

2

3

4

5

6

7

Guidelines for Derived Personal Identity Verification (PIV) Credentials

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

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

24

25

26

27

28

29

30

31

32 **Draft NIST Special Publication 800-157**

33

34

35

36

Guidelines for Derived Personal Identity Verification (PIV) Credentials

37

38

39

Hildegard Ferraiolo

40

David Cooper

41

Salvatore Francomacaro

42

Andrew Regenscheid

43

Computer Security Division

44

Information Technology Laboratory, NIST

45

46

William Burr

47

Dakota Consulting, Inc.

48

49

Jason Mohler

50

Sarbari Gupta

51

Electrosoft Services, Inc.

52

53

54

55

March 2014

56

57

58

59

60

61

62

63

64

65

66

U.S. Department of Commerce

67

Penny Pritzker, Secretary

68

69

National Institute of Standards and Technology

70

Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director



71
72

Authority

73 This publication has been developed by NIST to further its statutory responsibilities under the Federal
74 Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for
75 developing information security standards and guidelines, including minimum requirements for Federal
76 information systems, but such standards and guidelines shall not apply to national security systems
77 without the express approval of appropriate Federal officials exercising policy authority over such
78 systems. This guideline is consistent with the requirements of the Office of Management and Budget
79 (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-
80 130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130,
81 Appendix III, *Security of Federal Automated Information Resources*.

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

88
89
90
91

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

92

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.

93
94
95
96
97
98
99

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.

100
101

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>.

102
103
104
105
106
107
108

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

109 Reports on Computer Systems Technology

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

119

120 Abstract

121 This recommendation provides technical guidelines for the implementation of standards-based, secure,
122 reliable, interoperable PKI-based identity credentials that are issued by Federal departments and agencies
123 to individuals who possess and prove control over a valid PIV Card. The scope of this document includes
124 requirements for initial issuance, maintenance and termination of these credentials, certificate policies and
125 cryptographic specifications, technical specifications for permitted cryptographic token types and the
126 command interfaces for the removable implementations of such cryptographic tokens.

127

128 Keywords

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

131

132 Acknowledgments

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

139

140 Trademark Information

141 All registered trademarks or trademarks belong to their respective organizations.

142

143

144

Table of Contents

145	Executive Summary	iv
146	1. Introduction	5
147	1.1 BACKGROUND	5
148	1.2 PURPOSE AND SCOPE	6
149	1.3 AUDIENCE:	7
150	1.4 DOCUMENT STRUCTURE	7
151	1.5 KEY TERMINOLOGY	8
152	2. Lifecycle Activities and Related Requirements	9
153	2.1 INITIAL ISSUANCE	9
154	2.2 MAINTENANCE	9
155	2.3 TERMINATION	10
156	2.4 LINKAGE WITH PIV CARD	11
157	3. Technical Requirements	12
158	3.1 CERTIFICATE POLICIES	12
159	3.2 CRYPTOGRAPHIC SPECIFICATIONS	12
160	3.3 CRYPTOGRAPHIC TOKEN TYPES	12
161	3.3.1 <i>Removable (Non-Embedded) Hardware Cryptographic Tokens</i>	13
162	3.3.2 <i>Embedded Cryptographic Tokens</i>	15
163	3.4 ACTIVATION DATA	15
164	3.4.1 <i>Hardware Implementations</i>	15
165	3.4.2 <i>Software Implementations</i>	16
166		
167	Appendix A— Digital Signature and Key Management Keys (Informative)	17
168	Appendix B— Data Model and Interfaces for Removable (Non-Embedded) Hardware	
169	Cryptographic Tokens (Normative)	18
170	B.1 PIV DERIVED APPLICATION DATA MODEL AND REPRESENTATION	18
171	B.1.1 <i>PIV Derived Application Identifier</i>	18
172	B.1.2 <i>PIV Derived Application Data Model Elements</i>	18
173	B.1.3 <i>PIV Derived Application Data Objects Representation</i>	20
174	B.1.4 <i>PIV Derived Application Data Types and their Representation</i>	20
175	B.1.5 <i>PIV Derived Authentication Mechanisms</i>	21
176	B.2 PIV DERIVED APPLICATION TOKEN COMMAND INTERFACE	22
177	Appendix C— Derived PIV Credentials in Relation to OMB Memoranda (Informative)	23
178	Appendix D— Glossary (Informative)	24
179	Appendix E— Acronyms and Abbreviations (Informative)	25
180	Appendix F— References (Informative)	26
181		
182		
183	Table B-1 Mapping of Data Objects	20
184	Table B-2 Mapping of Key Types	21
185	Table C-1 Token types and Relation to OMB’s Electronic Authentication Guidelines	23

