

Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been followed by the document identified below.

Withdrawal Date July 15, 2024

Original Release Date September 27, 2023

The attached draft document is followed by:

Status Final

Series/Number NIST SP 800-73pt3-5

Title Interfaces for Personal Identity Verification: Part 3 – PIV Client
Application Programming Interface

Publication Date July 2024

DOI <https://doi.org/10.6028/NIST.SP.800-73pt3-5>

CSRC URL <https://csrc.nist.gov/pubs/sp/800/73/pt3/5/final>

Additional Information



**NIST Special Publication
NIST SP 800-73pt3-5 ipd**

Interfaces for Personal Identity Verification

Part 3 – PIV Client Application Programming Interface

Initial Public Draft

Hildegard Ferraiolo
Ketan Mehta
Salvatore Francomacaro
Ramaswamy Chandramouli
Sarbari Gupta

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-73pt3-5.ipd>

**NIST Special Publication
NIST SP 800-73pt3-5 ipd**

Interfaces for Personal Identity Verification

Part 3 – PIV Client Application Programming Interface

Initial Public Draft

Hildegard Ferraiolo
Ketan Mehta
Salvatore Francomacaro
Ramaswamy Chandramouli
*Computer Security Division
Information Technology Laboratory*

Sarbari Gupta
Electrosoft Services, Inc.

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-73pt3-5.ipd>

September 2023



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

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

1 Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in
2 this paper in order to specify the experimental procedure adequately. Such identification does not imply
3 recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or
4 equipment identified are necessarily the best available for the purpose.

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

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

14 **Authority**

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

21
22 Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding
23 on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be
24 interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or
25 any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and
26 is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

27 **NIST Technical Series Policies**

28 [Copyright, Use, and Licensing Statements](#)
29 [NIST Technical Series Publication Identifier Syntax](#)

30 **Publication History**

31 Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added on final publishing]
32 Supersedes NIST Series XXX (Month Year) DOI [Will be added on final publishing]

33 **How to Cite this NIST Technical Series Publication:**

34 Ferraiolo H, Mehta K, Francomacaro S, Chandramouli R, Gupta S (2023) Interfaces for Personal Identity
35 Verification: Part 3 – PIV Client Application Programming Interface. (National Institute of Standards and
36 Technology, Gaithersburg, MD), NIST Series (Special Publication) SP 800-73pt3-5 ipd.
37 <https://doi.org/10.6028/NIST.SP.800-73pt3-5.ipd>

38 **Author ORCID iDs**

39 Hildegard Ferraiolo: 0000-0002-7719-5999
40 Ketan Mehta: 0009-0001-1191-8656
41 Salvatore Francomacaro: 0009-0009-0487-2520

NIST SP 800-73pt3-5 ipd (Initial Public Draft)
September 2023

Interfaces for Personal Identity Verification: Part 3
PIV Client API

42 Ramaswamy Chandramouli: 0000-0002-7387-5858
43 Sarbari Gupta: 0000-0003-1101-0856

44 **Public Comment Period**

45 September 27, 2023 – November 15, 2023

46 **Submit Comments**

47 piv_comments@nist.gov

48

49 National Institute of Standards and Technology

50 Attn: Computer Security Division, Information Technology Laboratory

51 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

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

53 **Abstract**

54 FIPS 201 defines the requirements and characteristics of government-wide interoperable identity
55 credentials. It specifies that these identity credentials must be stored on a smart card and that
56 additional common identity credentials, known as derived PIV credentials, may be issued by a
57 federal department or agency and used when a PIV Card is not practical. This document contains
58 the technical specifications to interface with the smart card to retrieve and use the PIV identity
59 credentials. The specifications reflect the design goals of interoperability and PIV Card
60 functions. The goals are addressed by specifying a PIV data model, card edge interface, and
61 application programming interface. Moreover, this document enumerates requirements for the
62 options and branches in international integrated circuit card standards. The specifications go
63 further by constraining interpretations of the normative standards to ease implementation,
64 facilitate interoperability, and ensure performance in a manner tailored for PIV applications.

65 **Keywords**

66 authentication; FIPS 201; identity credential; logical access control; on-card biometric
67 comparison; Personal Identity Verification (PIV); physical access control; smart cards; secure
68 messaging.

