1

FIPS PUB 201-2

2

3

4

5 **FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION**

6

7

8

9

Personal Identity Verification (PIV)
10

of
11

Federal Employees and Contractors
12
DRAFT
13

14

15

16

17

18

19 Computer Security Division

20 Information Technology Laboratory

21 National Institute of Standards and Technology

22 Gaithersburg, MD 20899-8900

23

24

25 March 2011

26

27

28

29

30 **U.S. DEPARTMENT OF COMMERCE**

31 *Gary Locke, Secretary*

32

33

34 **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**

35 *Dr. Patrick D. Gallagher, Director*

36

37	**Acknowledgements**
38	
39	NIST would like to acknowledge the significant contributions of the Federal Identity
40	Credentialing Committee (FICC), Identity, Credential, and Access Management Subcommittee
41	(ICAMSC), and the Smart Card Interagency Advisory Board (IAB) for providing valuable
42	contributions to the development of technical frameworks on which this standard is based.
43	Special thanks to those who have participated in the business requirements meeting and provided
44	valuable comments in shaping this standard.

45 **FOREWORD**
46
47 The Federal Information Processing Standards Publication Series of the National Institute of Standards
48 and Technology (NIST) is the official series of publications relating to standards and guidelines adopted
49 and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of
50 2002.

51 Comments concerning FIPS publications are welcomed and should be addressed to the Director,
52 Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive,
53 Stop 8900, Gaithersburg, MD 20899-8900.

54   Cita Furlani, Director
55   Information Technology Laboratory
56
57
58
59
60 **ABSTRACT**
61

62 This standard specifies the architecture and technical requirements for a common identification standard
63 for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for
64 multiple applications by efficiently verifying the claimed identity of individuals seeking physical access
65 to Federally controlled government facilities and electronic access to government information systems.

66 The standard contains the minimum requirements for a Federal personal identity verification system that
67 meets the control and security objectives of Homeland Security Presidential Directive 12, including
68 identity proofing, registration, and issuance. The standard also provides detailed specifications that will
69 support technical interoperability among PIV systems of Federal departments and agencies. It describes
70 the card elements, system interfaces, and security controls required to securely store, process, and retrieve
71 identity credentials from the card. The physical card characteristics, storage media, and data elements
72 that make up identity credentials are specified in this standard. The interfaces and card architecture for
73 storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73,
74 *Interfaces for Personal Identity Verification*. The interfaces and data formats of biometric information
75 are specified in Special Publication 800-76, *Biometric Data Specification for Personal Identity
76 Verification*. The requirements for cryptographic algorithms are specified in the Special Publication 800-
77 78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. The requirements for the
78 accreditation of the PIV Card issuer are specified in the Special Publication 800-79, *Guidelines for the
79 Accreditation of Personal Identity Verification Card Issuers (PCI's)*. The unique organizational codes for
80 Federal agencies are assigned in the Special Publication 800-87, *Codes for the Identification of Federal
81 and Federally-Assisted Organizations*.

82 This standard does not specify access control policies or requirements for Federal departments and
83 agencies.

84

85 *Keywords*: Architecture, authentication, authorization, biometrics, credential, cryptography, Federal
86 Information Processing Standards (FIPS), HSPD-12, identification, identity, infrastructure, model,
87 Personal Identity Verification, PIV, validation, verification.

Federal Information Processing Standards 201
2011

Announcing the
Standard for

Personal Identity Verification
of
Federal Employees and Contractors
DRAFT

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to the Federal Information Security Management Act (FISMA) of 2002.

1. Name of Standard.

FIPS PUB 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors.[1]

2. Category of Standard.

Information Security.

3. Explanation.

Homeland Security Presidential Directive 12 (HSPD-12), dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors," directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. It further specified secure and reliable identification that—

+ Is issued based on sound criteria for verifying an individual employee's identity

+ Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation

+ Can be rapidly authenticated electronically

+ Is issued only by providers whose reliability has been established by an official accreditation process.

The directive stipulated that the standard include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. As promptly as possible, but in no case later than eight months after the date of promulgation, executive departments and agencies are required to implement the standard for identification issued to Federal employees and contractors in gaining physical access to controlled facilities and logical access to controlled information systems.

---

[1] This standard is in response to the Homeland Security Presidential Directive-12 which states that it is "intended only to improve the internal management of the executive branch of the Federal Government".

4. Approving Authority.

Secretary of Commerce.

5. Maintenance Agency.

Department of Commerce, NIST, Information Technology Laboratory (ITL).

6. Applicability.

This standard is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems except for "national security systems" as defined by 44 U.S.C. 3542(b)(2). Except as provided in HSPD-12, nothing in this standard alters the ability of government entities to use the standard for additional applications.

Special-Risk Security Provision—The U.S. Government has personnel, facilities, and other assets deployed and operating worldwide under a vast range of threats (e.g., terrorist, technical, intelligence), particularly heightened overseas. For those agencies with particularly sensitive OCONUS threats, the issuance, holding, and/or use of PIV credentials with full technical capabilities as described herein may result in unacceptably high risk. In such cases of extant risk (e.g., to facilities, individuals, operations, the national interest, or the national security), by the presence and/or use of full-capability PIV credentials, the head of a Department or independent agency may issue a select number of maximum security credentials that do not contain (or otherwise do not fully support) the wireless and/or biometric capabilities otherwise required/referenced herein. To the greatest extent practicable, heads of Departments and independent agencies should minimize the issuance of such special-risk security credentials so as to support inter-agency interoperability and the President's policy. Use of other risk-mitigating technical (e.g., high-assurance on-off switches for the wireless capability) and procedural mechanisms in such situations is preferable, and as such is also explicitly permitted and encouraged. As protective security technology advances, the need for this provision will be re-assessed as the standard undergoes the normal review and update process.

7. Specifications.

Federal Information Processing Standards (FIPS) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors.

8. Implementations.

The PIV standard satisfies the control objectives, security requirements, and technical interoperability requirements of HSPD-12. The PIV standard specifies implementation of identity credentials on integrated circuit cards for use in a Federal personal identity verification system.

A PIV Card must be personalized with identity information for the individual to whom the card is issued, in order to perform identity verification both by humans and automated systems. Humans can use the physical card for visual comparisons, whereas automated systems can use the electronically stored data on the card to conduct automated identity verification.

