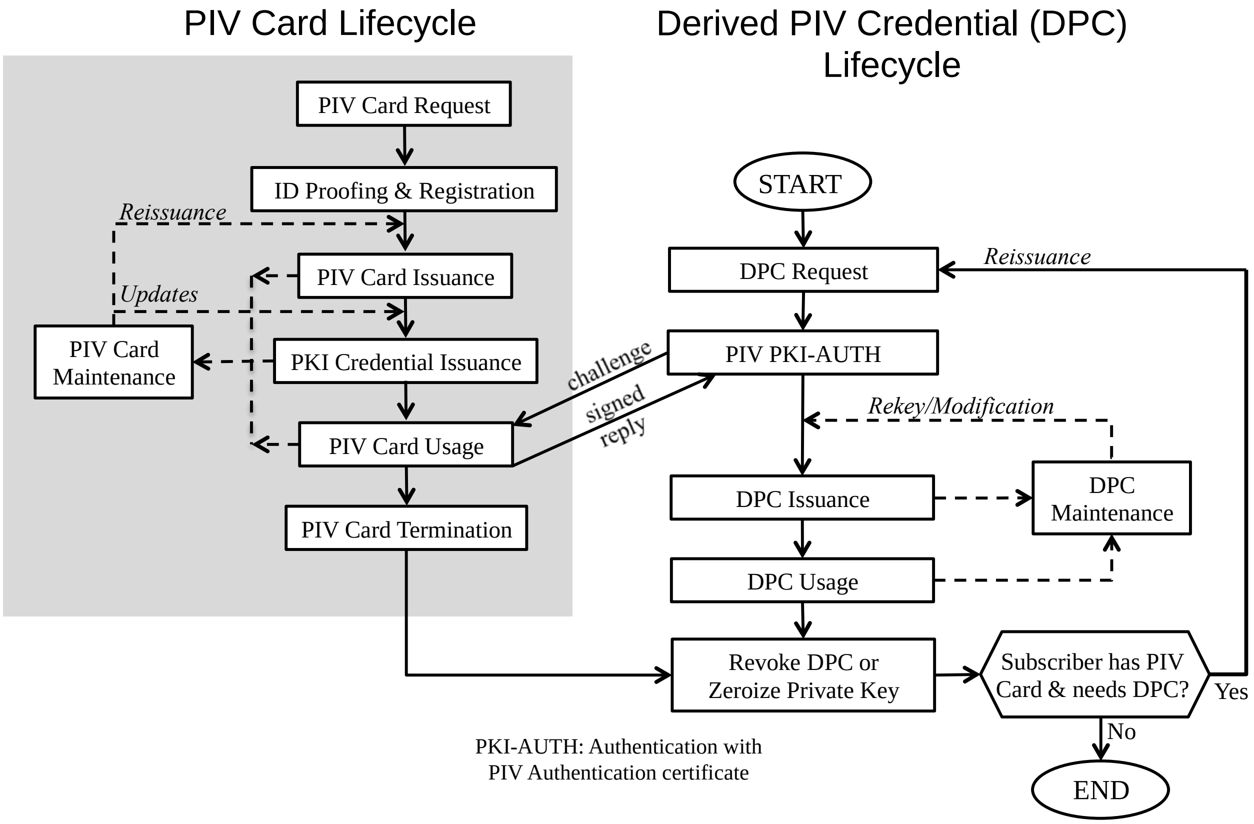


Figure 2-1 Derived PIV Credential Lifecycle Activities

The Derived PIV Credential lifecycle begins with a request for the issuance of a Derived PIV Credential to the Applicant and validation of the request. This request may be part of the process of provisioning a PIV cardholder with a government-issued mobile device or of approving the use of a personally-owned mobile device to access government information systems (see [SP800-96] Draft NIST Special Publication 800-96, *PIV Card to Reader Interoperability Guidelines*, NIST, September 2006, or as amended. Available at http://csrc.nist.gov.

[SP800-124]).

Once the request has been submitted the Applicant needs to authenticate to the Derived PIV Credential issuer using his/her PIV Card. The authentication is performed using the PKI-AUTH authentication mechanism from Section 6.2.3.1 of [FIPS201]. If the credential is being issued at LOA-3 this authentication may be performed remotely. At LOA-4, the authentication needs to be performed in person and has to be accompanied by a biometric authentication. In addition to authenticating the cardholder, performing the PKI-AUTH authentication mechanism verifies that the Applicant is currently eligible to possess PIV credentials. After the Applicant has been authenticated the Derived PIV Credential may be issued by the certification authority. The Derived PIV Credential may then be used for authentication to remote systems in the same way as the PIV Authentication certificate on the PIV Card is used.

The maintenance activities for a Derived PIV Credential are the same as for other X.509 public key certificate. Certificate re-key is typically used to replace a certificate that is nearing expiration. Certificate modification is used to replace a certificate if information about the Subscriber that appears in the certificate needs to be changed.

When the token containing the private key corresponding to the Derived PIV Credential is lost, stolen, damaged, or is being transferred to another individual, or when the Subscriber becomes ineligible to possess a PIV credential, the issuer needs to prevent further use of the Derived PIV Credential. If the private key corresponding to the Derived PIV Credential is created and stored on a hardware token that does not permit the key to be exported then this may be accomplished by zeroizing the private key or by destroying the token. In other cases, including when the token has been lost or stolen, the Derived PIV Credential (i.e., the Derived PIV Authentication certificate) needs to be revoked in order to ensure that it will no longer be accepted by relying parties. If the Derived PIV Credential was revoked (or the private key was zeroized) because the Subscriber is no longer eligible to possess a PIV Card or because the Subscriber no longer has a need for a Derived PIV Credential, then a new Derived PIV Credential cannot be issued. Otherwise, a new Derived PIV Credential may be issued by following the initial issuance process.

