The attached DRAFT document (provided here for historical purposes) has been superseded by the following publication:

Publication Number: **NIST Special Publication (SP) 800-157**

Title: **Guidelines for Derived Personal Identity Verification (PIV) Credentials**

Publication Date: **October 2015**

- Final Publication: http://dx.doi.org/10.6028/NIST.SP.800-157 (which links to http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf).
- Related Information on CSRC: http://csrc.nist.gov/groups/SNS/piv/
- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/

The following information was posted with the attached DRAFT document:

Mar 7, 2014

SP 800-157

DRAFT Guidelines for Derived Personal Identity Verification (PIV) Credentials

NIST announces that Draft Special Publication (SP) 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, is now available for public comments. Draft SP 800-157 defines a technical specification for implementing and deploying Derived PIV Credentials to mobile devices, such as smart phones and tablets. The goal of the Derived PIV Credential is to provide PIV-enabled authentication services from mobile devices to authenticate to remote systems.

The public comment period closes on **April 21, 2014**.

There is a comment template provided for submitting comments for this draft SP - see link below. Comments on this publication may be submitted to piv_comments @nist.gov.

Draft 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

I N F O R M A T I O N S E C U R I T Y

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

Draft 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, NIST

William Burr
Dakota Consulting, Inc.

Jason Mohler
Sarbari Gupta
Electrosoft Services, Inc.

March 2014

U.S. Department of Commerce
Penny Pritzker, *Secretary*

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and 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 (Draft)
Natl. Inst. Stand. Technol. Spec. Publ. 800-157, 29 pages (March 2014)
CODEN: NSPUE2

Public comment period: March 7, 2014 through April 21, 2014

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_comments@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 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, maintenance and termination 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, William Burr, David Cooper, Hildegard Ferraiolo, Salvatore Francomacaro and Andrew Regenscheid of the National Institute of Standards and Technology (NIST), and Sarbari Gupta and Jason Mohler of Electrosoft, 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

Table of Contents

List of Tables

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 for 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 department and agencies, the use of PIV Cards and separate card readers is a practical solution for authentication from mobile devices. Other department 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.

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 on 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 credential 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.

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, 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 type of readers to communicate with the PIV Card.

Newer technology could take advantage of mobile devices that can directly communicate with and use PIV Cards over a wireless interface using Near Field Communication (NFC). Similarly to the mobile devices and attached reader scenario, the use of NFC technology 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 antenna 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 (VCI).

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 impracticable. This guideline specifies the use of tokens with alternative form factors to the PIV Card that may be inserted into mobile devices, such as microSD tokens, 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.

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]