69 **Reports on Computer Systems Technology**

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

80 **Trademark Information**

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

82

83 **Call for Patent Claims**

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

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

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

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

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

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

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

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

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

109 **Table of Contents**

110 **1. Introduction 1**

111 1.1. Purpose 1

112 1.2. Scope 1

113 1.3. Audience and Assumptions 1

114 1.4. Content and Organization 2

115 **2. Overview: Concepts and Constructs 3**

116 **3. Client Application Programming Interface 4**

117 3.1. Entry Points for Communication 5

118 3.2. Entry Points for Data Access 7

119 3.3. Entry Points for Cryptographic Operations..... 11

120 3.4. Entry Points for Credential Initialization and Administration..... 12

121 **References..... 15**

122 **Appendix A. List of Symbols, Abbreviations, and Acronyms 17**

123 **Appendix B. Glossary 19**

124 **Appendix C. Notation 20**

125

126 **List of Tables**

127 **Table 1.** Entry points on PIV client application programming interface 4

128 **Table 2.** Data objects in a connection description template (Tag 0x7F21)..... 6

129 **Table 3.** Data objects in an authenticator template (Tag '67') 9

130

131 **Acknowledgments**

132 The authors — Hildegard Ferraiolo, Ketan Mehta, Salvatore Francomacaro, and Ramaswamy
133 Chandramouli of NIST and Sarbari Gupta of Electrosoft Services, Inc. — gratefully
134 acknowledge the contributions of David Cooper, James Dray, William MacGregor, Scott
135 Guthery, Teresa Schwarzhoff, and Jason Mohler, who co-authored prior versions of this three-
136 part publication. The authors also gratefully acknowledge and appreciate the many contributions
137 from the public and private sectors whose thoughtful and constructive comments improved the
138 quality and usefulness of this publication.

139 **1. Introduction**

140 Homeland Security Presidential Directive-12 (HSPD-12) called for the adoption of a common
141 identification standard to govern the interoperable use of identity credentials to allow physical
142 and logical access to federally controlled facilities and information systems. In response, Federal
143 Information Processing Standard (FIPS) 201 [FIPS201], *Personal Identity Verification (PIV) of*
144 *Federal Employees and Contractors*, was developed to define reliable, government-wide identity
145 credentials for use in applications such as access to federally controlled facilities and information
146 systems. FIPS 201 supports multiple types of authenticators, including authenticators on smart
147 cards (also known as PIV Cards) and derived PIV credential authenticators in various other form
148 factors. This publication contains technical specifications to interface with PIV Cards to retrieve
149 and use identity credentials. Other specifications, such as NIST Special Publication (SP) 800-
150 157r1 (Revision 1), contain procedures and life cycle activities to issue, maintain, and use
151 derived PIV credentials.

152 **1.1. Purpose**

153 FIPS 201 defines processes for binding identities to authenticators, such as the PIV Card and
154 derived PIV credentials used in the federal PIV system. SP 800-73-5 contains the technical
155 specifications to interface with the PIV Card to retrieve and use the identity credentials. The
156 specifications reflect the design goals of interoperability and PIV Card functions. The goals are
157 addressed by specifying a PIV data model, card edge interface, and application programming
158 interface. Moreover, this document enumerates requirements for the options and branches in
159 international integrated circuit card (ICC) standards [ISO7816]. The specifications go further by
160 constraining interpretations of the normative standards to ease implementation, facilitate
161 interoperability, and ensure performance in a manner tailored for PIV applications.

162 **1.2. Scope**

163 SP 800-73-5 specifies the PIV data model, application programming interface (API), and card
164 interface requirements necessary to comply with the use cases, as defined in Section 6 of FIPS
165 201 and further described in Appendix B of SP 800-73-5 Part 1. Interoperability is defined as the
166 use of PIV identity credentials such that client-application programs, compliant card
167 applications, and compliant ICCs CAN be used interchangeably by all information processing
168 systems across federal agencies. SP 800-73-5 defines the PIV data elements' identifiers,
169 structure, and format, as well as the client API and card command interface for use with the PIV
170 Card.

171 This document — SP 800-73-5, *Interfaces for Personal Identity Verification: Part 3 – PIV Client*
172 *Application Programming Interface* — contains technical specifications for the PIV client
173 application programming interface to the PIV Card.

174 **1.3. Audience and Assumptions**

175 This document is intended for federal agencies and implementers of PIV systems. Readers are
176 assumed to have a working knowledge of smart card standards and applications.

177 Readers should also be aware of the following important content in SP 800-73-5 Part 1:

- 178 • The front matter details configuration management recommendations and specifies
179 NPIVP conformance testing procedures.
- 180 • Appendix G provides the full Revision History of SP 800-73.
- 181 • Section 1.3 specifies the effective date of SP 800-73-5.

182 **1.4. Content and Organization**

183 All sections in this document are *normative* (i.e., mandatory for compliance) unless specified as
184 *informative* (i.e., non-mandatory) and are structured as follows:

- 185 • Section 1, *Introduction*, provides the purpose, scope, audience and assumptions of the
186 document and outlines its structure.
- 187 • Section 2, *Overview: Concepts and Constructs*, describes both the PIV Card Application
188 and the PIV client API. This section is *informative*.
- 189 • Section 3, *Client Application Programming Interface*, describes the set of entry points
190 accessible by client applications through the PIV Middleware to interact with the PIV
191 Card.
- 192 • Appendix A contains the list of acronyms used in this document. This section is
193 *informative*.
- 194 • Appendix B contains the Glossary of terms used in this document. This section is
195 *informative*.
- 196 • Appendix C explains the notation in use in this document. This section is *informative*.