Federal departments and agencies must use accredited issuers to issue identity credentials for Federal employees and contractors. For this purpose, NIST provided guidelines for the accreditation of PIV Card issuers in [SP 800-79]. NIST also developed a PIV Validation Program that tests implementations for

162 conformance with this standard, and specifically with [SP 800-73]. Additional information on this
163 program is published and maintained at http://csrc.nist.gov/groups/SNS/piv/npivp/.

164 The Office of Management and Budget (OMB) provides an implementation oversight of this standard.
165 The respective numbers of agency-issued 1) general credentials and 2) Special-risk credentials (issued
166 under the Special-Risk Security Provision) are subject to annual reporting to the OMB under the annual
167 reporting process in a manner prescribed by OMB.

168 **9. Effective Date.**

169 This standard is effective immediately. Federal departments and agencies shall meet the requirements of
170 this standard in accordance with the timetable specified by OMB. OMB has advised NIST that it plans to
171 issue guidance regarding the adoption and implementation of this standard.

172 **10. Qualifications.**

173 The security provided by the PIV system is dependent on many factors outside the scope of this standard.
174 Upon adopting this standard, organizations must be aware that the overall security of the personal
175 identification system relies on—

176   **+**   Assurance provided by the issuer of an identity credential that the individual in possession of the
177   credential has been correctly identified

178   **+**   Protection provided to an identity credential stored within the PIV Card and transmitted between
179   the card and the PIV issuance and usage infrastructure

180   **+**   Protection provided to the identity verification system infrastructure and components throughout
181   the entire life cycle.

182 Although it is the intent of this standard to specify mechanisms and support systems that provide high
183 assurance personal identity verification, conformance to this standard does not assure that a particular
184 implementation is secure. It is the implementer's responsibility to ensure that components, interfaces,
185 communications, storage media, managerial processes, and services used within the identity verification
186 system are designed and built in a secure manner.

187 Similarly, the use of a product that conforms to this standard does not guarantee the security of the overall
188 system in which the product is used. The responsible authority in each department and agency shall
189 ensure that an overall system provides the acceptable level of security.

190 Because a standard of this nature must be flexible enough to adapt to advancements and innovations in
191 science and technology, the NIST has a policy to review this standard within five years to assess its
192 adequacy.

193 **11. Waivers.**

194 As per the Federal Information Security Management Act of 2002, waivers to Federal Information
195 Processing Standards are not allowed.

196

197 **12. Where to Obtain Copies.**

198   This publication is available through the Internet by accessing http://csrc.nist.gov/publications/.

13. Patents.

201   Aspects of the implementation of this standard may be covered by U.S. or foreign patents.

Table of Contents

List of Appendices

List of Figures

List of Tables

1. Introduction

Authentication of an individual's identity is a fundamental component of physical and logical access control processes. When an individual attempts to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of an individual's identity is needed to make sound access control decisions.

A wide range of mechanisms is employed to authenticate identity, utilizing various classes of identity credentials. For physical access, individual identity has traditionally been authenticated by use of paper or other non-automated, hand-carried credentials, such as driver's licenses and badges. Access authorization to computers and data has traditionally been based on identities authenticated through user-selected passwords. More recently, cryptographic mechanisms and biometric techniques have been used in physical and logical security applications, replacing or supplementing the traditional identity credentials.

The strength of the authentication that is achieved varies, depending upon the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential. This document establishes a standard for a Personal Identity Verification (PIV) system based on secure and reliable forms of identity credentials issued by the Federal government to its employees and contractors. These credentials are intended to authenticate individuals who require access to Federally controlled facilities, information systems, and applications. This standard addresses requirements for initial identity proofing, infrastructures to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV credentials.

1.1 Purpose

This standard defines a reliable, government-wide identity credential for use in applications such as access to Federally controlled facilities and information systems. This standard has been developed within the context and constraints of Federal law, regulations, and policy based on information processing technology currently available and evolving.

This standard specifies a PIV system within which a common identity credential can be created and later used to verify a claimed identity. The standard also identifies Federal government-wide requirements for security levels that are dependent on risks to the facility or information being protected.

1.2 Scope

Homeland Security Presidential Directive 12 [HSPD-12], signed by the President on August 27, 2004, established the requirements for a common identification standard for identity credentials issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. HSPD-12 directs the Department of Commerce to develop a Federal Information Processing Standards (FIPS) publication to define such a common identity credential. In accordance with HSPD-12, this standard defines the technical requirements for the identity credential that—

+ Is issued based on sound criteria for verifying an individual employee's identity

+ Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation

+ Can be rapidly authenticated electronically

241   **+**   Is issued only by providers whose reliability has been established by an official accreditation
242   process.

243 This standard defines authentication mechanisms offering varying degrees of security. Federal
244 departments and agencies will determine the level of security and authentication mechanisms appropriate
245 for their applications. This standard does not specify access control policies or requirements for Federal
246 departments and agencies. Therefore, the scope of this standard is limited to authentication of an
247 individual's identity. Authorization and access control decisions are outside the scope of this standard.
248 Moreover, requirements for a temporary card used until the new PIV Card arrives are out of scope of this
249 standard.

1.3   Change Management

251 Every new revision of this standard introduces refinements and changes that may impact existing
252 implementations. FIPS 201 and its normative specifications encourage implementation approaches that
253 reduce the high cost of configuration and change management by architecting resilience to change into
254 system processes and components. Nevertheless, changes and modifications are introduced. Because of
255 the importance of this issue, the Change Management section has been added to the standard.

256 This section provides change management principles and guidance to manage newly introduced changes
257 and modifications to the previous version of this standard. Specifically, this section provides a
258 description of the types of changes expected in FIPS 201 revisions.

1.3.1   Backward compatible change

260 A backward compatible change is a change or modification to an existing feature that does not break the
261 systems using this feature. For example, changing the NACI indicator from mandatory to optional in the
262 PIV Authentication certificate does not affect the systems using the PIV Authentication certificate for PIV
263 authentication (i.e., using the PKI-PIV mechanism).