2.2 Initial Issuance

The initial issuance activity deals with the identification of an Applicant and the issuance of the Derived PIV Credential and other related data.

A Derived PIV Credential shall be issued following verification of the Applicant’s identity using the PIV Authentication key on his or her existing PIV Card. Verification is demonstrated by proving possession and control of the PIV Card through the PKI-AUTH authentication mechanism as per section 6.2.3.1 of [FIPS201]. The revocation status of the Applicant’s PIV Authentication certificate should be rechecked seven (7) calendar days following issuance of the Derived PIV Credential – this step can detect the use of a compromised PIV Card to obtain a Derived PIV Credential.

Derived PIV Credentials can be issued at identity assurance levels three or four (LOA-3 or LOA-4). The credential resides on a hardware or software security token as illustrated in Table D-1. Appendix C provides example issuance processes for Derived PIV Credentials.

An LOA-3 Derived PIV Credential may be issued remotely or in person in accordance with [SP800-63]. If the credential is issued remotely, all communications shall be authenticated and protected from modification (e.g., using Transport Layer Security (TLS)), and encryption shall be used, if necessary, to protect the confidentiality of any private or secret data. Moreover, if the issuance process involves two or more electronic transactions, the Applicant must identify himself/herself in each new encounter by presenting a temporary secret that was issued in a previous transaction, as described in Section 5.3.1 of [SP800-63].

An LOA-4 Derived PIV Credential shall be issued in person, in accordance with [SP800-63], and the Applicant shall identify himself/herself using a biometric sample that can be verified against the Applicant's PIV Card. If there are two or more transactions during the issuance process, the Applicant shall identify himself/herself using a biometric sample that can either be verified against the PIV Card or against a biometric that was recorded in a previous transaction. The issuer shall retain for future reference the biometric sample used to validate the Applicant.[4]

It may be noted that this guideline doesn't preclude the issuance of multiple Derived PIV Credentials to the same Applicant on the basis of the same PIV Card. Issuing several Derived PIV Credentials to an individual, however, could increase the risk that one of the tokens will be lost/stolen without the loss being reported, or that the Subscriber will inappropriately provide one of the tokens to someone else.

2.3 Maintenance

Derived PIV Credentials may require typical maintenance activities applicable to asymmetric cryptographic credentials – these maintenance activities include rekey, modification, and revocation. 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 re-key or modification is performed remotely for an LOA-4 Derived PIV Credential, the following shall apply:

- Communication between the issuer and the cryptographic module in which the Derived PIV Authentication private key is stored shall occur only over mutually authenticated secure sessions between tested and validated cryptographic modules.[5]
- Data transmitted between the issuer and the cryptographic module in which the Derived PIV Authentication private key is stored shall be encrypted and contain data integrity checks.

The initial issuance process (Section 2.2, above) shall be followed for:

1) re-key of an expired or compromised Derived PIV credential or

2) re-key of a Derived PIV Credential at LOA-4 to a new hardware token.

The Derived PIV Authentication certificate shall be revoked or the token containing the corresponding private key shall be either zeroized or destroyed when the binding between the Subscriber and the token containing the private key corresponding to the certificate is no longer considered valid or when the Subscriber no longer requires a Derived PIV Credential. Examples of circumstances that require one of these actions are–

- The token containing the private key corresponding to the Derived PIV Credential is lost, stolen, damaged or compromised.[6]

[4] The retained biometric shall be protected in a manner that protects the individual's privacy.

[5] In order to meet this requirement the issuer must be able to uniquely identify each hardware cryptographic module onto which Derived PIV Credentials are stored.

[6] Recovering from a mobile device computer security incident [SP800-61] may also require revoking the Derived PIV Authentication certificate.

- The token containing the private key corresponding to the Derived PIV Credential is transferred to another individual, including when a mobile device with an embedded cryptographic module is transferred to another individual.

- The department or agency that issued the credential determines that the Subscriber is no longer eligible to have a PIV Card (i.e., PIV Card is terminated[7]).

- The department or agency that issued the credential determines that the Subscriber no longer requires a Derived PIV Credential, even if the Subscriber's PIV Card is not being terminated. This may happen, for example, when the Subscriber's role in the agency changes such that he/she no longer has the need to access agency resources from a mobile device using a Derived PIV Credential.

If the Derived PIV Authentication private key was created and stored on a hardware cryptographic token that does not permit export of the private key and the token was collected and either zeroized or destroyed, then revocation of the Derived PIV Authentication certificate is optional. In all other cases, revocation of the Derived PIV Authentication certificate is mandatory.

The Derived PIV Credential is unaffected when the Subscriber replaces his/her PIV Card (reissuance) with a new PIV Card, including when the PIV Card is lost, stolen, or damaged.[8,9] The ability to use the Derived PIV Credential is especially useful in such circumstances because the PIV Card is unavailable, yet, while waiting to be issued a new PIV Card, the Subscriber is able to use the Derived PIV Credential to gain logical access to remote Federally controlled information systems from his/her mobile device. Similarly, the Derived PIV Credential is not necessarily affected by the revocation of the PIV Authentication certificate. 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 the Subscriber's name changing and the Subscriber's name appears in the Derived PIV Authentication certificate, a new Derived PIV Authentication certificate with the new name will also need to be issued.