197 **2. Overview: Concepts and Constructs**

198 SP 800-73-5 Parts 2 and 3 define two interfaces to an ICC that contain the PIV Card Application:
199 a low-level card command interface (SP 800-73-5 Part2) and a high-level client API (Part 3). SP
200 800-73-5 Part 3 (this document) is optional, and NIST Personal Identity Verification Program
201 (NPIVP) conformance testing for PIV Middleware in accordance with SP 800-73 Part 3 is
202 discontinued since endpoints support high level-client API natively at the time of this
203 publication.

204 The information processing concepts and data constructs on both interfaces are identical and
205 MAY be referred to generically as the information processing concepts and data constructs on the
206 *PIV interfaces* without specific reference to the client API or the card command interface.

207 The client API provides task-specific programmatic access to these concepts and constructs, and
208 the card command interface provides communication access. The client API is used by client
209 applications using the PIV Card Application. The card command interface is used by software
210 that implement the client API (middleware).

211 The client API is thought of as being at a higher level than the card command interface because
212 access to a single entry point on the client API may cause multiple card commands to traverse
213 the card command interface. In other words, it may require more than one card command on the
214 card command interface to accomplish the task represented by a single call on an entry point of
215 the client API.

216 The client API is a program execution, call/return style interface, whereas the card command
217 interface is a communication protocol, command/response style interface. Because of this
218 difference, the representation of the PIV concepts and constructs as bits and bytes on the client
219 API may be different from the representation of these same concepts and constructs on the card
220 command interface.

221 **3. Client Application Programming Interface**

222 **Table 1** lists the entry points on the PIV client API. This section references object identifiers
223 (OIDs), which are defined and can be found in SP 800-73-5 Part1, Table 3.

224 **Table 1.** Entry points on PIV client application programming interface

Type	Name
Entry Points for Communication	pivMiddlewareVersion
	pivConnect
	pivDisconnect
Entry Points for Data Access	pivSelectCardApplication
	pivEstablishSecureMessaging
	pivLogIntoCardApplication
	pivGetData
	pivLogoutOfCardApplication
Entry Points for Cryptographic Operations	pivCrypt
Entry Points for Credential Initialization and Administration	pivPutData
	pivGenerateKeyPair

225 If both the PIV Middleware and the PIV Card support secure messaging, then all non-card
226 management functionality¹ of the PIV Card MAY be accessed over either the contact or
227 contactless interface of the card. In order to perform non-card management functionality that
228 would otherwise be limited to the contact interface, the client application must first establish a
229 virtual contact interface by calling the `pivEstablishSecureMessaging` function and using the
230 `pivLogIntoCardApplication` function to submit the pairing code to the card.² If the client
231 application does not have another means of determining whether communication with the PIV
232 Card is over a contact or contactless interface, it MAY use the `pivGetData` function to attempt to
233 read a mandatory data object (e.g., such as the X.509 Certificate for PIV Authentication or the
234 security object) that has an access rule for read of “Always.” However, that is only accessible
235 over the contact and virtual contact interfaces (see SP 800-73-5 Part1, Table 2). If the return code
236 from `pivGetData` is `PIV_SECURITY_CONDITIONS_NOT_SATISFIED`, then the communication with
237 the card is over a contactless interface.

¹ Only the `pivPutData` and `pivGenerateKeyPair` API functions perform card management functionality.

² As noted in Part 1, Section 5.5, the pairing code does not need to be submitted if the Bit 3 of the first byte of the PIN Usage Policy is set to one.

238 3.1. Entry Points for Communication

239 3.1.1. pivMiddlewareVersion

240 **Purpose:** Returns the PIV Middleware version string

241 **Prototype:** `status_word pivMiddlewareVersion(
242 OUT version versionString
243);`

244 **Parameter:** **versionString**

- 245 • For SP 800-73-5 Part 3 conformant PIV Middleware, the parameter
246 returns “800-73-5 Client API” or “800-73-5 Client API with SM.”
- 247 • For SP 800-73-4 Part 3 conformant middleware, the parameter returns
248 “800-73-4 Client API” or “800-73-4 Client API with SM.”
- 249 • Earlier versions with versionString (e.g., “800-73-3 Client API,” “800-
250 73-2 Client API,” and “800-78-1 Client API”) are discontinued as they
251 do not conform to the requirements of FIPS 201-3.

252 **Return Codes:** PIV_OK

253 PIV Middleware that returns a versionString of “800-73-5 Client API with SM” and “800-73-4
254 Client API with SM” SHALL implement all PIV Middleware functions listed in **Table 1** and be
255 able to recognize and process all mandatory and optional PIV data objects. PIV Middleware that
256 returns a versionString of “800-73-5 Client API” and “800-73-4 Client API” SHALL implement
257 all PIV Middleware functions listed in **Table 1** except for pivEstablishSecureMessaging and
258 SHALL be able to recognize and process all mandatory and optional PIV data objects.

259 3.1.2. pivConnect

260 **Purpose:** Connects the client API to the PIV Card Application on a specific ICC.