List of Tables

186 Executive Summary

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

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

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

213 Derived PIV Credentials are based on the general concept of derived credential in SP 800-63-2, which
214 leverages identity proofing and vetting results of current and valid credentials. When applied to PIV,
215 identity proofing and vetting processes do not have to be repeated to issue a Derived PIV Credential.
216 Instead, the user proves possession of a valid PIV Card to receive a Derived PIV Credential. To achieve
217 interoperability with the PIV infrastructure and its applications, a Derived PIV Credential is a PKI
218 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.

219

220 **1. Introduction**

221 FIPS 201 specifies a common set of identity credentials for the purpose of HSPD-12 in a smart card form
222 factor, known as the Personal Identity Verification (PIV) Card. This publication is a companion document
223 to FIPS 201 that specifies use of an additional common identity credential, a Derived PIV Credential,
224 which is issued by a Federal department or agency and may be used with mobile devices where the use of
225 a PIV Card is not practical. Consistent with the goals of HSPD-12, the Derived PIV Credential is
226 designed to serve as a Federal government-wide standard for a secure and reliable identity credential that
227 is interoperable across agencies.

228 **1.1 Background**

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

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

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

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

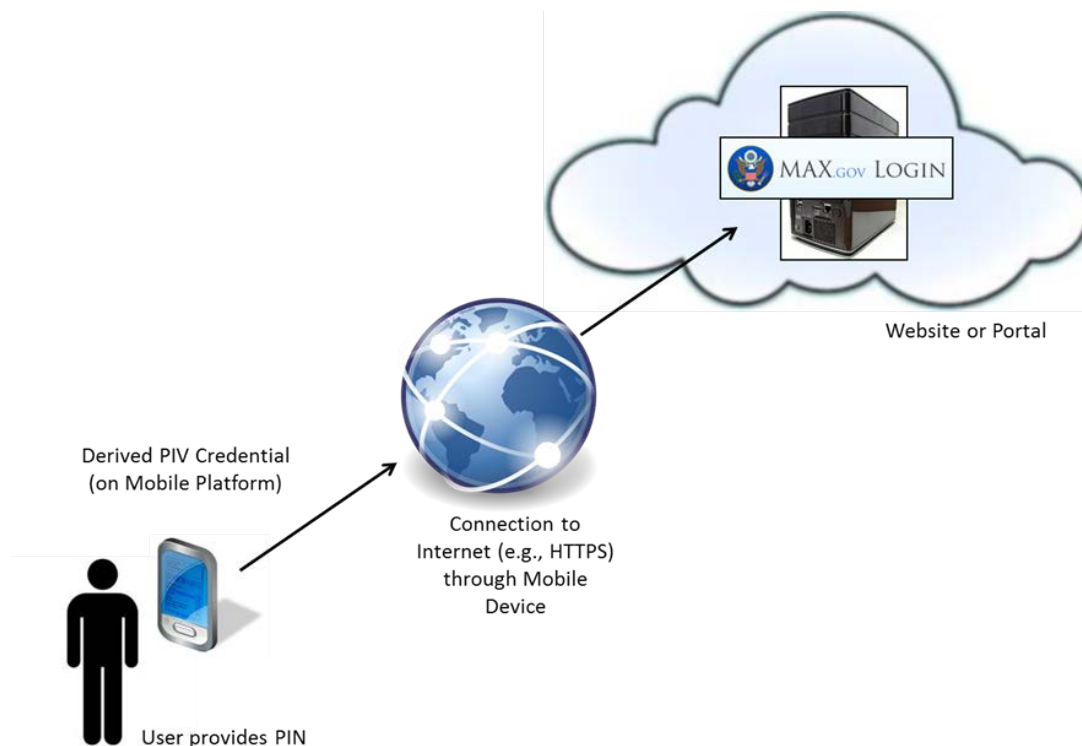
264 card-management functionalities of the PIV Card over a secure wireless channel using the virtual contact
 265 interface (VCI).

266 1.2 Purpose and Scope

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

276 The scope of the Derived PIV Credential is to provide PIV-enabled authentication services on the mobile
 277 device to authenticate the credential holder to remote systems as illustrated in Figure 1-1.