2.4 Linkage with PIV Card

A Derived PIV Credential issuer shall only issue a Derived PIV Credential to an Applicant if it has access to information about the Applicant's PIV Card from the issuer of the PIV Card. In particular the Derived PIV Credential issuer shall have a mechanism to periodically check with the PIV Card issuer to determine if the PIV Card has been terminated or if information about the individual that will appear in the Derived PIV Credential (e.g., name) has changed, as these would require revocation or modification of the Derived PIV Credential.

Section 2.9.4 of FIPS 201-2 requires PIV Card termination to be performed within 18 hours for cases where the PIV card cannot be collected. To maintain up-to-date status of the PIV Card, it is recommended that a Derived PIV Credential issuer check every 18 hours on the termination status. The periodic checking requirement can also be met if: 1) a notification mechanism is in place between the PIV Card issuer and Derived PIV Credential issuer or 2) the PIV Card record and the Derived PIV Credential

[7] Section 2.9.4 of [FIPS201] provides a list of circumstances that require PIV Card termination.

[8] Departments and agencies may adopt a more stringent approach and revoke any Derived PIV Credential when the associated PIV Card is being replaced.

[9] In the case of a lost or stolen PIV Card there is the risk that the PIV Card could be used to obtain a fraudulently issued Derived PIV Credential. If the issuer of the PIV Card also issues Derived PIV Credentials then when a PIV Card is reported lost or stolen the issuer should investigate whether any fraudulent Derived PIV Credentials might have been issued.

record are stored in the same system and termination of the PIV Card automatically triggers termination of the Derived PIV Credential.

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 scenarios where the card's PIV Authentication certificate is not revoked even though the PIV Card has been terminated. This may happen, for example, when a terminated PIV Card is collected and either zeroized or destroyed by an agency – in this case, in accordance with [FIPS201], the corresponding PIV Authentication certificate does not need to be revoked.

Additional methods must be employed for obtaining information about the PIV Card from the PIV Card issuer. Some example mechanisms are listed below – however, any other mechanism that meets the above requirements is also acceptable.

- If the Derived PIV Credential is issued by the same agency or issuer that issued the Subscriber's PIV Card, then the Derived PIV Credential issuer may have direct access to the Identity Management System (IDMS) database implemented by the issuing agency that contains the relevant information about the Subscriber.

- When the issuer of the Derived PIV Credential is different from the PIV Card Issuer, the following mechanisms may be applied:

    - The Backend Attribute Exchange [BAE] can be queried for the termination status of the PIV Card, if an attribute providing this information is defined and the issuer of the PIV Card maintains this attribute for the Subscriber. The BAE can also be queried for other attributes about the Subscriber (e.g., name) that may appear in the Derived PIV Authentication certificate.

    - The issuer of the Derived PIV Credential notifies the original PIV issuer when a Derived PIV Credential is created. The issuer of the PIV Card maintains a list of corresponding Derived PIV Credential issuers and sends notification to the latter set when the PIV Card is terminated or when attributes about the cardholder change. Such notification should provide evidence of receipt and the integrity of the message.

    - If a Uniform Reliability and Revocation Service (URRS) is implemented in accordance with Section 3.7 of [NISTIR7817], the issuer of a Derived PIV Credential may obtain termination status of the Subscriber's PIV Card through the URRS.

3. Technical Requirements

This section describes technical requirements related to Derived PIV Credentials and their tokens.

3.1 Certificate Policies

Derived PIV Authentication certificates shall be issued under either the id-fpki-common-pivAuth-derived-hardware (LOA-4) or the id-fpki-common-pivAuth-derived (LOA-3) policy of the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* [COMMON]. A Derived PIV Credential shall be deemed to satisfy e-Authentication LOA-4 if it is issued in conformance with the id-fpki-common-pivAuth-derived-hardware certificate policy, and e-Authentication LOA-3 if it is issued in conformance with the id-fpki-common-pivAuth-derived certificate policy.

The Derived PIV Authentication certificate shall comply with *Worksheet 10: Derived PIV Authentication Certificate Profile* in [PROF].

The expiration date of the Derived PIV Authentication certificate is based on the certificate policy of the issuer. There is no requirement to align the expiration date of the 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.

3.2 Cryptographic Specifications

The cryptographic algorithm and key size requirements for the Derived PIV Authentication certificate and private key 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 (LOA-4), the Derived PIV Authentication key pair shall be generated within a hardware cryptographic module that has been validated to [FIPS140] Level 2 or higher that provides Level 3 physical security to protect the Derived PIV Authentication private key while in storage and that does not permit exportation of the private key.

For Derived PIV Authentication certificates issued under id-fpki-common-pivAuth-derived (LOA-3), the Derived PIV Authentication key pair shall be generated within a cryptographic module that has been validated to [FIPS140] Level 1 or higher.

3.3 Cryptographic Token Types

The Derived PIV Credentials and their corresponding private keys may be used in a variety of cryptographic tokens available for use on mobile devices. These tokens may be hardware or software-only implementations.