261 **Prototype:** `status_word pivConnect(
262 IN Boolean sharedConnection,
263 INOUT sequence of bytes connectionDescription,
264 INOUT LONG CDLength,
265 OUT handle cardHandle
266);
267`

268 **Parameters:** **sharedConnection** If TRUE, other client applications CAN establish
269 concurrent connections to the ICC. If FALSE
270 and the connection is established, then the
271 calling client application has exclusive access to
272 the ICC.

273 **connectionDescription** A connection description data object (tag
274 0x7F21). See **Table 2**.

275

276 If the length of the value field of the ‘8x’ data
 277 object in the connection description data object
 278 is zero, then a list of the card readers of the type
 279 indicated by the tag of the ‘8x’ series data
 280 object and available at the ‘9x’ location is
 281 returned in the connectionDescription.
 282
 283 In order to provide sufficient space for the
 284 return value, the client application SHALL
 285 allocate a buffer of at least 2048 bytes for
 connectionDescription.
 286
 287 The connection description BER-TLV
 288 [ISO8825] used on the PIV client API SHALL
 have the structure described in **Table 2**.

Table 2. Data objects in a connection description template (Tag 0x7F21)

Description	Tag	Comment
Interface device – PC/SC	‘81’	Card reader name
Interface device – SCP	‘82’	Card reader identifier on terminal equipment
Interface device – EMR	‘83’	Contactless connection using radio transmission
Interface device – IR	‘84’	Contactless connection using infrared transmission
Interface device – PKCS #11	‘85’	PKCS #11 interface
Interface device – CryptoAPI	‘86’	CryptoAPI interface
Network node – Local	‘90’	No network between client application host and card reader host
Network node – IP	‘91’	IP address of card reader host
Network node – DNS	‘92’	Internet domain name of card reader host
Network node – ISDN	‘93’	ISDN dialing number string of terminal equipment containing the card reader

290 At most one selection from the ‘8x’ series and one selection from the ‘9x’ series SHALL appear
 291 in the connection description template. For example, ‘7F 21 0C 82 04 41 63 6D 65 91 04 C0 00
 292 02 17’ describes a connection to a generic card reader at internet address 192.0.2.23. In another
 293 example, ‘7F 21 0B 82 01 00 93 06 16 17 55 50 12 3F’ describes a connection to the subscriber
 294 identity module in the mobile phone at +1 617 555 0123.

295 When used as an argument to the pivConnect entry point on the PIV client API described in this
 296 section, an ‘8x’ series data object with zero length and a ‘9x’ series data object request the return
 297 of all available card readers of the described type on the described node. Thus, ‘7F 21 04 81 00
 298 90 00’ would request a list of all available PC/SC card readers on the host on which the client
 299 application was running.

300 **CDLength** Length of the card description parameter

301

302 **cardHandle** The returned opaque identifier of a
303 communication channel to a particular ICC and,
304 hence, of the card itself. `cardHandle` is used in all
305 other entry points on the PIV client API to
306 identify which card the functionality of the
307 entry point should be applied to.

308 **Return Codes:** PIV_OK
309 PIV_CONNECTION_DESCRIPTION_MALFORMED
310 PIV_CONNECTION_FAILURE
311 PIV_CONNECTION_LOCKED

312 3.1.3. `pivDisconnect`

313 **Purpose:** Disconnect the PIV API from the PIV Card Application and the ICC that contains
314 the PIV Card Application.

315 **Prototype:** status_word `pivDisconnect` (
316 IN handle **cardHandle**
317);

318 **Parameters:** **cardHandle** Opaque identifier of the card to be acted upon as
319 returned by `pivConnect`. The value of
320 `cardHandle` is undefined upon return from
321 `pivDisconnect`.

322 **Return Codes:** PIV_OK
323 PIV_INVALID_CARD_HANDLE
324 PIV_CARD_READER_ERROR

325 If secure messaging has been established, then the PIV Middleware SHALL zeroize the secure
326 messaging session keys.

327 3.2. Entry Points for Data Access

328 3.2.1.1. `pivSelectCardApplication`

329 **Purpose:** Set the PIV Card Application as the currently selected card application, and
330 establish the PIV Card Application's security state.

331 **Prototype:** status_word `pivSelectCardApplication` (
332 IN handle **cardHandle**,
333 IN sequence of byte **applicationAID**,
334 IN LONG **aidLength**,
335 OUT sequence of byte **applicationProperties**,
336 INOUT LONG **APLength**
337);

338 **Parameters:** `cardHandle` Opaque identifier of the card to be acted upon as
339 returned by `pivConnect`
340 `aidLength` Length of the PIV Card Application AID
341 `applicationAID` The AID of the PIV Card Application that is to
342 become the currently selected card application
343 `applicationProperties` The application properties of the selected PIV Card
344 Application; see SP 800-73-5 Part2, Table 3
345 `APLength` As an input, length of the buffer allocated for
346 applicationProperties; as an output, length of the
347 application properties

348 **Return Codes:** `PIV_OK`
349 `PIV_INVALID_CARD_HANDLE`
350 `PIV_CARD_APPLICATION_NOT_FOUND`
351 `PIV_CARD_READER_ERROR`
352 `PIV_INSUFFICIENT_BUFFER`

353 If the length of application properties is longer than the buffer allocated by the client application,
354 then the PIV Middleware SHALL return `PIV_INSUFFICIENT_BUFFER` but SHALL still set
355 `APLength` to the length of the application properties.