278 To achieve interoperability with the PIV infrastructure and its applications, public key infrastructure
 279 (PKI) technology has been selected as the basis for the Derived PIV Credential. The PKI based Derived
 280 PIV Credentials specified in this document are issued at levels of assurance (LOA) 3 and 4.³



281

282

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.

283 Derived PIV Credentials are based on the general concept of derived credential in SP 800-63, which
284 leverages identity proofing and vetting results of current and valid credentials. When applied to PIV,
285 identity proofing and vetting processes do not have to be repeated to issue a Derived PIV Credential.
286 Instead, the user proves possession of a valid PIV Card to receive a Derived PIV Credential. The Derived
287 PIV Credential is a PIV Derived Authentication certificate, which is an X.509 public key certificate that
288 has been issued in accordance with the requirements of this document and the *X.509 Certificate Policy for*
289 *the U.S. Federal PKI Common Policy Framework* [COMMON]. While the PIV Card may be used as the
290 basis for issuing other types of derived credentials, the issuance of these other credentials is outside the
291 scope of this document. Only derived credentials issued in accordance with this document are considered
292 to be Derived PIV credentials.

293 The document provides the technical guidelines on:

- 294 • Three primary lifecycle activities for the Derived PIV Credential – initial issuance, maintenance
295 and termination – and the requirements for each activity to ensure security; and
- 296 • Technical requirements for the Derived PIV Credential including certificate policies,
297 cryptographic specifications, types of cryptographic implementation that are permitted and
298 mechanisms for activation and use of the credential.

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

301 **1.3 Audience:**

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

304 **1.4 Document Structure**

305 The structure of the rest of this document is as follows:

- 306 • Section 2 describes Derived PIV Credential lifecycle activities and related requirements. This
307 section is *normative*.
- 308 • Section 3 describes the technical requirements for implementing Derived PIV Credentials. This
309 section is *normative*.
- 310 • Appendix A contains guidance on digital signature and key management keys. This appendix is
311 *informative*.
- 312 • Appendix B provides detailed interface requirements for the removable hardware
313 implementations. This appendix is *normative* for implementation of Derived PIV on removable
314 (non-embedded) hardware cryptographic tokens.
- 315 • Appendix C summarizes the association of the Derived PIV Credentials' token types with the
316 electronic authentication policies in OMB memoranda M-06-16 and M-07-16. This appendix is
317 *informative*.
- 318 • Appendix D contains a glossary defining selected terms from this document. This appendix is
319 *informative*.

320 • Appendix E defines acronyms and other abbreviations used in this document. This appendix is
321 *informative*.

322 • Appendix F provides a list of references for this document. This appendix is *informative*.

323 **1.5 Key Terminology**

324 Certain key PIV terms have assigned meanings within the context of this document. The term “PIV
325 Cardholder” refers to a person who possesses a valid PIV Card, regardless of whether they have been
326 issued a Derived PIV Credential. The term “Applicant” refers to a PIV Cardholder who is pending
327 issuance of a Derived PIV Credential, and the term “Subscriber” refers to a PIV Cardholder who has
328 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

369 under which the PIV Derived Authentication certificate is issued. When certificate re-key or modification
370 is performed remotely for an LOA-4 Derived PIV Credential, the following shall apply:

371 + Communication between the issuer and the cryptographic module in which the PIV Derived
372 Authentication private key is stored shall occur only over mutually authenticated secure sessions
373 between tested and validated cryptographic modules.

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

376 The initial issuance process shall be followed for:

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

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

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

382 The Derived PIV Credential is unaffected by loss, theft or damage to the Subscriber's PIV Card.⁵ The
383 ability to use the Derived PIV Credential is especially useful in such circumstances because the PIV Card
384 is unavailable, yet the Subscriber is able to use the Derived PIV Credential to gain logical access to
385 remote Federally controlled information systems from his/her mobile device. Similarly, the Derived PIV
386 Credential is unaffected by the revocation of the PIV Authentication certificate. Some maintenance
387 activities for the subscriber's PIV Card may trigger corresponding maintenance activities for the Derived
388 PIV Credential. For example, if the subscriber's PIV Card is reissued as a result of the Subscriber's name
389 change, a new PIV Derived Authentication certificate with the new name may also need to be issued.