Hardware tokens may either be removable or embedded within a mobile device. Three kinds of removable hardware tokens are permitted, each with well-defined physical and logical interfaces, to facilitate token portability between mobile devices in a manner analogous to PIV Card interchangeability. Embedded hardware tokens are not removable from the mobile device, and may be accessed by software using the underlying cryptographic interface of the mobile device; however, nothing here is intended to either require or prohibit emulation of PIV Card or a removable token software interface. Similar rules apply to embedded software tokens; nothing here is intended to either require or prohibit the emulation of the software interfaces to PIV Cards or other removable tokens.

The cryptographic tokens permitted for Derived PIV Credentials are described in the subsections below.

3.3.1 Removable (Non-Embedded) Hardware Cryptographic Tokens

This section provides requirements for implementations where the Derived PIV Authentication private key resides in a hardware cryptographic module (or token) that can be removed from the mobile device. In such cases, a *Derived PIV Application*, as defined in Appendix B, shall be installed on the hardware cryptographic token. The use of this data model and its interface supports interoperability and ensures the Derived PIV Credential interface is aligned with the interface of the PIV Card.

The permitted types of removable hardware cryptographic tokens are described in the following subsections. Each token type is a standards-based hardware form-factor that supports compatibility and portability across a variety of mobile computing devices. In each case, the form-factor supports a secure element (SE), a tamper resistant cryptographic component that provides security and confidentiality.

The Application Protocol Data Units (APDUs) for the Derived PIV Application command interface (as defined in Appendix B) are transported to the secure element within each form-factor over a transport protocol appropriate for that form factor. Further details of the required transport protocols are provided below.

As described in Appendix B, the Derived PIV Application may include digital signature and key management private keys and their corresponding certificates in addition to the Derived PIV Authentication private key and its corresponding certificate.

3.3.1.1 SD Card with Cryptographic Module

A Secure Digital (SD) Card is a non-volatile memory card format for use in portable devices such as mobile phones and tablet computers. The SD format is available in three different physical sizes – "original," "mini," and "micro." While any size is permissible for Derived PIV Credential issuance, the microSD form factor is the most likely to be available for use within a mobile device.

A Derived PIV Application may reside on an SD Card implementation that includes an on-board secure element or security system. An example of a security system is an implementation of the smartSD standard, which describes a smart card element within an SD memory card.

The secure element used for the Derived PIV Application shall support an interface with the card commands specified in Appendix B of this document. It should be noted that there is no widely adopted interoperable standard transport mechanism for the APDUs, which may limit portability between devices.

3.3.1.2 Removable UICC with Cryptographic Module

The Universal Integrated Circuit Card (UICC) configuration is based on the GlobalPlatform Card Specification v2.2.1 [GP-SPEC]. The UICC configuration standardizes a minimum level of interoperability for mobile products that support remote application management. UICC represents a new generation Subscriber Identity Module (SIM) card.

The UICC includes storage and processing, as well as input/output capabilities. Unlike the SIM card, the UICC can also support a variety of other applications and services and multiple security domains.[10] [GP-

[10] A security domain is a protected area on a UICC. To this security domain are assigned applications, which can use cryptographic services it offers. By default only the security domain of the card issuer exists on a card. If another institution

A] defines a mechanism for an application provider to manage (i.e., load, install and personalize) its application in a confidential manner while using a third party communication network. The Derived PIV Application shall be installed in a security domain that is separate from other security domains, dedicated to the Derived PIV Credential, and under the explicit control of the issuing agency. The APDUs as specified in Appendix B shall be used with this secure element containing the PIV Derived Application.[11]

A UICC is a secure element, which may be capable of hosting a Derived PIV Application. A UICC used to host a Derived PIV Credential shall implement the GlobalPlatform Card Secure Element Configuration v1.0 [GP-SE].

3.3.1.3 USB Token with Cryptographic Module

A Universal Serial Bus (USB) token is a device that plugs into the USB port on various IT computing platforms, including mobile devices. USB tokens typically include onboard storage and may also include cryptographic processing capabilities (e.g., cryptographic mechanisms to verify the identity of users).

USB token implementations that contain an integrated secure element (an Integrated Circuit Card or ICC) are suitable for issuance of Derived PIV Credentials. Such implementations are called USB Integrated Circuit(s) Card Devices (ICCD) and shall comply with the Universal Serial Bus Device Class: Smart Card ICCD Specification for USB Integrated Circuit(s) Card Devices [ICCDSPEC].

The APDUs for the Derived PIV Application (as specified in Appendix B) shall be transported to the secure element using the Bulk-Out command pipe and the responses shall be received from the secure element using the Bulk-In command pipe.

USB tokens with cryptographic modules that support a Derived PIV Application shall also be compliant with the specifications in [SP800-96] for APDU support for contact card readers. The requirements for the Application Programming Interface (API) for Derived PIV Application implementations are beyond the scope of this document.

3.3.2 Embedded Cryptographic Tokens

A Derived PIV Credential and its associated private key may be used in cryptographic modules that are embedded within mobile devices (see Draft NIST Interagency Report 7981, *Mobile, PIV, and Authentication* [NISTIR7981]). These modules may either be in the form of a hardware cryptographic module that is a component of the mobile device or in the form of a software cryptographic module that runs on the device.

Protecting and using the Derived PIV Credential's corresponding private key in software may potentially increase the risk that the key could be stolen or compromised. For this reason, software-based Derived PIV Credentials cannot be issued at LOA-4.

Note: Many mobile devices on the market provide a hybrid approach where the key is stored in hardware, but a software cryptographic module uses the key during an authentication operation. While the hybrid approach is a LOA-3 solution, it does provide many security benefits over software-only approaches.

wants its own security domain, e.g., for having its own secure application environment or managing its own applications, such a domain can be created with the help of the card issuer. Institutions managing their own applications are also referred to as application providers. A controlling authority security domain, that is optionally present, offers a confidential personalization service to authenticated application providers.