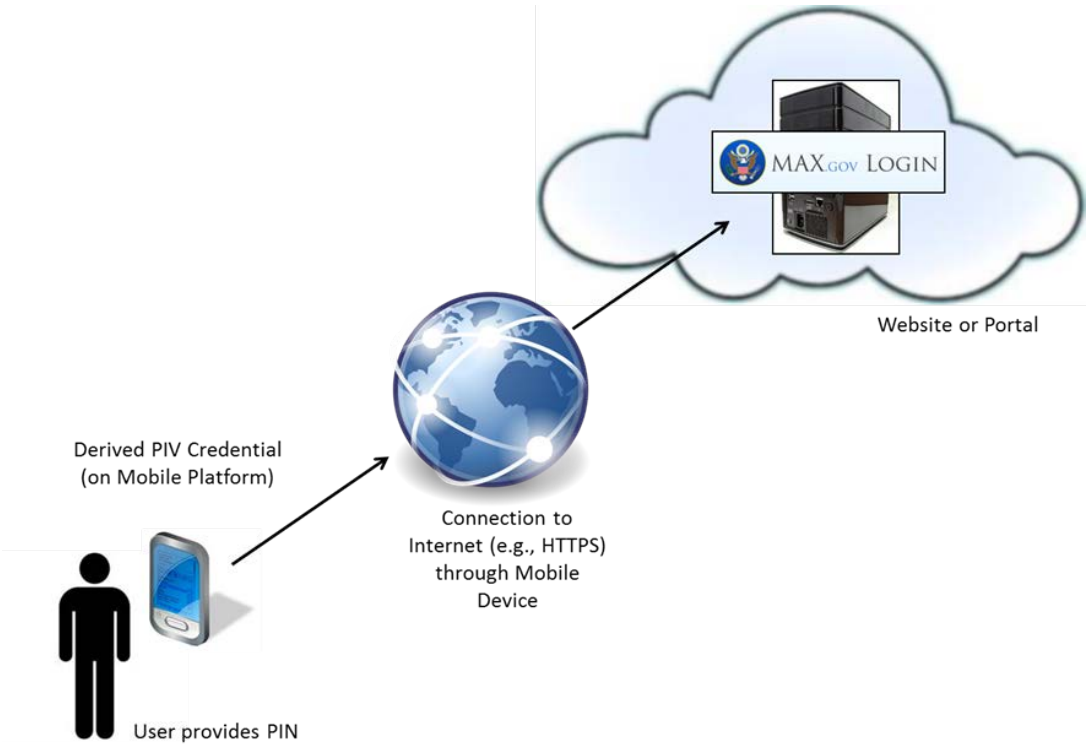

Figure 1-1 Use of Derived PIV Credential

[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.

Derived PIV Credentials are based on the general concept of derived credential in SP 800-63, 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 PIV Derived 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 in accordance with this document are considered to be Derived PIV credentials.

The document provides the technical guidelines on:

- Three primary lifecycle activities for the Derived PIV Credential – initial issuance, maintenance and termination – 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 software developers and others 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:

- 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 the removable hardware implementations. This appendix is *normative* for implementation of Derived PIV on removable (non-embedded) hardware cryptographic tokens.
- Appendix C 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 D contains a glossary defining selected terms from 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 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, maintenance, and termination. 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 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. The PIV Authentication certificate shall be validated as being active and not revoked prior to issuance of a Derived PIV Credential, and the Applicant must demonstrate possession and control of the related PIV Card via the PKI-AUTH authentication mechanism as per section 6.2.3.1 of [FIPS 201]. The revocation status of the Applicant's PIV Authentication certificate shall be rechecked seven (7) calendar days following issuance of the Derived PIV Credential – this step protects against 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 C-1.

An LOA-3 Derived PIV Credential may be issued remotely or in person in accordance with [SP800-63]. If the credential is issued over an electronic session, all communications shall be authenticated and protected from modification (e.g., using 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.

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.

2.2 Maintenance

Derived PIV Credentials may require typical maintenance activities applicable to asymmetric cryptographic credentials – these include rekey, modification, and revocation. These operations may be performed either remotely or in-person and shall be performed in accordance with the certificate policy

under which the PIV Derived 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 PIV Derived Authentication private key is stored shall occur only over mutually authenticated secure sessions between tested and validated cryptographic modules.

+ Data transmitted between the issuer and the cryptographic module in which the PIV Derived Authentication private key is stored shall be encrypted and contain data integrity checks.

The initial issuance process 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.

If the token corresponding to the Derived PIV Credential is lost, stolen, damaged or compromised, the PIV Derived Authentication certificate shall be revoked in accordance with the underlying certificate policy. [4]

The Derived PIV Credential is unaffected by loss, theft or damage to the Subscriber's PIV Card.[5] The ability to use the Derived PIV Credential is especially useful in such circumstances because the PIV Card is unavailable, yet 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 unaffected 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. For example, if the subscriber's PIV Card is reissued as a result of the Subscriber's name change, a new PIV Derived Authentication certificate with the new name may also need to be issued.

2.3 Termination

A Derived PIV Credential shall be terminated when 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[6]). A Derived PIV Credential may also be terminated when the department or agency that issued the credential determines that the Subscriber no longer requires a derived credential, even if the Subscriber's PIV Card is not being terminated. The latter 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 PIV Derived Authentication private key was created and stored on a hardware cryptographic token that does not permit the user to export the private key, then termination of the Derived PIV Credential may be performed by either: 1) collecting and either zeroizing the private key or destroying the token or 2) revoking the PIV Derived Authentication certificate. In all other cases, termination shall be performed by revoking the PIV Derived Authentication certificate.