356 3.2.2. `pivEstablishSecureMessaging`

357 **Purpose:** Establish secure messaging with the PIV Card Application.

358 **Prototype:** `status_word pivEstablishSecureMessaging (`
359 `IN handle cardHandle,`
360 `);`

361 **Parameters:** `cardHandle` Opaque identifier of the card to be acted upon as
362 returned by `pivConnect`

363 **Return Codes:** `PIV_OK`
364 `PIV_INVALID_CARD_HANDLE`
365 `PIV_CARD_READER_ERROR`
366 `PIV_SM_FAILED`

367 After successful execution of the key establishment protocol, the PIV Middleware SHALL
368 perform all subsequent GET DATA, VERIFY, and GENERAL AUTHENTICATE commands
369 over secure messaging with the exception of any subsequent uses of the GENERAL
370 AUTHENTICATE command to perform the key establishment protocol.

371 3.2.3. `pivLogIntoCardApplication`

372 **Purpose:** Set the security state within the PIV Card Application.

```

373 Prototype:  status_word pivLogIntoCardApplication (
374             IN handle   cardHandle,
375             IN sequence of byte authenticators,
376             IN LONG     AuthLength
377         );
378 Parameters: cardHandle      Opaque identifier of the card to be acted upon as
379                                     returned by pivConnect
380             authenticators    A sequence of zero or more BER-TLV-encoded
381                                     authenticators to be used to authenticate and set
382                                     the security state/status in the PIV Card
383                                     Application context.
384                                     The authenticator BER-TLV used on the PIV
385                                     client API SHALL have the structure described
386                                     in Table 3.
387             AuthLength        Length of the authenticator template.

```

Table 3. Data objects in an authenticator template (Tag '67')

Description	Tag	M/O	Comment
Reference data	'81'	M	Value of the PIV Card Application PIN, Global PIN, or pairing code, as described in Section 2.4.3 of SP 800-73-5 Part2, or OCC data, as described in Section 5.5.2 of [SP800-76]
Key reference	'83'	M	See Table 4 of SP 800-73-5 Part1 for PIV Card Application PIN, Global PIN, pairing code, and OCC key reference values

```

389 Return Codes:  PIV_OK
390                   PIV_INVALID_CARD_HANDLE
391                   PIV_AUTHENTICATOR_MALFORMED
392                   PIV_AUTHENTICATION_FAILURE
393                   PIV_SECURITY_CONDITIONS_NOT_SATISFIED
394                   PIV_CARD_READER_ERROR
395                   PIV_SM_FAILED

```

396 The PIV Middleware SHALL NOT submit authenticators to the PIV Card over a contactless
397 interface without secure messaging. If secure messaging has not been established, then the
398 pivLogIntoCardApplication function SHALL return
399 PIV_SECURITY_CONDITIONS_NOT_SATISFIED.

400 **3.2.3.1. pivGetData**

401 **Purpose:** Return the entire data content of the named data object.

```

402 Prototype:  status_word pivGetData (

```

```
403         IN handle           cardHandle,  
404         IN string          OID,  
405         IN LONG            oidLength,  
406         OUT sequence of byte data,  
407         INOUT LONG         DataLength  
408     );
```

409 **Parameters:**

410	cardHandle	Opaque identifier of the card to be acted upon as
411		returned by <code>pivConnect</code>
412	OID	Object identifier of the object whose data content is
413		to be retrieved coded as a string (e.g.,
414		“2.16.840.1.101.3.7.2.96.80”). See SP 800-73-5
415		Part1, Table 3.
416	oidLength	Length of the object identifier.
417	data	Retrieved data content.
418	DataLength	As an input, length of the buffer allocated for data.
419		As an output, length of the data retrieved from the
420		PIV Card.

421 **Return Codes:**

```
421     PIV_OK  
422     PIV_INVALID_CARD_HANDLE  
423     PIV_INVALID_OID  
424     PIV_DATA_OBJECT_NOT_FOUND  
425     PIV_SECURITY_CONDITIONS_NOT_SATISFIED  
426     PIV_CARD_READER_ERROR  
427     PIV_SM_FAILED  
428     PIV_INSUFFICIENT_BUFFER
```

429 If the length of the retrieved data is longer than the buffer allocated by the client application, then
430 the PIV Middleware SHALL return `PIV_INSUFFICIENT_BUFFER` but SHALL still set
431 `DataLength` to the length of the retrieved data. If the PIV Card Application returns a zero-length
432 data object, then the PIV Middleware SHALL return `PIV_DATA_OBJECT_NOT_FOUND`.