1.3.2   Non-backward compatible change

265 A non-backward compatible change is a change or modification to an existing feature such that the
266 modified feature cannot be used with existing systems. For example, changing the format of the
267 biometric data would not be compatible with the existing system, because a biometric authentication
268 attempt with the modified format would fail. Similarly, changing the PIV Card Application IDentifier
269 (AID) would introduce a non-backward compatible change. As a result, all systems interacting with the
270 PIV card would need to be changed to accept the new PIV AID.

1.3.3   New Features

272 New features are optional or mandatory features that are added to the standard. New features do not
273 interfere with backward compatibility because they are not part of the existing systems. For example, the
274 addition of an optional On-Card Biometric comparison (OCC) authentication mechanism is a new feature
275 that does not affect the features in the current systems. The systems will need to be updated if an agency
276 decides to support the OCC authentication mechanism.

1.3.4   Deprecated and removed

278 When a feature is discontinued or no longer needed, it is deprecated. Such a feature remains in the
279 current standard as an optional feature but its use is strongly discouraged. A deprecated feature does not

280 affect existing systems but should be phased out in future systems, because the feature will be removed in
281 the next revision of the standard. For example, existing PIV Cards with deprecated data elements remain
282 valid until they naturally expire. Replacement PIV Cards, however, should not re-use the deprecated
283 features because the next revision of the standard will remove the support for deprecated data elements.

284 **1.3.5 FIPS 201 Version Management**

285 Subsequent revisions of this standard may necessitate FIPS 201 version management that introduces new
286 version numbers for FIPS 201 products. Components that may be affected by version management
287 include, for example, PIV Cards, PIV middleware software, and card issuance systems.

288 New version numbers may be assigned in [SP 800-73] depending on the nature of the change. For
289 example, new mandatory features introduced in a revision of this standard, may necessitate a new PIV
290 card application version number so that systems can quickly discover the new mandatory features.
291 Optional features, on the other hand, may be discoverable by an on-card discovery mechanism.

292 **1.4 Document Organization**

293 This standard describes the minimum requirements for a Federal personal identification system that meets
294 the control and security objectives of HSPD-12, including identity proofing, registration, and issuance. It
295 provides detailed technical specifications to support the control and security objectives of HSPD-12 as
296 well as interoperability among Federal departments and agencies. This standard describes the policies
297 and minimum requirements of a PIV Card that allows interoperability of credentials for physical and
298 logical access. The physical card characteristics, storage media, and data elements that make up identity
299 credentials are specified in this standard. The interfaces and card architecture for storing and retrieving
300 identity credentials from a smart card are specified in NIST Special Publication 800-73 [SP 800-73],
301 *Interfaces for Personal Identity Verification*. Similarly, the requirements for collection and formatting of
302 biometric information are specified in NIST Special Publication 800-76 [SP 800-76], *Biometric Data*
303 *Specification for Personal Identity Verification*. The requirements for cryptographic algorithms are
304 specified in the Special Publication 800-78 [SP 800-78], *Cryptographic Algorithms and Key Sizes for*
305 *Personal Identity Verification*. The requirements for the accreditation of PIV Card issuers are specified in
306 the Special Publication 800-79 [SP 800-79], *Guidelines for the Accreditation of Personal Identity*
307 *Verification Card Issuers (PCI's)*. The unique organizational codes for Federal agencies are assigned in
308 the Special Publication 800-87 [SP 800-87], *Codes for the Identification of Federal and Federally-*
309 *Assisted Organizations*. The requirements for the PIV Card reader are provided in Special Publication
310 800-96 [SP 800-96], *PIV Card to Reader Interoperability Guidelines*.

311 All sections in this document are *normative* (i.e., mandatory for compliance) unless specified as
312 *informative* (i.e., non-mandatory). Following is the structure of this document:

313   +   Section 1, Introduction, provides background information for understanding the scope of this
314   standard. This section is *informative*.

315   +   Section 2, Common Identification, Security, and Privacy Requirements, outlines the requirements
316   for identity proofing, registration, and issuance, by establishing the control and security
317   objectives for compliance with HSPD-12. This section is *normative*.

318   +   Section 3, PIV System Overview, serves to provide a PIV system overview. This section is
319   *informative*.

320   **+**   Section 4, PIV Front-End Subsystem, provides the requirements for the components of the PIV
321   front-end subsystem. Specifically, this section defines requirements for the PIV Card, logical
322   data elements, biometrics, cryptography, and card readers. This section is *normative*.

323   **+**   Section 5, PIV Key Management Requirements, defines the processes and components required
324   for managing PIV Card life cycle. It also provides the requirements and specifications related to
325   this subsystem. This section is *normative*.

326   **+**   Section 6, PIV Cardholder Authentication, defines a suite of identity authentication mechanisms
327   that are supported by the PIV Card, and their applicability in meeting the requirements of
328   graduated levels of identity assurance. This section is *normative*.

329   **+**   Appendix A, PIV Validation, Certification, and Accreditation, provides additional information
330   regarding compliance with this document. This appendix is *normative*.

331   **+**   Appendix B, Background Check Descriptions, provides the requirements for background checks.
332   This appendix is *informative*.

333   **+**   Appendix C, PIV Card Processes, provides the summary of requirements for PIV card issuance
334   and maintenance processes. This appendix is *informative*.

335   **+**   Appendix D, PIV Object Identifiers and Certificate Extension, provides additional details for the
336   PIV objects identified in Section 4. This appendix is *normative*.

337   **+**   Appendix E, Glossary of Terms, Acronyms, and Notations, describes the vocabulary and textual
338   representations used in the document. This appendix is *informative*.

339   **+**   Appendix F, References, lists the specifications and standards referred to in this document. This
340   appendix is *informative*.

341   **+**   Appendix G, Revision History, lists changes made to this standard from its inception. This
342   appendix is *informative*.

343

344

345 ## 2.   Common Identification, Security, and Privacy Requirements

346 This section addresses the fundamental control and security objectives outlined in HSPD-12, including the
347 identity proofing requirements for Federal employees and contractors.

348 ### 2.1   Control Objectives

349 [HSPD-12] established control objectives for secure and reliable identification of Federal employees and
350 contractors. These control objectives, provided in paragraph 3 of the directive, are quoted here:

351 (3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a)
352 is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to
353 identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated
354 electronically; and (d) is issued only by providers whose reliability has been established by an official
355 accreditation process.