[4] Recovering from a mobile device computer security incident [SP 800-61] may also require revoking the PIV Derived Authentication certificate.

[5] 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.

[6] [FIPS201] provides a list of circumstances that require PIV Card termination.

2.4 Linkage with PIV Card

The issuer of the Derived PIV Credential shall implement a process that maintains a link between the Subscriber's PIV Card and the Derived PIV Credential to enable the issuer of the latter credential to track the status of the PIV Card in order to perform timely maintenance and termination activities in response to changes in the status of the PIV Card.

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 maintaining a linkage between the current PIV Card and the corresponding Derived PIV Credential. Some example mechanisms to maintain this linkage 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 that issued the Subscriber's PIV Card, the linkage between the two credentials may be maintained through the common Identity Management System (IDMS) database implemented by the issuing agency.

- 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 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.

    - 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.

The linkage between the Derived PIV Credential and the Subscriber's PIV Card shall be updated when the Subscriber obtains a new PIV Card (e.g., the Subscriber obtains a replacement PIV Card after compromise of the original PIV Card).

3. Technical Requirements

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

3.1 Certificate Policies

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

The expiration date of the PIV Derived Authentication certificate is based on the certificate policy of the issuer and need not be related to the expiration date of the PIV Authentication certificate or the expiration of the PIV Card.

3.2 Cryptographic Specifications

The cryptographic algorithm and key size requirements for the PIV Derived 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 PIV Derived Authentication certificates issued under id-fpki-common-pivAuth-derived-hardware, the PIV Derived 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 PIV Derived Authentication private key while in storage and that does not permit exportation of the private key.

For PIV Derived Authentication certificates issued under id-fpki-common-pivAuth-derived, the PIV Derived 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 specified, 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 native cryptographic interface of the mobile device; however, nothing here is intended to either require or prohibit emulation of PIV Card or the 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.

Although software tokens are considered embedded tokens for this reason, as a practical matter it will often be impossible to prevent users from making copies of software tokens or porting them to other devices.

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 PIV Derived Authentication private key resides in a hardware cryptographic module (or token) that can be removed from the mobile device. In such cases, a *PIV Derived Application*, as defined in Appendix B, shall be implemented on the hardware cryptographic token. When the removable hardware cryptographic module supports multiple security domains[7] managed by independent issuers, the PIV Derived Application shall be implemented 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 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 PIV Derived Application command interface (as defined in Appendix B) are transported to the secure element within each form-factor over a standardized transport protocol appropriate for that form factor. Further details of the required transport protocols are provided below.

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

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 sizes – the original size, the "mini" size, and the "micro" size. While any size is permissible for Derived PIV Credential issuance, the microSD form factor is more likely to be available for use within a mobile device.

A PIV Derived Application may reside on SD Card implementations that include 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 PIV Derived Application shall support the Advanced Security SD (ASSD) Extension Simplified Specification [ASSD-EXT] to interface with the card commands specified in Appendix B of this document. [ASSD-EXT] serves as an extension to the SD Card Physical Layer Specification and provides all of the definitions required to transport security system specific command

[7] A security domain is a protected area on a smart card. 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 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.

packets from the ASSD enabled host (such as a mobile device) to the ASSD-enabled secure element and vice versa.

For use as a transport mechanism for APDUs, [ASSD-EXT] is constrained/profiled as below to promote interoperability between mobile devices and token implementations:

- The commands for the PIV Derived Application shall be transported only in ASSD mode.
- Only the [ASSD-EXT] command transfer protocol is supported for interoperable use. The secure data transfer commands are not relevant for PIV Derived Application use.
- A secure commands sequence composed of a WRITE_SEC_CMD command in cmd-mode shall always be followed by a READ_SEC_CMD command to retrieve the response to the command.
- The WRITE_SEC_CMD shall be implemented only in blocking mode to ensure that there is no interleaving of commands.