433 **3.2.4. pivLogoutOfCardApplication**

434 **Purpose:** Reset the application security state/status of the PIV Card Application.

```
435 Prototype: status_word pivLogoutOfCardApplication(  
436     IN handle cardHandle  
437 );
```

438 **Parameters:** `cardHandle` Opaque identifier of the card to be acted upon as
439 returned by `pivConnect`. The `cardHandle` remains
440 valid after execution of this function.

441 **Return Codes:** `PIV_OK`
442 `PIV_INVALID_CARD_HANDLE`
443 `PIV_CARD_READER_ERROR`

444 3.3. Entry Points for Cryptographic Operations

445 3.3.1. `pivCrypt`

446 **Purpose:** Perform a cryptographic operation,³ such as encryption or signing on a sequence
447 of bytes. SP 800-73-5 Part1, Appendix C describes recommended procedures for
448 PIV algorithm identifier discovery.

449 **Prototype:** `status_word pivCrypt(`
450 `IN handle` `cardHandle,`
451 `IN byte` `algorithmIdentifier,`
452 `IN byte` `keyReference,`
453 `IN sequence of byte` `algorithmInput,`
454 `IN LONG` `inputLength,`
455 `OUT sequence of byte` `algorithmOutput,`
456 `INOUT LONG` `outputLength`
457 `);`

458 **Parameters:** `cardHandle` Opaque identifier of the card to be acted upon as
459 returned by `pivConnect`
460 `algorithmIdentifier` Identifier of the cryptographic algorithm to be used
461 for the cryptographic operation [SP800-78, Tables 9
462 and 10]
463 `keyReference` Identifier of the on-card key to be used for the
464 cryptographic operation. See [SP800-78, Table 8]
465 and SP 800-73-5 Part1, Table 5.
466 `algorithmInput` Sequence of bytes used as the input to the
467 cryptographic operation. The `algorithmInput` for
468 RSA algorithms SHALL be restricted to the range 0
469 to $n-1$, where n is the RSA modulus.
470 `inputLength` Length of the algorithm input

³ The `pivCrypt` function does not perform any cryptographic operations itself. It provides the interface to the GENERAL AUTHENTICATE command to perform cryptographic operations on-card. All cryptographic operations are performed outside of the PIV Middleware except for SM on the client side.

506	Parameters:	cardHandle	Opaque identifier of the card to be acted upon as returned by pivConnect
507			
508		OID	Object identifier of the object whose data content is to be replaced coded as a string (e.g., “2.16.840.1.101.3.7.2.96.80”). See SP 800-73-5 Part1, Table 3.
509			
510			
511			
512		oidLength	Length of the object identifier
513		data	Data to be used to replace in its entirety the data content of the named data object
514			
515		dataLength	Length of the provided data
516	Return Codes:	PIV_OK	
517		PIV_INVALID_CARD_HANDLE	PIV_INVALID_OID
518		PIV_CARD_READER_ERROR	PIV_INSUFFICIENT_CARD_RESOURCE
519		PIV_SECURITY_CONDITIONS_NOT_SATISFIED	
520		PIV_FUNCTION_NOT_SUPPORTED	

521 3.4.2. pivGenerateKeyPair

522 **Purpose:** Generates an asymmetric key pair in the currently selected card application.
 523 If the provided key reference exists and the cryptographic mechanism associated
 524 with the reference data identified by this key reference is the same as the provided
 525 cryptographic mechanism, then the generated key pair replaces in entirety the key
 526 pair currently associated with the key reference.

527 **Prototype:** `status_word pivGenerateKeyPair (`
 528 `IN handle cardHandle,`
 529 `IN byte keyReference,`
 530 `IN byte cryptographicMechanism,`
 531 `OUT sequence of byte publicKey,`
 532 `INOUT LONG KeyLength`
 533 `);`

534	Parameters:	cardHandle	Opaque identifier of the card to be acted upon as returned by pivConnect
535			
536		keyReference	The key reference of the generated key pair
537		cryptographicMechanism	The type of key pair to be generated. See SP 800-73-5 Part1, Table 7.
538			
539		publicKey	BER-TLV data objects defining the public key of the generated key pair. See SP 800-73-5 Part2, Table 11.
540			
541			

542 **KeyLength** As an input, the length of the buffer allocated for
543 publicKey; as an output, length of the public key-
544 related data retrieved from the PIV Card

545 **Return Codes:** PIV_OK
546 PIV_INVALID_CARD_HANDLE
547 PIV_SECURITY_CONDITIONS_NOT_SATISFIED
548 PIV_FUNCTION_NOT_SUPPORTED
549 PIV_INVALID_KEY_OR_KEYALG_COMBINATION
550 PIV_UNSUPPORTED_CRYPTOGRAPHIC_MECHANISM
551 PIV_CARD_READER_ERROR
552 PIV_INSUFFICIENT_BUFFER

553 If the length of public key-related data retrieved from the PIV Card is longer than the buffer
554 allocated by the client application, then the PIV Middleware SHALL return
555 PIV_INSUFFICIENT_BUFFER but SHALL still set KeyLength to the length of the public key-
556 related data retrieved from the PIV Card.