356 Each agency's PIV implementation shall meet the four control objectives (a) through (d) listed above
357 such that—

358 + Credentials are issued 1) to individuals whose true identity has been verified and 2) after a proper
359   authority has authorized issuance of the credential;

360 + A credential is issued only after National Agency Check with Written Inquiries (NACI) or
361   equivalent is initiated and the FBI National Criminal History Check (NCHC) is completed;

362 + An individual is issued a credential only after presenting two identity source documents, at least
363   one of which is a Federal or State government issued picture ID;

364 + Fraudulent identity source documents are not accepted as genuine and unaltered;

365 + A person suspected or known to the government as being a terrorist is not issued a credential;

366 + No substitution occurs in the identity proofing process. More specifically, the individual who
367   appears for identity proofing, and whose fingerprints are checked against databases, is the person
368   to whom the credential is issued;

369 + No credential is issued unless requested by proper authority;

370 + A credential remains serviceable only up to its expiration date. More precisely, a revocation
371   process exists such that expired or invalidated credentials are swiftly revoked;

372 + A single corrupt official in the process may not issue a credential with an incorrect identity or to a
373   person not entitled to the credential;

374 + An issued credential is not modified, duplicated, or forged.

375

376 ## 2.2   Credentialing Requirements

377 Federal departments and agencies shall use the Credentialing guidance as contained in a memorandum
378 dated July 31, 2008, from Linda M. Springer, the Director of the Office of Personnel Management, to
379 Heads of Departments and Agencies when determining whether to issue or revoke PIV Cards.
380 [SPRINGER MEMO]

381 ## 2.3   PIV Identity Proofing and Registration Requirements

382 Departments and agencies shall follow an identity proofing and registration process that meets the
383 requirements defined below when issuing PIV Cards.

384 + The organization shall adopt and use an approved identity proofing and registration process in
385   accordance with [SP 800-79].

386 + The process shall begin with initiation of a NACI or equivalent. This requirement may also be satisfied
387   by locating and referencing a completed and successfully adjudicated NACI. Also, the FBI NCHC
388   (fingerprint check) shall be completed before credential issuance. Appendix B, Background Check
389   Descriptions, provides further details on NACI.

390 + The applicant shall appear in-person at least once before the issuance of a PIV credential.

391 + During identity proofing, the applicant shall be required to provide two forms of identity source
392   documents in original form. The primary identity source document shall be neither expired nor
393   cancelled, shall be one of the following forms of identification:

394 − A U.S. Passport or a U.S. Passport Card;

395 − Permanent Resident Card or Alien Registration Receipt Card (Form I-551)

396 − Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation
397   on a machine-readable immigrant visa

398 − Employment Authorization document that contains a photograph (Form I-766)

399 − In the case of a nonimmigrant alien authorized to work for a specific employer incident to
400   status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the
401   passport and containing an endorsement has not yet expired and the proposed employment is
402   not in conflict with any restrictions or limitations identified on the form

403 − Passport from the Federal States of Micronesia (FSM) or the Republic of the Marshall Islands
404   (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact
405   of Free Association Between the US and the FSM or RMI

406 − A Driver's license or an ID card issued by a state or possession of the United States provided
407   it contains a photograph;

408 − A U.S. Military ID card;

409 − A U.S. Military dependent's ID card; or

410 − A Department of Defense Common Access Card.

411 The secondary identity source document may be from the list above, but cannot be of the same
412 type as the primary identity source document. The secondary identity source document may also
413 be any of the following:

414 − A U.S. Social Security Card issued by the Social Security Administration;

415 − An original or certified copy of a birth certificate issued by a state, county, municipal
416 authority, possession, or outlying possession of the United States bearing an official seal;

417 − An ID card issued by a Federal, state, or local government agency or entity, provided it
418 contains a photograph;

419 − A School ID with photograph;

420 − A Voter's registration card;

421 − A U.S. Coast Guard Merchant Mariner card;

422 − A Certificate of U.S. Citizenship (Form N-560 or N-561);

423 − A Certificate of Naturalization (Form N-550 or N-570);

424 − A U.S. Citizen ID Card (Form I-197);

425 − An ID Card for use of Resident Citizen in the United States (Form I-179);

426 − A Certification of Birth or Certification of Report of Birth issued by the Department of State
427 (Form FS-545 or Form DS-1350);

428 − Unexpired Temporary Resident Card (Form I-688);

429 − Unexpired Employment Authorization Card (Form I-688A);

430 − Unexpired Reentry Permit (Form I-327);

431 − Unexpired Refugee Travel Document (Form I-571);

432 − Unexpired employment authorization document issued by Department of Homeland Security
433 (DHS);

434 − Unexpired Employment Authorization Document issued by DHS with photograph (Form I-
435 688B);

436 − A driver's license issued by a Canadian government entity; or

437 − A Native American tribal document.

438 + The PIV identity proofing, registration, and issuance process shall adhere to the principle of
439 separation of duties to ensure that no single individual has the capability to issue a PIV credential
440 without the cooperation of another authorized person.

441 + A new chain-of-trust record shall be created in accordance with Section 4.4.1 for the applicant.

442 The identity proofing and registration process used when verifying the identity of the applicant shall be
443 accredited by the department or agency as satisfying the requirements above and approved in writing by
444 the head of the Federal department or agency.

445 These identity proofing requirements also apply to citizens of foreign countries who are working for the
446 Federal government overseas. However, a process for registration and approval must be established using
447 a method approved by the U.S. Department of State's Bureau of Diplomatic Security, except for
448 employees under the command of a U.S. area military commander. These procedures may vary
449 depending on the country.

450 ## 2.4 PIV Card Issuance Requirements

451 Departments and agencies shall meet the requirements defined below when issuing identity credentials.
452 The issuance process used when issuing credentials shall be accredited by the department as satisfying the
453 requirements below and approved in writing by the head of the Federal department or agency.

454 + Credentials are issued after a proper authority has authorized issuance of the credential.

455 + The organization shall use an approved PIV credential issuance process in accordance with
456 [SP 800-79].

457 + The process shall ensure the initiation of a NACI or equivalent or the location of a completed and
458 successfully adjudicated NACI or equivalent. The process shall also ensure the FBI NCHC is
459 completed before issuing an identity credential. The PIV credential shall be revoked if the results
460 of the investigation so justify.