3.3.1.2 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 via over-the-air (OTA) mechanisms. 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. [GP-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 PIV Derived Application shall be implemented 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.

A UICC is a secure element, which may be capable of hosting a PIV Derived 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 Chip Card Interface Devices (CCID) and shall comply with the Universal Serial Bus Device Class: Smart Card CCID Specification for Integrated Circuit(s) Cards Interface Devices Specification [CCIDSPEC].

The APDUs for the PIV Derived 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 PIV Derived 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 PIV Derived 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. 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. 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

The Subscriber shall be authenticated to the cryptographic token before the private key corresponding to the Derived PIV Credential can be used. The subsections below include requirements on activation data establishment and reset for hardware as well as software implementations of the Derived PIV Credential.

3.4.1 Hardware Implementations

When the private key corresponding to the Derived PIV Credential is stored in a (removable or embedded) hardware cryptographic module, Personal Identification Number based (PIN-based) Subscriber activation shall be implemented. The PIN should not be easily guessable or otherwise individually identifiable in nature (e.g., part of a Social Security Number, phone number). The required PIN length shall be a minimum of six bytes.

At LoA-4, the hardware cryptographic module shall include a mechanism to block use of the PIV Derived Authentication private key after a number of consecutive failed authentication attempts as stipulated by the department or agency.[8] When required, PIN reset may be performed as described below.

The PIN may need to be reset if the Subscriber has forgotten the PIN or if PIN-lockout has occurred following repeated use of invalid PINs. PIN 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 PIN 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 PIV-AUTH mechanism as per section 6.2.3.1 of [FIPS 201]) prior to PIN 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. The issuer shall verify that the Derived PIV Credential is for the same Subscriber for whom the biometric match was completed.

[8] Subscribers may change their PINs anytime by providing the current PIN and the new PIN values.

578 • For remote PIN reset for hardware cryptographic modules the Subscriber's PIV Card shall be used
579 to authenticate the Subscriber (via PIV-AUTH authentication mechanism as per Section 6.2.3.1 of
580 [FIPS 201]) prior to PIN reset. If the reset occurs over a session that is separate from the session
581 over which the PIV-AUTH authentication mechanism was completed, strong linkage (e.g., using a
582 temporary secret) must be established between the two sessions. The issuer shall verify that the
583 Derived PIV Credential is for the same Subscriber that authenticated using the PIV Card. The
584 remote PIN reset shall be completed over a protected session (e.g., using TLS).

585 ### 3.4.2 Software Implementations

586 For software implementations (LOA-3) of Derived PIV Credentials, a password-based mechanism shall
587 be used to perform cryptographic operations with the private key corresponding to the Derived PIV
588 Credential. The password shall meet the requirements of an LOA-2 memorized secret token as specified
589 in Table 6, Token Requirements per Assurance Level, in [SP800-63].

590 For software cryptographic modules, password reset is not supported. The initial issuance process shall be
591 followed if the password is forgotten.

592 Lockout mechanisms for repeated unsuccessful activation attempts are not required for software
593 cryptographic modules.

594

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

In addition to the PIV Authentication key, [FIPS 201] 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 PIV Derived 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 key on the mobile device to be the same key as the one on the PIV Card. Neither [FIPS 201] nor [COMMON] precludes the 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 the key management private key in [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 certificate for 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 PIV Derived Applications implemented on removable hardware cryptographic tokens.

B.1 PIV Derived Application Data Model and Representation

The data model and representation requirements for PIV Derived 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 PIV Derived Application.

B.1.1 PIV Derived Application Identifier

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

'A0 00 00 03 08 XX XX XX XX XX XX' [Note: the specific value for the AID will be included in the final version of this document. It will be different from the AID of the PIV Card Application.]

The PIV Derived 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 XX XX XX XX'

B.1.2 PIV Derived Application Data Model Elements

The PIV Derived Application shall contain the following mandatory interoperable data object:

- **X.509 Certificate for PIV Derived Authentication—**The read access control rule for X.509 PIV Derived Authentication Certificate 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 [SP 800-73Part1].