557 **References**

- 558 [FIPS201] National Institute of Standards and Technology (2022) Personal Identity
559 Verification (PIV) of Federal Employees and Contractors. (U.S. Department
560 of Commerce, Washington, DC), Federal Information Processing Standards
561 Publication (FIPS) 201-3. <https://doi.org/10.6028/NIST.FIPS.201-3>
- 562 [ISO7816] International Organization for Standardization/International Electrotechnical
563 Commission (2004-2020) ISO/IEC 7816 — Identification cards — Integrated
564 circuit cards (multiple parts):
- 565 ■ International Organization for Standardization/International
566 Electrotechnical Commission (2020) ISO/IEC 7816-4:2020 —
567 Identification cards — Integrated circuit cards — Part 4: Organization,
568 security and commands for interchange. (International Organization for
569 Standardization, Geneva, Switzerland) [or as amended]. Available at
570 <https://www.iso.org/standard/77180.html>
 - 571 ■ International Organization for Standardization/International
572 Electrotechnical Commission (2004) ISO/IEC 7816-5:2004 —
573 Identification cards — Integrated circuit cards — Part 5: Registration of
574 application providers. (International Organization for Standardization,
575 Geneva, Switzerland) [or as amended]. Available at
576 <https://www.iso.org/standard/34259.html>
 - 577 ■ International Organization for Standardization/International
578 Electrotechnical Commission (2016) ISO/IEC 7816-6:2016 —
579 Identification cards — Integrated circuit cards — Part 6: Interindustry data
580 elements for interchange. (International Organization for Standardization,
581 Geneva, Switzerland) [or as amended]. Available at
582 <https://www.iso.org/standard/64598.html>
 - 583 ■ International Organization for Standardization/International
584 Electrotechnical Commission (2016) ISO/IEC 7816-8:2021 —
585 Identification cards — Integrated circuit cards — Part 8: Commands and
586 mechanisms for security operations. (International Organization for
587 Standardization, Geneva, Switzerland) [or as amended]. Available at
588 <https://www.iso.org/standard/79893.html>
 - 589 ■ International Organization for Standardization/International
590 Electrotechnical Commission (2017) ISO/IEC 7816-9:2017 —
591 Identification cards — Integrated circuit cards — Part 9: Commands for
592 card management. (International Organization for Standardization,
593 Geneva, Switzerland) [or as amended]. Available at
594 <https://www.iso.org/standard/67802.html>
- 595 [ISO8825] International Organization for Standardization/International Electrotechnical
596 Commission (2015) ISO/IEC 8825-1:2015— Information technology —
597 ASN.1 encoding rules: Specification of Basic Encoding Rules (BER),
598 Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
599 Part 1. (International Organization for Standardization, Geneva, Switzerland)
600 [or as amended]. Available at <https://www.iso.org/standard/81420.html>

- 601
602 [SP800-76] Grother PJ, Salamon WJ, Chandramouli R (2013) Biometric Specifications for
603 Personal Identity Verification. (National Institute of Standards and Technology,
604 Gaithersburg, MD), NIST Special Publication (SP) 800-76-2 [or as amended].
605 <https://doi.org/10.6028/NIST.SP.800-76-2>
606 [SP800-78] Polk WT, Dodson DF, Burr WE, Ferraiolo H, Cooper DA (2015) Cryptographic
607 Algorithms and Key Sizes for Personal Identity Verification. (National Institute of
608 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-
609 78-4 [or as amended]. <https://doi.org/10.6028/NIST.SP.800-78-4>

610 **Appendix A. List of Symbols, Abbreviations, and Acronyms**

611	AID
612	Application Identifier
613	API
614	Application Programming Interface
615	ASN.1
616	Abstract Syntax Notation One
617	BER
618	Basic Encoding Rules
619	FIPS
620	Federal Information Processing Standard
621	FISMA
622	Federal Information Security Management Act
623	GSC-IS
624	Government Smart Card Interoperability Specification
625	HSPD
626	Homeland Security Presidential Directive
627	ICC
628	Integrated Circuit Card
629	IEC
630	International Electrotechnical Commission
631	INCITS
632	InterNational Committee for Information Technology Standards
633	ISDN
634	Integrated Services Digital Network
635	ISO
636	International Organization for Standardization
637	ITL
638	Information Technology Laboratory
639	LSB
640	Least Significant Bit
641	MSB
642	Most Significant Bit
643	NIST
644	National Institute of Standards and Technology
645	OCC
646	On-Card Biometric Comparison
647	OID
648	Object Identifier

649 **OMB**
650 Office of Management and Budget

651 **PC/SC**
652 Personal Computer/Smart Card

653 **PIN**
654 Personal Identification Number

655 **PIV**
656 Personal Identity Verification

657 **PKCS**
658 Public-Key Cryptography Standards

659 **PKI**
660 Public Key Infrastructure

661 **RFU**
662 Reserved for Future Use

663 **SM**
664 Secure Messaging

665 **SP**
666 Special Publication

667 **TLV**
668 Tag-Length-Value

669 **Appendix B. Glossary**

670 **application identifier**

671 A globally unique identifier of a card application. [[ISO7816](#), Part 4, adapted]

672 **application session**

673 The period of time within a card session between when a card application is selected and a different card application
674 is selected or the card session ends.