461 + Biometrics used to personalize the PIV Card must be taken from the card issuer's chain-of-trust
462 for the applicant.

463 + During the issuance process, the issuer shall verify that the individual to whom the credential is to
464 be issued is the same as the intended applicant/recipient as approved by the appropriate authority.

465 + Before the card is provided to the applicant, the issuer shall perform a 1:1 biometric match of the
466 applicant against the biometric included in the PIV Card. The 1:1 biometric match requires either
467 a match of fingerprint(s) or a match of iris image(s). Minimum accuracy requirements for the
468 biometric match are specified in [SP 800-76]. On successful match, the PIV Card shall be
469 released to the applicant.

470 + The organization shall issue PIV credentials only through systems and providers whose reliability
471 has been established by the agency and so documented and approved in writing (i.e., accredited).

472 + The PIV Card shall be valid for no more than six years.

473 Cards that contain topographical defects (e.g., scratches, poor color, fading, etc), contain errors in
474 optional fields, are not properly printed, or are not delivered to the cardholder are not considered PIV
475 Issued Cards. PIV Card issuer is responsible for the card stock, its management, and its integrity. This
476 standard does not place any requirements on these cards. Agencies may reuse them or discard them, as
477 they deem appropriate.

478 ### 2.4.1 Special Rule for Pseudonyms

479 In limited circumstances Federal employees are permitted to use pseudonyms during the performance of
480 their official duties with the approval of their employing agency. (See, for example, Section 1.2.4 of the
481 Internal Revenue Service Manual, which authorizes approval by an employee's supervisors of the use of a
482 pseudonym to protect the employee's personal safety. Section 1.2.4.6.6 of the Manual provides that

483 employees authorized to use a pseudonym in the course of their official duties will be "given a new ID
484 Card with a new ID number", which will also serve as the employee's building pass.) In instances where
485 an agency has formally authorized the use of a pseudonym, the card issuer shall issue a PIV Card to the
486 employee using the agency-approved employee pseudonym. The issuance of a PIV Card using a
487 pseudonym shall follow the procedures in PIV Card Issuance Requirements for employee name changes
488 except that the employee must provide evidence satisfactory to the card issuer that the pseudonym is
489 authorized by the employee's agency.
490
491 **2.4.2   Grace Period**

492 In some instances an individual's status as a Federal employee or contractor will lapse for a brief time
493 period. In instances where such an interregnum does not exceed 60 days, a card issuer shall issue the
494 employee or contractor a new PIV Card in a manner consistent with PIV Card Issuance.

495 **2.5   PIV Card Maintenance Requirements**

496 The PIV Card shall be maintained using processes that comply with this section.

497 The data and credentials held by the PIV Card may need to be updated or invalidated prior to the
498 expiration date of the card. The cardholder may change his or her name, retire, or change jobs; or the
499 employment may be terminated, thus requiring invalidation of a previously issued card. The PIV system
500 should ensure that this information is distributed effectively within the PIV management infrastructure.
501 Background Investigation status information shall be made available to authenticating parties,
502 government-wide, through the Office of Personnel Management (OPM) Central Verification System,
503 Backend Attribute Exchange, or other operational system approved by OMB. In this regard, procedures
504 for PIV Card maintenance must be integrated into department and agency procedures to ensure effective
505 card maintenance.

506 **2.5.1   PIV Card Renewal Requirements**

507 Renewal is the process by which a valid PIV Card is replaced without the need to repeat the entire
508 identity proofing and registration procedure. The original PIV Card must be surrendered when requesting
509 a renewal. The PIV Card is renewed only after a proper authority has authorized renewal of the
510 credential. The issuer shall verify that the employee remains in good standing and personnel records are
511 current before renewing the card and associated credentials. When renewing identity credentials for
512 current employees, the NACI check shall be followed in accordance with OPM guidance. The issuer
513 shall perform a 1:1 biometric match of the applicant to reconnect to the chain-of-trust. The 1:1 biometric
514 match requires either a match of fingerprint(s) or a match of iris image(s). Minimum accuracy
515 requirements for the biometric match are specified in [SP 800-76]. The entire identity proofing and
516 registration is required if a cardholder's chain-of-trust record is not available.

517 A cardholder shall be allowed to apply for a renewal starting twelve weeks prior to the expiration of a
518 valid PIV Card and until the actual expiration of the card. The cardholder will not be allowed to start the
519 renewal process if the original PIV Card is expired. The original PIV Card must be collected and
520 destroyed. If there is any data change about the cardholder, the issuer will record this in the chain-of-trust
521 and distribute the changed data within the PIV management infrastructure. If the changed data is the
522 cardholder's name, then the issuer shall meet the requirements in Section 2.5.2.1, Special Rule for Name
523 Change by Cardholder.

524 The same biometric data may be reused with the new PIV Card if the expiration date of the new PIV Card
525 is no later than twelve years after the date that the biometric data was obtained. The digital signature
526 must be recomputed with the new FASC-N.

527 The expiration date of the PIV Authentication Key certificate, Card Authentication Key certificate, and
528 optional Digital Signature Key certificate shall not be later than the expiration date of the PIV Card.
529 Hence, a new PIV Authentication Key and certificate and a new asymmetric Card Authentication Key and
530 certificate shall be generated. Key Management key(s) and certificate(s) may be imported to the new PIV
531 Card.

532 ### 2.5.2   PIV Card Reissuance Requirements

533 A cardholder shall apply for reissuance of a new PIV Card if the old PIV Card has been compromised,
534 lost, stolen, or damaged. The cardholder can also apply for reissuance of a valid PIV Card in the event of
535 an employee status or attribute change or if one or more logical credentials have been compromised.

536 In case of reissuance, the complete registration and issuance process is not required if the applicant for
537 reissuance can be reconnected to the chain-of-trust record. Reconnecting to the chain-of-trust requires a
538 1:1 biometric match against the biometric reference data held in a chain-of-trust (see Section 4.4.1). The
539 1:1 biometric match requires either a match of fingerprint(s) or a match of iris image(s). Minimum
540 accuracy requirements for the biometric match are specified in [SP 800-76]. The card issuer shall verify
541 that the employee remains in good standing and personnel records are current before reissuing the card
542 and associated credentials. The entire identity proofing and registration is required if a cardholder's
543 chain-of-trust record is not available.