[11] The requirements in this section only apply to removable UICCs. An embedded UICC may be used to host a Derived PIV Credential in accordance with the requirements in Section 3.3.2

Therefore the hybrid approach is recommended when supported by mobile devices and applications.

The cryptographic module shall satisfy the requirements in Section 3.2 for either certificates issued under id-fpki-common-pivAuth-derived-hardware or id-fpki-common-pivAuth-derived. As described in Appendix A, these same cryptographic modules may also hold other keys, such as digital signature and key management private keys and their corresponding certificates.

3.4 Activation Data

Use of the Derived PIV Authentication private key, or access to the plaintext or wrapped private key, shall be blocked prior to password-based Subscriber authentication.[12] The password should not be easily guessable or otherwise individually identifiable in nature (e.g., part of a Social Security Number, phone number). The required password length shall be a minimum of six characters.[13]

There shall be a mechanism to block use of the Derived PIV Authentication private key after a number of consecutive failed activation attempts as stipulated by the department or agency. Throttling mechanisms may be used to limit the number of attempts that may be performed over a given period of time.

For embedded tokens at LOA-3, the authentication mechanism may be implemented by hardware or software mechanisms outside the boundary of the cryptographic module, provided that the strength of the authentication mechanism meets the requirements in this section. For removable tokens, or embedded tokens at LOA-4, the authentication mechanism shall be implemented and enforced by the cryptographic module itself.

The password may need to be reset if the Subscriber has forgotten the password or if password-lockout has occurred following repeated use of invalid passwords.[14] Password reset may be performed at the issuer’s facility, at an unattended kiosk operated by the issuer, or remotely via a general computing platform.

- When password reset is performed in-person at the issuer's facility, or at an unattended kiosk operated by the issuer, it shall be implemented through one of the following processes:
    - The Subscriber’s PIV Card shall be used to authenticate the Subscriber (via PKI-AUTH mechanism as per Section 6.2.3.1 of [FIPS201]) prior to password reset. The issuer shall verify that the Derived PIV Credential is for the same Subscriber that authenticated using the PIV Card.
    - A 1:1 biometric match shall be performed against the biometric sample retained during initial issuance of the Derived PIV Credential, a stored biometric on the PIV Card, or biometric data stored in the chain-of-trust [FIPS201]. The issuer shall verify that the Derived PIV Credential is for the same Subscriber for whom the biometric match was completed.
- For remote password reset the Subscriber’s PIV Card shall be used to authenticate the Subscriber (via PKI-AUTH authentication mechanism as per Section 6.2.3.1 of [FIPS201]) prior to password reset. If the reset occurs over a session that is separate from the session over which the PKI-AUTH

[12] For embedded cryptographic tokens individual implementations may limit the set of characters from which the password may be chosen (e.g., to only decimal digits). Appendix B.2.1 requires that removable cryptographic tokens allow the use of decimal digits, lower case characters, and upper case characters.

[13] Departments and agencies may choose to impose stronger password requirements for embedded cryptographic tokens.

[14] Subscribers may change their passwords anytime by providing the current password and the new password values.

authentication mechanism was completed, strong linkage (e.g., using a temporary secret) must be established between the two sessions. The issuer shall verify that the Derived PIV Credential is for the same Subscriber that authenticated using the PIV Card. The remote password reset shall be completed over a protected session (e.g., using TLS).

Removable hardware tokens shall support the password reset functionality as per Appendix B. At LOA-3 support for password reset is not required, and implementations may instead choose to issue a new certificate following the initial issuance process if the password is forgotten.

Appendix A—Digital Signature and Key Management Keys (Informative)

In addition to the PIV Authentication key, [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 Authentication certificate for use with a mobile device may also have a need to use a digital signature and key management key with that mobile device.

For most Subscribers, it will be necessary for the key management private key and certificate on the mobile device to be the same key as the one on the PIV Card. Similarly it will be necessary for copies of all of the retired key management private keys and certificates on the PIV Card to be on the mobile device as well. 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 smart phone) as long as all of the requirements of the policy under which the key management certificate was issued are satisfied. Note that this means that in order to be able 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 issued to mobile devices.

As the digital signature key on a PIV Card cannot be copied, a mobile device will have to be issued a new digital signature private key and certificate. The issuance of this private key and certificate is completely independent of the issuance of the PIV Card, although the issuer may choose to leverage the Applicant's PIV Card to identity proof the Applicant prior to issuing the digital signature certificate. 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 mobile device may be issued under one of these policies, as long as all of the requirements of the policy are satisfied.

Appendix B—Data Model and Interfaces for Removable (Non-Embedded) Hardware Cryptographic Tokens (Normative)

This appendix provides data model and interface requirements for the Derived PIV Applications implemented on removable 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 [SP800-73Part1] . The specifications for the mandatory and optional data objects listed below are the same as the specifications of the corresponding data objects on a PIV Card Application as described in [SP800-73Part1] , except for the general difference that the contactless interface is not supported by the Derived PIV Application.

B.1.1 Derived PIV Application Identifier

The Application Identifier (AID) of the Derived PIV Application shall be:

```
'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:

```
'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 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 Section 3.1.3 of [SP800-73Part1] .

The optional data objects are as follows:

- **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 Section 3.2.1 of [SP800-73Part1] .