390 **2.3 Termination**

391 A Derived PIV Credential shall be terminated when the department or agency that issued the credential
392 determines that the Subscriber is no longer eligible to have a PIV Card (i.e., PIV Card is terminated⁶). A
393 Derived PIV Credential may also be terminated when the department or agency that issued the credential
394 determines that the Subscriber no longer requires a derived credential, even if the Subscriber's PIV Card
395 is not being terminated. The latter may happen, for example, when the Subscriber's role in the agency
396 changes such that he/she no longer has the need to access agency resources from a mobile device using a
397 Derived PIV Credential.

398 If the PIV Derived Authentication private key was created and stored on a hardware cryptographic token
399 that does not permit the user to export the private key, then termination of the Derived PIV Credential
400 may be performed by either: 1) collecting and either zeroizing the private key or destroying the token or
401 2) revoking the PIV Derived Authentication certificate. In all other cases, termination shall be performed
402 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.

403 **2.4 Linkage with PIV Card**

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

408 The issuer of the Derived PIV Credential shall not solely rely on tracking the revocation status of the PIV
409 Authentication certificate as a means of tracking the termination status of the PIV Card. This is because
410 there are scenarios where the card's PIV Authentication certificate is not revoked even though the PIV
411 Card has been terminated. This may happen, for example, when a terminated PIV Card is collected and
412 either zeroized or destroyed by an agency – in this case, in accordance with [FIPS201], the corresponding
413 PIV Authentication certificate does not need to be revoked.

414 Additional methods must be employed for maintaining a linkage between the current PIV Card and the
415 corresponding Derived PIV Credential. Some example mechanisms to maintain this linkage are listed
416 below – however, any other mechanism that meets the above requirements is also acceptable.

- 417 • If the Derived PIV Credential is issued by the same agency that issued the Subscriber's PIV Card,
418 the linkage between the two credentials may be maintained through the common Identity
419 Management System (IDMS) database implemented by the issuing agency.
- 420 • When the issuer of the Derived PIV Credential is different from the PIV Card Issuer, the
421 following mechanisms may be applied:
 - 422 ○ The Backend Attribute Exchange [BAE] can be queried for the termination status of the
423 PIV Card, if an attribute providing this information is defined and the issuer of the PIV
424 Card maintains this attribute for the Subscriber.
 - 425 ○ The issuer of the PIV Card maintains a list of corresponding Derived PIV Credential
426 issuers and sends notification to the latter set when the PIV Card is terminated.
 - 427 ○ If a Uniform Reliability and Revocation Service (URRS) is implemented in accordance
428 with Section 3.7 of [NISTIR7817], the issuer of a Derived PIV Credential may obtain
429 termination status of the Subscriber's PIV Card through the URRS.

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

433 **3. Technical Requirements**

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

435 **3.1 Certificate Policies**

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

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

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

447 **3.2 Cryptographic Specifications**

448 The cryptographic algorithm and key size requirements for the PIV Derived Authentication certificate and
449 private key are the same as the requirements for the PIV Authentication certificate and private key, as
450 specified in [SP800-78].

451 For PIV Derived Authentication certificates issued under id-fpki-common-pivAuth-derived-hardware, the
452 PIV Derived Authentication key pair shall be generated within a hardware cryptographic module that has
453 been validated to [FIPS140] Level 2 or higher that provides Level 3 physical security to protect the PIV
454 Derived Authentication private key while in storage and that does not permit exportation of the private
455 key.

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

459 **3.3 Cryptographic Token Types**

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

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

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

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

475 **3.3.1 Removable (Non-Embedded) Hardware Cryptographic Tokens**

476 This section provides requirements for implementations where the PIV Derived Authentication private
477 key resides in a hardware cryptographic module (or token) that can be removed from the mobile device.
478 In such cases, a *PIV Derived Application*, as defined in Appendix B, shall be implemented on the
479 hardware cryptographic token. When the removable hardware cryptographic module supports multiple
480 security domains⁷ managed by independent issuers, the PIV Derived Application shall be implemented in
481 a security domain that is separate from other security domains, dedicated to the Derived PIV Credential,
482 and under the explicit control of the issuing agency.

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

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

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

493 **3.3.1.1 SD Card with Cryptographic Module**

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

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

501 The secure element used for the PIV Derived Application shall support the Advanced Security SD
502 (ASSD) Extension Simplified Specification [ASSD-EXT] to interface with the card commands specified
503 in Appendix B of this document. [ASSD-EXT] serves as an extension to the SD Card Physical Layer
504 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.