544 When reissuing a PIV Card, normal operational procedures must be in place to ensure the following:

545   +   The PIV Card itself is revoked. Any local databases that contain FASC-N values must be
546   updated to reflect the change in status.

547   +   The CA shall be informed and the certificates corresponding to the PIV Authentication Key and
548   asymmetric Card Authentication Key on the PIV Card shall be revoked. Revocation of the
549   Digital Signature Key certificate is only optional if the PIV Card has been collected and zeroized
550   or destroyed. Similarly, the Key Management Key certificate should also be revoked if there is
551   risk that the private key was compromised. Certificate revocation lists (CRL) issued shall include
552   the appropriate certificate serial numbers.

553   +   Online Certificate Status Protocol (OCSP) responders shall be updated so that queries with
554   respect to certificates on the PIV Card are answered appropriately. This may be performed
555   indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal
556   revocation records).

557 The PIV Card shall be collected and destroyed if possible. If the card cannot be collected, normal
558 operational procedures shall be completed within 18 hours of notification. In certain cases, 18 hours is an
559 unacceptable delay and in those cases emergency procedures must be executed to disseminate the
560 information as rapidly as possible. Departments and agencies are required to have procedures in place to
561 issue emergency notifications in such cases.

562 If the expiration date of the reissued PIV Card is later than the expiration date of the old card, the card
563 issuer shall ensure a proper authority has authorized reissuance of the credential and the NACI check is
564 followed in accordance with OPM guidance. The same biometric data may be reused with the new PIV

565 Card if the expiration date of the new PIV Card is no later than twelve years after the date that the
566 biometric data was obtained.

567 ### 2.5.2.1   Special Rule for Name Change by Cardholder

568 Name changes are a frequent occurrence. People's names often change as a result of marriage or divorce.
569 Less frequently, people change their names as a matter of personal preference. In the event that a
570 cardholder notifies a card issuer that his or her name has changed, and presents the card issuer with
571 evidence of a formal name change, such as a marriage certificate, a divorce decree, judicial recognition of
572 a name change, or other mechanism permitted by State law or regulation, the card issuer shall issue the
573 cardholder a new card following the procedures set out in Section 2.5.2, PIV Card Reissuance. Also, the
574 card issuer shall update the chain-of-trust record to include the evidence of a formal name change.
575
576 ### 2.5.3   PIV Card Re-Key Requirements

577 There may be instances where keys on the PIV Card or in the PIV System are compromised and the issuer
578 is required to replace the keys on the PIV Card with new ones. The cardholder data and any other related
579 data on the card shall not be changed. Only the keys and certificates shall be updated.

580 ### 2.5.4   PIV Card Post Issuance Update Requirements

581 A PIV Card post issuance update may be performed without replacing the PIV Card in cases where none
582 of the printed information on the surface of the card is changed. The Post Issuance update applies to
583 cases where one or more certificates, keys, biometric data objects, or signed data objects are updated.
584 The PIV Card expiration date or the FASC-N shall not be modified by a Post Issuance update.

585 A PIV Card post issuance update may be done locally (performed with the issuer in physical custody of
586 the PIV Card) or remotely (performed with the PIV Card at a remote location). Post issuance updates
587 shall be performed with issuer security controls equivalent to those applied during PIV Card reissuance.
588 For remote post issuance updates, the following shall apply:

589 + Communication between the PIV Card issuer and the PIV Card shall occur only over mutually
590   authenticated secure sessions between tested and validated cryptographic modules (one being the
591   PIV Card).
592 + Data transmitted between the PIV Card issuer and PIV Card shall be encrypted and contain data
593   integrity checks.
594 + The PIV Card will communicate with no end point entity other than the PIV Card issuer during
595   the remote post issuance update.
596 + If the PIV Card post issuance update begins[2] but fails for any reason, the PIV Card issuer shall
597   immediately terminate the PIV Card as described in Section 2.5.6, and a diligent attempt shall be
598   made to collect and destroy the PIV Card.
599
600 Post issuance updates to biometric data objects, other than to the digital signature blocks within the
601 biometric data objects, shall satisfy the requirements for verification data reset specified in Section 2.5.5.
602

---

[2] A post issuance update has "begun" if the PIV Card Issuer has established the mutually authenticated session to the PIV Card and the PIV Card Issuer has sent any command to the PIV Card that could modify the persistent state of the PIV Card.

2.5.5 PIV Card Verification Data Reset

The PIN on a PIV Card may need to be reset if the cardholder wants to change their PIN, if the cardholder has forgotten the PIN, or if PIN-based cardholder authentication has been disabled from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency. PIN resets may be performed by the card issuer. Before the reset PIV Card is provided back to the cardholder, the card issuer shall ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card.[3] Departments and agencies may adopt more stringent procedures for PIN reset (including requiring in-person appearance or disallowing PIN reset, and requiring the termination of PIV Cards that have been locked); such procedures shall be formally documented by each department and agency.

Verification data other than the PIN may also be reset (i.e., re-enrollment) by the card issuer. Before the reset PIV Card is provided back to the cardholder, the card issuer shall either ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card or the biometric in the cardholder's chain-of-trust (see Section 4.4.1), or require the cardholder to provide a primary identity source document (see Section 2.3). If a biometric match is performed, then the type of biometric used for the match shall not be the same as the type of biometric data that is being reset. Departments and agencies may adopt more stringent procedures for verification data reset (including disallowing verification data reset, and requiring the termination of PIV Cards that have been locked); such procedures shall be formally documented by each department and agency.

2.5.6 PIV Card Termination Requirements

The termination process is used to permanently destroy or invalidate the use of a card, including the data and the keys on it, such that it cannot be used again. The PIV Card shall be terminated under the following circumstances:

+   A Federal employee separates (voluntarily or involuntarily) from Federal service

+   An employee of a Federal contractor separates (voluntarily or involuntarily) from their employer

+   A contractor changes positions and no longer needs access to Federal buildings or systems

+   A cardholder is determined to hold a fraudulent identity

+   A cardholder passes away.