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 3.3.2 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 “PIV Derived Application

655 AID."

656 o References to "PIV Card Application PIN" are replaced by "PIV Derived Application
657 PIN."

658 o The first byte of the PIN Usage Policy shall be set to 0x40. (This means that the Global
659 PIN does not satisfy the access control rules for command execution and data object
660 access within the PIV Derived Application.)

661 • **Key History Object—**Up to 20 retired key management private keys may be stored in the PIV
662 Derived Application. The Key History Object shall be present in the PIV Derived Application if
663 the PIV Derived Application contains any retired key management private keys, but may be
664 present even if no such keys are present in the PIV Derived Application. The requirements for
665 the Key History object are as described in Section 3.3.3 of [SP800-73Part1] except for the
666 following:

667 o References to "*keysWithOnCardCerts*" should be interpreted as keys for which the
668 corresponding certificate is populated within the PIV Derived Application.

669 o References to "*keysWithOffCardCerts*" should be interpreted as keys for which the
670 corresponding certificate is not populated within the PIV Derived Application.

671 o References to "*offCardCertURL*" should be interpreted as a URL that points to a file
672 containing the certificates corresponding to all of the retired key management private
673 keys within the PIV Derived Application including those for which the corresponding
674 certificate is stored within the PIV Derived Application.

675 • **Retired X.509 Certificates for Key Management**—The read access control rules for the Retired
676 X.509 Certificates for Key Management and PKI cryptographic function access rules for
677 corresponding private keys are as described in Section 3.3.4 of [SP800-73Part1].

678 • **Security Object—**The Security Object shall be present in the PIV Derived Application if either
679 the Discovery Object or the Key History Object is present, and shall be absent otherwise. The
680 requirements for the Security Object are as described in Section 3.1.7 of [SP800-73Part1], except
681 for the following:

682 o The Security Object for a PIV Derived Application is signed using a private key whose
683 corresponding public key is contained in a PIV content signing certificate that satisfies
684 the requirements for certificates used to verify signatures on Cardholder Unique
685 Identifiers (CHUID), as specified in Section 4.2.1 of [FIPS 201].

686 o The signature field of the Security Object, tag 0xBB, shall include the Derived PIV
687 Credential Issuer's certificate.

688 o All unsigned data objects (i.e., the Discovery Object and the Key History Object) within
689 the PIV Derived Application shall be included in the Security Object.

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

692 Section 3.5 of [SP800-73Part1] provides the container IDs and Access Rules for the mandatory and

693 optional data objects for a PIV Derived Application with the following mappings:

694

695

PIV Derived Application Data Object	PIV Card Application Data Object
X.509 Certificate for PIV Derived 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*

696 **Table B-1 Mapping of Data Objects**

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

700 • References to contactless interface are not applicable. The PIV Derived Application only supports
701 a contact interface.

702 • The Security Object for the PIV Derived Application is optional. It is required if either the
703 optional Discovery Object or the optional Key History Object is present.

704 ### B.1.3 PIV Derived Application Data Objects Representation

705 The ASN.1 object identifiers (OID) and "basic encoding rules – tag length value" (BER-TLV) tags for
706 the various mandatory and optional data objects within the PIV Derived Application are the same as for
707 the corresponding data objects (mapped per the table above) of the PIV Card Application as described in
708 Section 4 of [SP800-73Part1].

709 ### B.1.4 PIV Derived Application Data Types and their Representation

710 This appendix provides a description of the data types used in the PIV Derived Application Command
711 Interface.

712 #### B.1.4.2 PIV Derived Application Key References

713 Key references are assigned to keys and PINs of the PIV Derived Application. Table 6-1 of [SP800-78]
714 and Table 4 of [SP800-73Part1] define the key reference values that shall be used on the PIV Derived
715 Application interfaces with the following mappings:

716

PIV Derived Key Type	PIV Key Type
Global PIN	Global PIN

PIV Derived Key Type	PIV Key Type
PIV Derived Application PIN	PIV Card Application PIN
PIV Unblocking Key	PIN Unblocking Key
PIV Derived Authentication Key	PIV Authentication Key
PIV Derived 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 PIV Derived Application (mapped per the table above) except for the following:

- References to "PIV Card Application" are replaced by "PIV Derived Application"

B.1.4.3 PIV Derived Application Cryptographic Algorithm and Mechanism Identifiers

The algorithm identifiers for the cryptographic algorithms that may be recognized on the PIV Derived Application interfaces are the asymmetric and symmetric identifiers specified in Table 6-2 of [SP 800-78]. The cryptographic mechanism identifiers that may be recognized on the PIV Derived Application interfaces are those specified in Table 5 of [SP800-73Part1].

B.1.4.4 PIV Derived Application Status Words

The status words that may be returned on the PIV Derived Application command interface are as specified in Section 5.6 of [SP800-73Part1].

B.1.5 PIV Derived Authentication Mechanisms

The PIV Derived Application supports the following validation steps:

- Credential Validation (CredV) through verification of the certificates retrieved from the PIV Derived Application and checking of the revocation status of these certificates.

- PIV Derived Application Holder Validation (HolderV) through matching the PIN provided by the token holder with the PIN within the PIV Derived Application.

The PIV Derived Application facilitates a single authentication mechanism, which is a cryptographic challenge and response authentication protocol using the PIV Derived Authentication private key as described in Appendix B.1.2 of [SP80073Part1] with the following translations:

- References to "PIV Application" are replaced by "PIV Derived Application."

- References to "PIV Auth Certificate" are replaced by "PIV Derived Authentication Certificate."

- References to "PIV Card App ID" are replaced with "PIV Derived Application ID."

B.2 PIV Derived Application Token Command Interface

This appendix contains the technical specifications of the command interface to the PIV Derived Application surfaced by the card edge of the Integrated Circuit Card (ICC) that represents the removable hardware cryptographic token. The command interface for the PIV Derived 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 “PIV Derived Application”
- References to the contactless interface are ignored
- References to “PIV Data Objects” are replaced by “PIV Derived Data Objects”
- References to “PIV Authentication Key” are replaced with “PIV Derived Authentication Key”
- In Appendix A:
    - References to “PIV Card Application Administrator” are replaced by “PIV Derived Application Administrator”
    - References to “Card Management Key” are replaced by “PIV Derived 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 PIV Derived Application, or it may be another application.

Appendix C—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 C-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 smaller 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 C-1,[9] four of the five tokens with Derived Credentials are integrated. For these tokens, future 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	Future Alternate OMB Guidance for Integrated Tokens
PIV Derived 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 C-1 Token types and Relation to OMB's Electronic Authentication Guidelines

[9] 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 D—Glossary (Informative)

Selected terms used in the guide are defined below.

Derived PIV Credential: An X.509 PIV Derived 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 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.

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

All other significant technical terms used within this document are defined in other key documents including [FIPS201], [SP800-63] and [SP 800-73].

Appendix E—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
ASSD	Advanced Security SD
BER	Basic Encoding Rules
CCID	Chip Card Interface Device
FIPS	Federal Information Processing Standard
HSPD	Homeland Security Presidential Directive
ICC	Integrated Circuit Card
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
OTA	Over-the-Air
PCI	PIV Card Issuer
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
P.L.	Public Law
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
VCI	Virtual Contact Interface

Appendix F—References (Informative)

This appendix provides references for the document.

[ASSD-EXT] *Advanced Security SD Extension Simplified Specification Version 2.00*, May 2010. Available at https://www.sdcard.org/downloads/pls/simplified_specs/archive/partA1_200.pdf.

[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.

[CCID] *Universal Serial Bus Device Class: Smart Card CCID Specification for Integrated Circuit(s) Cards Interface Devices*, Revision 1.1, April 2005. Available at http://www.usb.org/developers/devclass_docs/DWG_Smart-Card_CCID_Rev110.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.

[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] Draft NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, NIST, May 2013, or as amended. Available at http://csrc.nist.gov.

[SP800-78] Draft NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, May 2013, 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, or as amended. Soon 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.