- **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 Section 3.2.2 of [SP800-73Part1] .

- **Discovery Object—**The requirements for the Discovery Object are as described in Section 3.3.2 of [SP800-73Part1] 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 Application

Password."

  - The first byte of the PIN Usage Policy shall be set to 0x40. (This means that neither the Global PIN nor On-Card Biometric Comparison (OCC) satisfy 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 Section 3.3.3 of [SP800-73Part1] 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 corresponding 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 PKI cryptographic function access rules for corresponding private keys are as described in Section 3.3.4 of [SP800-73Part1] .

- **Security Object—**The Security Object shall be present in the Derived PIV Application if either the Discovery Object or the Key History object is present, and shall be absent otherwise. The requirements for the Security Object are as described in Section 3.1.7 of [SP800-73Part1] , 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 Section 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 and the Key History object) within the Derived PIV Application shall be included in the Security Object.

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

Section 3.5 of [SP800-73Part1] provides the container IDs and Access Rules for the mandatory and optional data objects for a Derived PIV Application with the following mappings:

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 *n*	Retired X.509 Certificate for Key Management *n*

Table B-1 Mapping of Data Objects

The detailed data model specifications for each of the data objects of the Derived PIV Application are the same as the specifications of the corresponding data objects (mapped per the table above) of the PIV Card Application as described in Appendix A of [SP800-73Part1] , except for the following:

- References to contactless interface are not applicable. The Derived PIV Application only supports a contact interface.
- The Security Object for the Derived PIV Application is optional. It is required if either the optional Discovery Object or the optional Key History object 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 various mandatory and optional data objects within the Derived PIV Application are the same as for the corresponding data objects (mapped per the table above) of the PIV Card Application as described in Section 4 of [SP800-73Part1] .

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 passwords of the Derived PIV Application. Table 6-1 of [SP800-78] and Table 4 of [SP800-73Part1] define the key reference values that shall be used on the Derived PIV Application interfaces with the following mappings:

Derived PIV Key Type	PIV Key Type
Derived PIV Application Password	PIV Card Application PIN
Password Unblocking Key	PIN Unblocking Key

Derived PIV Key Type	PIV Key Type
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

Table B-2 Mapping of Key Types

The key reference specifications in Section 5.1 of [SP800-73Part1] are applicable to the corresponding keys included in the Derived PIV Application (mapped per the table above) except for the following:

- References to "PIV Card Application" are replaced by "Derived PIV Application"
- References in the "Security Conditions for Use" column to "PIN or OCC" are replaced by "Derived PIV Application Password"

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 asymmetric and symmetric 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 [SP800-73Part1] .

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 Section 5.6 of [SP800-73Part1] .

B.1.5 Derived PIV Authentication Mechanisms

The Derived PIV Application supports the following validation steps:

- Credential Validation (CredV) through verification of the certificates retrieved from the Derived PIV Application and checking of the revocation status of these certificates.
- Derived PIV Application Holder Validation (HolderV) through matching the password provided by the token holder with the password within the Derived PIV Application.

The Derived PIV Application facilitates a single authentication mechanism, which is a cryptographic challenge and response authentication protocol using the Derived PIV Authentication private key as described in Appendix B.1.2 of [SP800-73Part1] with the following translations:

- References to "PIV Application" are replaced by "Derived PIV Application."
- References to "PIV Auth Certificate" are replaced by "Derived PIV Authentication Certificate."
- References to "PIV Card App ID" are replaced with "Derived PIV Application ID."

B.2 Derived PIV Application Token Command Interface

This appendix contains the technical specifications of 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 [SP800-73Part2] , 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 [SP800-73Part2] , except for the following deviations:

- References to “PIV Card Application” are replaced by “Derived PIV Application”
- References to the contactless interface are ignored
- References to “PIV Data Objects” are replaced by “Derived PIV Data Objects”
- References to “PIV Authentication Key” are replaced with “Derived PIV Authentication Key”
- The Derived PIV Application Password shall satisfy the criteria specified in Appendix B.2.1 of this document rather than Section 2.4.3 of [SP800-73Part2] .
- In Appendix A:
  - References to “PIV Card Application Administrator” are replaced by “Derived PIV Application Administrator”
  - References to “Card Management Key” are replaced by “Derived PIV Token Management Key”

The token platform shall support a default selected application. In other words, there shall be a currently selected application immediately after a cold or warm reset. This application is the default selected application. The default application may be the Derived PIV Application, or it may be another application.

B.2.1 Authentication of an Individual

Knowledge of a password is the means by which an individual can be authenticated to the Derived PIV Application.

The Derived PIV Application Password shall be between 6 and 8 bytes in length. If the actual length of Derived PIV Application Password is less than 8 bytes it shall be padded to 8 bytes with 'FF' when presented to the token command interface. The 'FF' padding bytes shall be appended to the actual value of the password. The bytes comprising the Derived PIV Application Password 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 Application Password: “Pass12” or '50 61 73 73 31 32'
+ Padded Derived PIV Application Password presented to the card command interface: '50 61 73 73 31 32 FF FF'

The Derived PIV Application shall enforce the minimum length requirement of six bytes for the Derived PIV Application Password (i.e., shall verify that at least the first six bytes of the value presented to the card command interface are in the range [0x30 – 0x39, 0x41 – 0x5A, 0x61 – 0x7A]) as well as the other formatting requirements specified in this section.