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

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

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

516 **3.3.1.2 UICC with Cryptographic Module**

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

521 The UICC includes storage and processing, as well as input/output capabilities. Unlike the SIM card, the
522 UICC can also support a variety of other applications and services and multiple security domains. [GP-A]
523 defines a mechanism for an application provider to manage (i.e., load, install and personalize) its
524 application in a confidential manner while using a third party communication network. The PIV Derived
525 Application shall be implemented in a security domain that is separate from other security domains,
526 dedicated to the Derived PIV Credential, and under the explicit control of the issuing agency.

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

530 **3.3.1.3 USB Token with Cryptographic Module**

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

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

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

541 USB tokens with cryptographic modules that support a PIV Derived Application shall also be compliant

542 with the specifications in [SP800-96] for APDU support for contact card readers.

543 The requirements for the Application Programming Interface (API) for PIV Derived Application
544 implementations are beyond the scope of this document.

545 **3.3.2 Embedded Cryptographic Tokens**

546 A Derived PIV Credential and its associated private key may be used in cryptographic modules that are
547 embedded within mobile devices. These modules may either be in the form of a hardware cryptographic
548 module that is a component of the mobile device or in the form of a software cryptographic module that
549 runs on the device. The cryptographic module shall satisfy the requirements in Section 3.2 for either
550 certificates issued under id-fpki-common-pivAuth-derived-hardware or id-fpki-common-pivAuth-derived.
551 As described in Appendix A, these same cryptographic modules may also hold other keys, such as digital
552 signature and key management private keys and their corresponding certificates.

553 **3.4 Activation Data**

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

557 **3.4.1 Hardware Implementations**

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

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

566 The PIN may need to be reset if the Subscriber has forgotten the PIN or if PIN-lockout has occurred
567 following repeated use of invalid PINs. PIN reset may be performed at the issuer's facility, at an
568 unattended kiosk operated by the issuer, or remotely via a general computing platform.

- 569
- 570 • When PIN reset is performed in-person at the issuer's facility, or at an unattended kiosk operated
571 by the issuer, it shall be implemented through one of the following processes:
 - 572 ○ The Subscriber's PIV Card shall be used to authenticate the Subscriber (via PIV-AUTH
573 mechanism as per section 6.2.3.1 of [FIPS 201]) prior to PIN reset. The issuer shall verify
574 that the Derived PIV Credential is for the same Subscriber that authenticated using the
575 PIV Card.
 - 576 ○ A 1:1 biometric match shall be performed against the biometric sample retained during
577 initial issuance of the Derived PIV Credential. The issuer shall verify that the Derived PIV
578 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

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

596 In addition to the PIV Authentication key, [FIPS 201] also requires each PIV Card to have a digital
597 signature key and a key management key, unless the cardholder does not have a government-issued email
598 account at the time of credential issuance. A subscriber who has been issued a PIV Derived
599 Authentication certificate for use with a mobile device may also have a need to use a digital signature and
600 key management key with that mobile device.

601 For most Subscribers, it will be necessary for the key management key on the mobile device to be the
602 same key as the one on the PIV Card. Neither [FIPS 201] nor [COMMON] precludes the key
603 management private key from being used on more than one device (e.g., the PIV Card and a smart phone)
604 as long as all of the requirements of the policy under which the key management certificate was issued are
605 satisfied. Note that this means that in order to be able to use a copy of the key management private key in
606 [FIPS140] Level 1 software cryptographic module the corresponding certificate would have to be issued
607 under a certificate policy, such as id-fpki-common-policy, that does not require the use of a [FIPS140]
608 Level 2 hardware cryptographic module. This should be taken into account at the time that the key
609 management certificate that will be placed on the PIV Card is issued. Key recovery mechanisms are
610 encouraged for key management keys issued to mobile devices.

611 As the digital signature key on a PIV Card cannot be copied, a mobile device will have to be issued a new
612 digital signature private key and certificate. The issuance of this private key and certificate is completely
613 independent of the issuance of the PIV Card, although the issuer may choose to leverage the Applicant's
614 PIV Card to identity proof the Applicant prior to issuing the digital signature certificate. As the certificate
615 policies associated with digital signature certificates in [COMMON] (id-fpki-common-policy, id-fpki-
616 common-hardware, and id-fpki-common-High) are not limited to use with PIV Cards, a certificate for a
617 digital signature certificate for a mobile device may be issued under one of these policies, as long as all of
618 the requirements of the policy are satisfied.