675 **Algorithm identifier**

676 A 1-byte identifier that specifies a cryptographic algorithm and key size. For symmetric cryptographic operations,
677 the algorithm identifier also specifies a mode of operation (i.e., ECB).

678 **BER-TLV data object**

679 A data object coded according to [ISO/IEC 8824-2:2021](#).

680 **Card**

681 An integrated circuit card.

682 **Card application**

683 A set of data objects and card commands that can be selected using an application identifier.

684 **Card interface device**

685 An electronic device that connects an integrated circuit card and the card applications therein to a client application.

686 **Card reader**

687 Synonym for *card interface device*.

688 **Client application**

689 A computer program running on a computer in communication with a card interface device.

690 **Card management operation**

691 Any operation involving the PIV Card Application Administrator.

692 **Data object**

693 An item of information seen at the card command interface for which is specified a name, a description of logical
694 content, a format, and a coding.

695 **Interface device**

696 Synonym for *card interface device*.

697 **Key reference**

698 A 1-byte identifier that specifies a cryptographic key according to its PIV Key Type. The identifier is part of
699 cryptographic material used in a cryptographic protocol, such as an authentication or a signing protocol.

700 **Object identifier**

701 A globally unique identifier of a data object. [[ISO8824](#), adapted]

702 **reference data**

703 Cryptographic material used in the performance of a cryptographic protocol, such as an authentication or a signing
704 protocol. The reference data length is the maximum length of a password or PIN. For algorithms, the reference data
705 length is the length of a key.

706 **status word**

707 Two bytes returned by an integrated circuit card after processing any command that encodes the success of or errors
708 encountered during said processing.

709 **template**

710 A (constructed) BER-TLV data object whose value field contains specific BER-TLV data objects.

711 **Appendix C. Notation**

712 The 16 hexadecimal digits SHALL be denoted using the alphanumeric characters 0, 1, 2, ..., 9,
713 A, B, C, D, E, and F. A byte consists of two hexadecimal digits, for example, '2D'. The two
714 hexadecimal digits are represented in quotations '2D' or as 0x2D. A sequence of bytes MAY be
715 enclosed in single quotation marks (e.g., 'A0 00 00 01 16') rather than given as a sequence of
716 individual bytes (e.g., 'A0' '00' '00' '01' '16').

717 A byte can also be represented by bits b8 to b1, where b8 is the most significant bit (MSB) and
718 b1 is the least significant bit (LSB) of the byte. In textual or graphic representations, the leftmost
719 bit is the MSB. Thus, for example, the most significant bit b8 of '80' is 1, and the least significant
720 bit b1 is 0.

721 All bytes specified as RFU SHALL be set to '00', and all bits specified as RFU SHALL be set to
722 0.

723 All lengths SHALL be measured in number of bytes unless otherwise noted.

724 Data objects in templates are described as being mandatory (M), optional (O), or conditional (C).
725 Mandatory means that the data object SHALL appear in the template. Optional means that the
726 data object MAY appear in the template.

727 In other tables the M/O/C column identifies properties of the PIV Card Application that SHALL
728 be present (M), may be present (O), or are conditionally required to be present (C).

729 BER-TLV data object tags are represented as byte sequences, as described above. Thus, for
730 example, 0x4F is the interindustry data object tag for an application identifier, and 0x7F60 is the
731 interindustry data object tag for the Biometric Information Templates Group template.

732 This document uses the following typographical conventions in text:

- 733 • ASN.1 data types are represented in a monospaced font. For example, SignedData and
734 SignerInfo are data types defined for digital signatures.
- 735 • Specific terms in **CAPITALS** represent normative requirements. When these same terms
736 are not in **CAPITALS**, the term does not represent a normative requirement.
- 737 • The terms **SHALL** and **SHALL NOT** indicate requirements to be followed strictly in
738 order to conform to the publication and from which no deviation is permitted.
- 739 • The terms **SHOULD** and **SHOULD NOT** indicate that among several possibilities, one
740 is recommended as particularly suitable without mentioning or excluding others, that a
741 certain course of action is preferred but not necessarily required, or that — in the negative
742 form — a certain possibility or course of action is discouraged but not prohibited.
- 743 • The terms **MAY** and **NEED NOT** indicate a course of action that is permissible within
744 the limits of the publication.
- 745 • The terms **CAN** and **CANNOT** indicate a material, physical, or causal possibility or
746 capability or — in the negative — the absence of that possibility or capability.