Appendix C—Example Issuance Processes (Informative)

The issuance process for a Derived PIV Credential varies depending whether the Derived PIV Credential is issued at LOA-3 or LOA-4. Section 2.2 specifies the requirements for initial issuance. This appendix provides two example issuance processes that satisfy those requirements, one at LOA-3 and another at LOA-4.

C.1 Example Issuance of Derived PIV Credentials at Level of Identity Assurance 3

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.

Once the employee has received the device and the request has been approved the employee starts the issuance process by visiting a Web site operated by a registration authority (RA) that is associated with the certification authority (CA) that will issue the Derived PIV Credential. The Web site requires TLS client authentication using the PIV Authentication certificate on the employee's PIV Card. Since the employee cannot use the PIV Card with the mobile device the employee performs this step from a desktop computer. By requiring the use of the PIV Authentication certificate when connecting to the Web site and by validating the certificate, the server not only authenticates the employee, but also verifies that the employee is still eligible to possess a PIV credential. If the employee successfully authenticates to the server then the RA issues the employee a one-time password (OTP).

The employee then runs a provisioning application on the mobile device. The application asks the employee to enter the OTP that was previously provided and to create a password, 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 OTP and newly generated public key to the RA as part of a certificate request. The RA authenticates the employee by verifying that the OTP in the certificate request matches the one that it previously issued, signs the certificate request, and forwards it to the CA, which 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.

C.2 Example Issuance of Derived PIV Credentials at Level of Identity Assurance 4

An employee requests a mobile device and Derived PIV Credential for work. The request is approved by the agency's approval authority.

The IT department sets up an appointment for Derived PIV Credential issuance and device pickup. At the appointment, the IT staff directs the employee to an issuance station where the employee is asked to insert the PIV Card into the issuance workstation and provide the password and a fingerprint. The issuance station performs the PKI-AUTH and BIO authentication mechanisms from Section 6.2 of [FIPS201].

An IT staff member assigns a USB token to the employee and inserts it into the USB port of the issuance station. The issuance station generates the Derived PIV Credential's key pair on the USB token, creates a certificate request that includes the newly generated public key, and forwards the request to the CA, which issues the Derived PIV Credential (i.e., the Derived PIV Authentication certificate). The employee is asked to set the password to activate the cryptographic module on the USB token. As a last step, the issuance station loads the Derived PIV Authentication certificate on the USB token.

Appendix D—Derived PIV Credentials in Relation to OMB Memoranda (Informative)

This document provides a spectrum of choices for two-factor remote authentication with a mobile device, all of which are subject to OMB guidance on remote electronic authentication.

Table D-1 summarizes the association of Derived PIV Credentials' token types with the existing remote electronic authentication policies in OMB memoranda M-06-16 [M0616] and M-07-16 [M0716]. Both memoranda specify a "Control Remote Access" provision that calls for two-factor authentication where one of the two factors is provided by a device that is separate from the device accessing the remote resource.

Increasingly, mobile devices are becoming thinner and/or lighter. These constraints limit external ports and force the integration of authentication tokens and security features. As indicated by column 6 in Table D-1,[15] four of the five tokens with Derived PIV Credentials are integrated. For these tokens, guidance will be made available by OMB to provide an alternative to the remote authentication policy in M-06-16 and M-07-16. With integrated tokens, authentication factors are not provided by a separate token and sensitive government information may be at greater risk of loss. OMB's alternative guidance intends to also address these risks by pointing to NIST guidelines for compensating controls (e.g., SP 800-53, SP 800-124, SP 800-164).

Note: To provide a complete set of options for PIV-enabled remote access with mobile devices, the PIV Card as token type has been included.

Credential Type	Token Type	PIV Assurance Level	Comparable OMB E-Authentication Level	Target Guidance:	
				M-06-16/M-07-16 for Separate Tokens	Alternate OMB Guidance for Integrated Tokens
Derived PIV Authentication certificate	MicroSD Token	Very High	4		✓
	USB Security Token	Very High	4	✓	
	Software Token	High	3		✓
	Embedded Hardware Token	Very High	4		✓
	UICC Token	Very High	4		✓
PIV Card's PIV Authentication certificate credential	PIV Card (via attached reader or NFC)	Very High	4	✓	

Table D-1 Token types and Relation to OMB's Electronic Authentication Guidelines

[15] Draft NIST Interagency Report 7981 [NISTIR7981] summarizes the unique set of constraints for mobile devices that necessitate alternative OMB guidance for e-authentication for mobile devices.

Appendix E—Glossary (Informative)

Selected terms used in the guide are defined below.

Applicant: An individual who has applied for, but has not yet been issued, a Derived PIV Credential.

Application Protocol Data Unit: A part of the application layer in the Open Systems Interconnection Reference model that is used for communication between two separate device's applications. In the context of smart cards, an APDU is the communication unit between a smart card reader and a smart card. The structure of the APDU is defined by [ISO7816-4].

Derived PIV Application: A standardized application residing on a removable, hardware cryptographic token that hosts a Derived PIV Credential and associated mandatory and optional elements.

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 and that is used with mobile devices.

Mobile Device: A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.

Subscriber: The individual who is the subject named or identified in a Derived PIV Authentication certificate and who holds the token that contains the private key that corresponds to the public key in the certificate.

All other significant technical terms used within this document are defined in other key documents including [FIPS201], [SP800-63] and [SP800-73] Revised Draft NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, NIST, May 2014, or as amended. Available at http://csrc.nist.gov.