Similar to the situation in which the card or a credential is compromised, normal termination procedures must be in place as to ensure the following:

+   The PIV Card is collected and destroyed.

+   The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status.

+   The CA shall be informed and the certificates corresponding to PIV Authentication Key and the asymmetric Card Authentication Key on the PIV Card must be revoked. Departments and

---

[3] If no biometric data could be collected from the cardholder then the cardholder may instead provide a primary identity source document (see Section 2.3).

638 agencies may revoke certificates corresponding to the optional Digital Signature and Key
639 Management keys. CRLs issued shall include the appropriate certificate serial numbers.

640 + OCSP responders shall be updated so that queries with respect to certificates on the PIV Card are
641 answered appropriately. This may be performed indirectly (by publishing the CRL above) or
642 directly (by updating the OCSP server's internal revocation records).

643 + The IIF collected from the cardholder is disposed of in accordance with the stated privacy and
644 data retention policies of the department or agency.

645 A summary of PIV Card Issuance and PIV Card Maintenance requirements is provided in Appendix C.

646 ## 2.6   PIV Privacy Requirements

647 HSPD-12 explicitly states that "protect[ing] personal privacy" is a requirement of the PIV system. As
648 such, all departments and agencies shall implement the PIV system in accordance with the spirit and letter
649 of all privacy controls specified in this standard, as well as those specified in Federal privacy laws and
650 policies including but not limited to the E-Government Act of 2002 [E-Gov], the Privacy Act of 1974
651 [PRIVACY], and Office of Management and Budget (OMB) Memorandum M-03-22 [OMB322], as
652 applicable.

653 Departments and agencies may have a wide variety of uses of the PIV system and its components that
654 were not intended or anticipated by the President in issuing [HSPD-12]. In considering whether a
655 proposed use of the PIV system is appropriate, departments and agencies shall consider the
656 aforementioned control objectives and the purpose of the PIV standard, namely "to enhance security,
657 increase Government efficiency, reduce identity fraud, and protect personal privacy." [HSPD-12] No
658 department or agency shall implement a use of the identity credential inconsistent with these control
659 objectives.

660 To ensure the privacy throughout PIV life cycle:

661 + Assign an individual to the role of senior agency official for privacy. The senior agency official
662 for privacy is the individual who oversees privacy-related matters in the PIV system and is
663 responsible for implementing the privacy requirements in the standard. The individual serving in
664 this role shall not assume any other operational role in the PIV system.

665 + Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal
666 information in identifiable form for the purpose of implementing PIV, consistent with
667 methodology of [E-Gov] and the requirements of [OMB322]. Consult with appropriate personnel
668 responsible for privacy issues at the department or agency (e.g., Chief Information Officer)
669 implementing the PIV system.

670 + Write, publish, and maintain a clear and comprehensive document listing the types of information
671 that will be collected (e.g., transactional information, personally identifiable information (PII), the
672 purpose of collection, what information may be disclosed to whom during the life of the
673 credential, how the information will be protected, and the complete set of uses of the credential
674 and related information at the department or agency).

675 + PIV applicants shall be provided full disclosure of the intended uses of the PIV credential and the
676 related privacy implications.

677   + Assure that systems that contain PII for the purpose of enabling the implementation of PIV are
678   handled in full compliance with fair information practices as defined in [PRIVACY].

679   + Maintain appeals procedures for those who are denied a credential or whose credentials are
680   revoked.

681   + Ensure that only personnel with a legitimate need for access to PII in the PIV system are
682   authorized to access the PII, including but not limited to information and databases maintained
683   for registration and credential issuance.[4]

684   + Coordinate with appropriate department or agency officials to define consequences for violating
685   privacy policies of the PIV system.

686   + Assure that the technologies used in the department or agency's implementation of the PIV
687   system allow for continuous auditing of compliance with stated privacy policies and practices
688   governing the collection, use, and distribution of information in the operation of the program.

689   + Utilize security controls described in NIST SP 800-53 [SP 800-53], *Recommended Security*
690   *Controls for Federal Information Systems*, to accomplish privacy goals, where applicable.

691   + Ensure that the technologies used to implement PIV sustain and do not erode privacy protections
692   relating to the use, collection, and disclosure of information in identifiable form. Specifically,
693   employ an electromagnetically opaque sleeve or other technology to protect against any
694   unauthorized contactless access to information stored on a PIV Card.

695
696

---

[4] Agencies may refer to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), for a best practice guideline on protection of PII.

697 # 3.   PIV System Overview

698   A notional PIV system architecture is presented in this section. The PIV system is composed of
699   components and processes that support a common (smart card-based) platform for identity authentication
700   across Federal departments and agencies for access to multiple types of physical and logical access
701   environments. The specifications for the PIV components in this standard promote uniformity and
702   interoperability among the various PIV system components, across departments and agencies, and across
703   installations. The specifications for processes in this standard are a set of minimum requirements for the
704   various activities that need to be performed within an operational PIV system. When implemented in
705   accordance with this standard, the PIV Card supports a suite of identity authentication mechanisms that
706   can be used consistently across departments and agencies. The authenticated identity information can
707   then be used as a basis for access control in various Federal physical and logical access environments.
708   The following sections briefly discuss the functional components of the PIV system and the life cycle
709   activities of the PIV Card.

710   ## 3.1   Functional Components

711   An operational PIV system can be logically divided into the following three major subsystems:

712   +   **PIV Front-End Subsystem**—PIV Card, card and biometric readers, and personal identification
713   number (PIN) input device. The PIV cardholder interacts with these components to gain physical
714   or logical access to the desired Federal resource.

715   +   **PIV Card Issuance and Management Subsystem**—the components responsible for identity
716   proofing and registration, card and key issuance and management, and the various repositories
717   and services (e.g., public key infrastructure (PKI) directory, certificate status servers) required as
718   part of the verification infrastructure.

719   +   **PIV Relying Subsystem**—the physical and logical access control systems, the protected
720   resources, and the authorization data.

721   The PIV Relying subsystem becomes relevant when the PIV Card is used to authenticate a cardholder
722   who is seeking access to a physical or logical resource. Although this standard does not provide technical
723   specifications for this subsystem, various mechanisms for identification and authentication are defined in
724   Section 6 to provide consistent and secure means for performing the authentication function preceding an
725   access control decision.