619 **Appendix B—Data Model and Interfaces for Removable (Non-Embedded) Hardware** 620 **Cryptographic Tokens (Normative)**

621 This appendix provides data model and interface requirements for the PIV Derived Applications
622 implemented on removable hardware cryptographic tokens.

623 **B.1 PIV Derived Application Data Model and Representation**

624 The data model and representation requirements for PIV Derived Applications are based on the
625 requirements for PIV Card Applications as described in [SP800-73Part1]. The specifications for the
626 mandatory and optional data objects listed below are the same as the specifications of the corresponding
627 data objects on a PIV Card Application as described in [SP800-73Part1], except for the general difference
628 that the contactless interface is not supported by the PIV Derived Application.

629 **B.1.1 PIV Derived Application Identifier**

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

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

635 The PIV Derived Application can be selected as the current application on the removable hardware
636 cryptographic token by providing the full AID listed above or by providing the right truncated version, as
637 follows:

638 'A0 00 00 03 08 XX XX XX XX'

639 **B.1.2 PIV Derived Application Data Model Elements**

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

641 • **X.509 Certificate for PIV Derived Authentication**—The read access control rule for X.509 PIV
642 Derived Authentication Certificate and the PKI cryptographic function access rule for the
643 corresponding private key are as described for the X.509 Certificate for PIV Authentication in
644 Section 3.1.3 of [SP 800-73Part1].

645 The optional data objects are as follows:

646 • **X.509 Certificate for Digital Signature**—The read access control rule for the X.509 Certificate
647 for Digital Signature and the PKI cryptographic function access rule for the corresponding private
648 key are as described in Section 3.2.1 of [SP800-73Part1].

649 • **X.509 Certificate for Key Management**—The read access control rule for the X.509 Certificate
650 for Key Management and the PKI cryptographic function access rule for the corresponding
651 private key are as described in Section 3.3.2 of [SP800-73Part1].

652 • **Discovery Object**—The requirements for the Discovery Object are as described in Section 3.3.2
653 of [SP800-73Part1] except for the following:

654 ○ References to “PIV Card Application AID” are replaced by “PIV Derived Application

- 655 AID.”
- 656 ○ References to “PIV Card Application PIN” are replaced by “PIV Derived Application
657 PIN.”
- 658 ○ 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 ○ References to “*keysWithOnCardCerts*” should be interpreted as keys for which the
668 corresponding certificate is populated within the PIV Derived Application.
- 669 ○ References to “*keysWithOffCardCerts*” should be interpreted as keys for which the
670 corresponding certificate is not populated within the PIV Derived Application.
- 671 ○ 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 ○ 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 ○ The signature field of the Security Object, tag 0xBB, shall include the Derived PIV
687 Credential Issuer’s certificate.
- 688 ○ 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 Security Object	X.509 Certificate for PIV Authentication 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 <i>n</i>	Retired X.509 Certificate for Key Management <i>n</i>

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

717 **Table B-2 Mapping of Key Types**

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

- 720 • References to “PIV Card Application” are replaced by “PIV Derived Application”

721 **B.1.4.3 PIV Derived Application Cryptographic Algorithm and Mechanism** 722 **Identifiers**

723 The algorithm identifiers for the cryptographic algorithms that may be recognized on the PIV Derived
724 Application interfaces are the asymmetric and symmetric identifiers specified in Table 6-2 of [SP 800-
725 78]. The cryptographic mechanism identifiers that may be recognized on the PIV Derived Application
726 interfaces are those specified in Table 5 of [SP800-73Part1].

727 **B.1.4.4 PIV Derived Application Status Words**

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

730 **B.1.5 PIV Derived Authentication Mechanisms**

731 The PIV Derived Application supports the following validation steps:

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

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

- 739 • References to “PIV Application” are replaced by “PIV Derived Application.”
- 740 • References to “PIV Auth Certificate” are replaced by “PIV Derived Authentication Certificate.”
- 741 • References to “PIV Card App ID” are replaced with “PIV Derived Application ID.”