[SP800-73Part1] Revised Draft NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, Part 1- *PIV Card Application Namespace, Data Model and Representation*, NIST, May 2014, or as amended. Available at http://csrc.nist.gov.

[SP800-73Part2] Revised Draft NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification***,** Part 2- *PIV Card Application Card Command Interface*, May 2014 or as amended. Available at http://csrc.nist.gov.

.

Appendix F—Acronyms and Abbreviations (Informative)

Selected acronyms and abbreviations used in the guide are defined below.

AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
CA	Certification Authority
FIPS	Federal Information Processing Standard
HSPD	Homeland Security Presidential Directive
ICC	Integrated Circuit Card
ICCD	Integrated Circuit(s) Card Device
IDMS	Identity Management System
IT	Information Technology
ITL	Information Technology Laboratory
LOA	Level of Assurance
NFC	Near Field Communication
NIST IR	National Institute of Standards and Technology Interagency or Internal Reports
NIST	National Institute of Standards and Technology
OID	Object Identifier
OMB	Office of Management and Budget
OTP	One-time password
PCI	PIV Card Issuer
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
P.L.	Public Law
RA	Registration Authority
SD	Secure Digital
SE	Secure Element
SIM	Subscriber Identity Module
SP	Special Publication
TLS	Transport Layer Security
TLV	Tag-Length-Value
UICC	Universal Integrated Circuit Card
URL	Uniform Resource Locator
USB	Universal Serial Bus

Appendix G—References (Informative)

This appendix provides references for the document.

[BAE] *Backend Attribute Exchange (BAE) v2.0 Overview*, January 2012. Available at http://idmanagement.gov/sites/default/files/documents/BAE_v2_Overview_Document_Final_v1.0.0.pdf.

[COMMON] *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Version 1.21, December 2012. Available at http://www.idmanagement.gov/documents/common-policy-framework-certificate-policy. [Note: A change proposal that would add the id-fpki-common-pivAuth-derived and id-fpki-common-pivAuth-derived-hardware policies to this certificate policy has been submitted to the Federal PKI Policy Authority.]

[FIPS140] FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001, or as amended. Available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[FIPS201] FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, NIST, August 2013, or as amended. Available at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf.

[GP-A] *Confidential Card Content Management – GlobalPlatform Card Specification v2.2 - Amendment A v1.0.1*, January 2011. Available at http://www.globalplatform.org/specificationscard.asp.

[GP-SPEC] *GlobalPlatform Card Specification Version 2.2.1*, January 2011. Available at http://www.globalplatform.org/specificationscard.asp.

[GP-SE] *GlobalPlatform Card Secure Element Configuration v1.0*, October 2012. Available at http://www.globalplatform.org/specificationscard.asp.

[HSPD-12] Homeland Security Presidential Directive-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

[ICCDSPEC] *Universal Serial Bus Device Class: Smart Card ICCD Specification for USB Integrated Circuit(s) Card Devices*, Revision 1.0, April 2005. Available at http://www.usb.org/developers/devclass_docs/DWG_Smart-Card_USB-ICC_ICCD_rev10.pdf.

[ISO7816-4] ISO/IEC 7816-4, *Identification cards — Integrated circuit cards – Part 4: Organzation, security and commands for interchange.*

[M0404] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, OMB, December 2003.

[M0616] OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, OMB, December 2006.

[M0716] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, OMB, May 2007.

[NISTIR7817] NIST Interagency Report 7817, *A Credential Reliability and Revocation Model for Federated Identities*, November 2012. Available at http://csrc.nist.gov.

[NISTIR7981] Draft NIST Interagency Report 7981, *Mobile, PIV, and Authentication*, March 2014. Available at http://csrc.nist.gov.

[PROF] *X.509 Certificate and Certificate Revocation List (CRL) Profile for the Shared Service Providers (SSP) Program*, Version 1.5, January 2008, or as amended. Available at http://csrc.nist.gov. [Note: A change proposal that would add Worksheet 10 has been submitted to the Federal PKI Policy Authority.]

[SP800-53] NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST, April 2013, or as amended. Available at http://csrc.nist.gov.

[SP800-61] NIST Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012, or as amended. Available at http://csrc.nist.gov.

[SP800-63] NIST Special Publication 800-63-2, *Electronic Authentication Guideline*, NIST, August 2013, or as amended. Available at http://csrc.nist.gov.

[SP800-73] Revised Draft NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, NIST, May 2014, or as amended. Available at http://csrc.nist.gov.

[SP800-73Part1] Revised Draft NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, Part 1- *PIV Card Application Namespace, Data Model and Representation*, NIST, May 2014, or as amended. Available at http://csrc.nist.gov.

[SP800-73Part2] Revised Draft NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, Part 2- *PIV Card Application Card Command Interface*, May 2014 or as amended. Available at http://csrc.nist.gov.

[SP800-78] Revised Draft NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, May 2014, or as amended. Available at http://csrc.nist.gov.

[SP800-79] Draft NIST Special Publication 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers and Derived PIV Credential Issuers*, NIST, June 2014, or as amended. Available at http://csrc.nist.gov.

[SP800-96] Draft NIST Special Publication 800-96, *PIV Card to Reader Interoperability Guidelines*, NIST, September 2006, or as amended. Available at http://csrc.nist.gov.

[SP800-124] NIST Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST, June 2013, or as amended. Available at http://csrc.nist.gov.

[SP800-164] Draft NIST Special Publication 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices*, NIST, October 2012, or as amended. Available at http://csrc.nist.gov.