742 **B.2 PIV Derived Application Token Command Interface**

743 This appendix contains the technical specifications of the command interface to the PIV Derived
744 Application surfaced by the card edge of the Integrated Circuit Card (ICC) that represents the removable
745 hardware cryptographic token. The command interface for the PIV Derived Application shall implement
746 all of the card commands supported by the PIV Card Application as described in [SP800-73Part2], which
747 include:

- 748 • SELECT
- 749 • GET DATA
- 750 • VERIFY
- 751 • CHANGE REFERENCE DATA
- 752 • RESET RETRY COUNTER
- 753 • GENERAL AUTHENTICATE
- 754 • PUT DATA
- 755 • GENERATE ASYMMETRIC KEY PAIR

756 The specifications for the token command interface shall be the same as the specifications for the
757 corresponding card edge commands for a PIV Card as described in [SP800-73Part2], except for the
758 following deviations:

- 759 • References to “PIV Card Application” are replaced by “PIV Derived Application”
- 760 • References to the contactless interface are ignored
- 761 • References to “PIV Data Objects” are replaced by “PIV Derived Data Objects”
- 762 • References to “PIV Authentication Key” are replaced with “PIV Derived Authentication Key”
- 763 • In Appendix A:
 - 764 ○ References to “PIV Card Application Administrator” are replaced by “PIV Derived
765 Application Administrator”
 - 766 ○ References to “Card Management Key” are replaced by “PIV Derived Token
767 management Key”

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

772 **Appendix C—Derived PIV Credentials in Relation to OMB Memoranda (Informative)**

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

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

780 Increasingly, mobile devices are becoming smaller and/or lighter. These constraints limit external ports
781 and force the integration of authentication tokens and security features. As indicated by column 6 in
782 Table C-1,⁹ four of the five tokens with Derived Credentials are integrated. For these tokens, future
783 guidance will be made available by OMB to provide an alternative to the remote authentication policy in
784 M-06-16 and M-07-16. With integrated tokens, authentication factors are not provided by a separate
785 token and sensitive government information may be at greater risk of loss. OMB's alternative guidance
786 intends to also address these risks by pointing to NIST guidelines for compensating controls (e.g., SP
787 800-53, SP 800-124, SP 800-164).

788 Note: To provide a complete set of options for PIV-enabled remote access with mobile devices, the PIV
789 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	✓	

790 **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)

792 Selected terms used in the guide are defined below.

793 **Derived PIV Credential:** An X.509 PIV Derived Authentication certificate, which is issued in
794 accordance with the requirements specified in this document where the PIV Authentication certificate on
795 the applicant's PIV Card serves as the original credential. The Derived PIV Credential is an additional
796 common identity credential under HSPD-12 and FIPS 201 that is issued by a Federal department or
797 agency and used with mobile devices.

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

804
805 **PIV Derived Application:** A standardized application residing on a removable, hardware cryptographic
806 token that hosts a Derived PIV Credential and associated mandatory and optional elements.

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

809

810 **Appendix E—Acronyms and Abbreviations (Informative)**

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

812	AID	Application Identifier
813	APDU	Application Protocol Data Unit
814	API	Application Programming Interface
815	ASN.1	Abstract Syntax Notation One
816	ASSD	Advanced Security SD
817	BER	Basic Encoding Rules
818	CCID	Chip Card Interface Device
819		
820	FIPS	Federal Information Processing Standard
821	HSPD	Homeland Security Presidential Directive
822	ICC	Integrated Circuit Card
823	IT	Information Technology
824	ITL	Information Technology Laboratory
825	LOA	Level of Assurance
826	NFC	Near Field Communication
827	NIST IR	National Institute of Standards and Technology Interagency or Internal Reports
828	NIST	National Institute of Standards and Technology
829		
830	OID	Object Identifier
831	OMB	Office of Management and Budget
832	OTA	Over-the-Air
833	PCI	PIV Card Issuer
834	PIN	Personal Identification Number
835	PIV	Personal Identity Verification
836	PKI	Public Key Infrastructure
837	P.L.	Public Law
838	SD	Secure Digital
839	SE	Secure Element
840	SIM	Subscriber Identity Module
841	SP	Special Publication
842	TLS	Transport Layer Security
843	TLV	Tag-Length-Value
844	UICC	Universal Integrated Circuit Card
845	URL	Uniform Resource Locator
846	USB	Universal Serial Bus
847	VCI	Virtual Contact Interface
848		

849 Appendix F—References (Informative)

- 850 This appendix provides references for the document.
- 851 [ASSD-EXT] *Advanced Security SD Extension Simplified Specification Version 2.00*, May 2010.
852 Available at https://www.sdcard.org/downloads/pls/simplified_specs/archive/partA1_200.pdf.
- 853 [BAE] *Backend Attribute Exchange (BAE) v2.0 Overview*, January 2012. Available at
854 http://idmanagement.gov/sites/default/files/documents/BAE_v2_Overview_Document_Final_v1.0.0.pdf.
- 855 [CCID] *Universal Serial Bus Device Class: Smart Card CCID Specification for Integrated Circuit(s)*
856 *Cards Interface Devices*, Revision 1.1, April 2005. Available at
857 http://www.usb.org/developers/devclass_docs/DWG_Smart-Card_CCID_Rev110.pdf.
- 858 [COMMON] *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Version
859 1.21, December 2012. Available at [http://www.idmanagement.gov/documents/common-policy-](http://www.idmanagement.gov/documents/common-policy-framework-certificate-policy)
860 [framework-certificate-policy](http://www.idmanagement.gov/documents/common-policy-framework-certificate-policy). [Note: A change proposal that would add the id-fpki-common-pivAuth-
861 derived and id-fpki-common-pivAuth-derived-hardware policies to this certificate policy has been
862 submitted to the Federal PKI Policy Authority.]
- 863 [FIPS140] FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25,
864 2001, or as amended. Available at <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.
- 865 [FIPS201] FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and*
866 *Contractors*, NIST, August 2013, or as amended. Available at
867 <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf>.
- 868 [GP-A] *Confidential Card Content Management – GlobalPlatform Card Specification v2.2 - Amendment*
869 *A v1.0.1*, January 2011. Available at <http://www.globalplatform.org/specificationscard.asp>.
- 870 [GP-SPEC] *GlobalPlatform Card Specification Version 2.2.1*, January 2011. Available at
871 <http://www.globalplatform.org/specificationscard.asp>.
- 872 [GP-SE] *GlobalPlatform Card Secure Element Configuration v1.0*, October 2012. Available at
873 <http://www.globalplatform.org/specificationscard.asp>.
- 874 [M0404] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, OMB,
875 December 2003.
- 876 [M0616] OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, OMB, December
877 2006.
- 878 [M0716] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of*
879 *Personally Identifiable Information*, OMB, May 2007.
- 880 [NISTIR7817] NIST Interagency Report 7817, *A Credential Reliability and Revocation Model for*
881 *Federated Identities*, November 2012. Available at <http://csrc.nist.gov>.
- 882 [NISTIR7981] Draft NIST Interagency Report 7981, *Mobile, PIV, and Authentication*, March 2014.
883 Available at <http://csrc.nist.gov>.

- 884 [PROF] *X.509 Certificate and Certificate Revocation List (CRL) Profile for the Shared Service Providers*
885 *(SSP) Program*, Version 1.5, January 2008, or as amended. Available at <http://csrc.nist.gov>. [Note: A
886 change proposal that would add Worksheet 10 has been submitted to the Federal PKI Policy Authority.]
- 887 [SP800-53] NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal*
888 *Information Systems and Organizations*, NIST, April 2013, or as amended. Available at
889 <http://csrc.nist.gov>.
- 890 [SP800-61] NIST Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*,
891 August 2012, or as amended. Available at <http://csrc.nist.gov>.
- 892 [SP800-63] NIST Special Publication 800-63-2, *Electronic Authentication Guideline*, NIST, August
893 2013, or as amended. Available at <http://csrc.nist.gov>.
- 894 [SP800-73] Draft NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, NIST,
895 May 2013, or as amended. Available at <http://csrc.nist.gov>.
- 896 [SP800-78] Draft NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for*
897 *Personal Identity Verification*, NIST, May 2013, or as amended. Available at <http://csrc.nist.gov>.
- 898 [SP800-79] Draft NIST Special Publication 800-79-2, *Guidelines for the Authorization of Personal*
899 *Identity Verification Card Issuers and Derived PIV Credential Issuers*, NIST, or as amended. Soon
900 available at <http://csrc.nist.gov>.
- 901 [SP800-124] NIST Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of*
902 *Mobile Devices in the Enterprise*, NIST, June 2013, or as amended. Available at <http://csrc.nist.gov>.
- 903 [SP800-164] Draft NIST Special Publication 800-164, *Guidelines on Hardware-Rooted Security in*
904 *Mobile Devices*, NIST, October 2012, or as amended. Available at <http://csrc.nist.gov>.