726   Figure 3-1 illustrates a notional model for the operational PIV system, identifying the various system
727   components and the direction of data flow between these components. The boundary shown in the figure
728   is not meant to preclude FIPS 201 requirements on systems outside these boundaries.

729
730
731
732
733
734
735
736
737
738

739
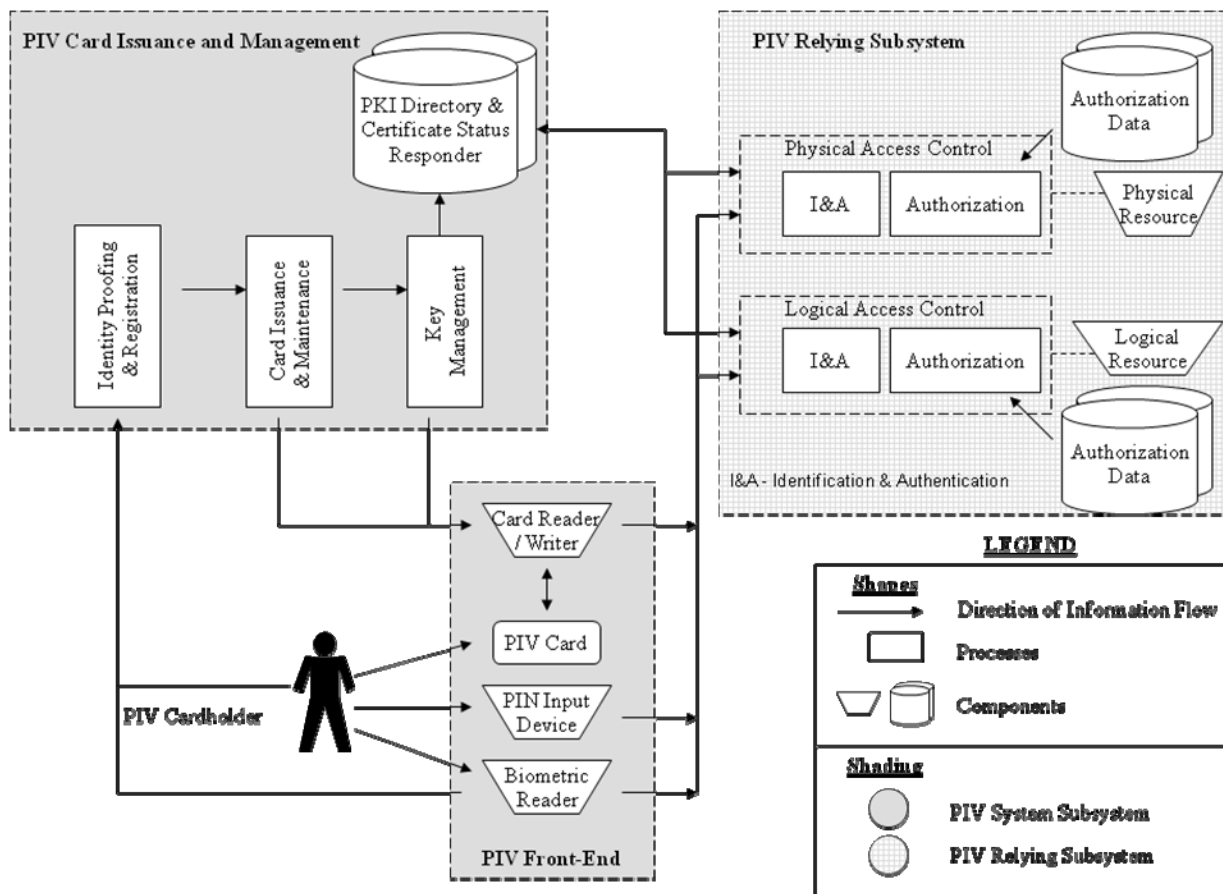
740
741
742 **Figure 3-1. PIV System Notional Model**

743
744 ### 3.1.1   PIV Front-End Subsystem

745 The PIV Card will be issued to the applicant when all identity proofing, registration, and issuance
746 processes have been completed. The PIV Card has a credit card-size form factor, with one or more
747 embedded integrated circuit chips (ICC) that provide memory capacity and computational capability. The
748 PIV Card is the primary component of the PIV system. The holder uses the PIV Card for authentication
749 to various physical and logical resources.

750 Card readers are located at access points for controlled resources where a cardholder may wish to gain
751 access (physical and logical) by using the PIV Card. The reader communicates with the PIV Card to
752 retrieve the appropriate information, located in the card's memory, to relay it to the access control
753 systems for granting or denying access.

754 Card writers that are very similar to the card readers personalize and initialize the information stored on
755 PIV Cards. The data to be stored on PIV Cards includes personal information, certificates, cryptographic
756 keys, the PIN, and biometric data, and is discussed in further detail in subsequent sections.

757 Biometric readers may be located at secure locations where a cardholder may want to gain access. These
758 readers depend upon the use of biometric data of the cardholder, stored in the memory of the card, and its

759   comparison with a real-time biometric sample. The use of biometrics provides an additional factor of
760   authentication ("something you are") in addition to providing the card ("something you have").[5]

761   PIN input devices can also be used along with card readers when a higher level of authentication
762   assurance is required. The cardholder presenting the PIV Card must type in his or her PIN into the PIN
763   input device. For physical access, the PIN is typically entered using a PIN pad device; a keyboard is
764   generally used for logical access. The input of a PIN introduces the use of an additional factor of
765   authentication ("something you know") to control access to information resident on the card ("something
766   you have"). This provides for a higher level of authentication assurance.

767   ### 3.1.2   PIV Card Issuance and Management Subsystem

768   The identity proofing and registration component in Figure 3-1 refers to the process of collecting, storing,
769   and maintaining all information and documentation that is required for verifying and assuring the
770   applicant's identity. Various types of information are collected from the applicant at the time of
771   registration.

772   The card issuance and maintenance component deals with the personalization of the physical (visual
773   surface) and logical (contents of the ICC) aspects of the card at the time of issuance and maintenance
774   thereafter. This includes printing photographs, names, and other information on the card and loading the
775   relevant card applications, biometrics, and other data.

776   The key management component is responsible for the generation of key pairs, the issuance and
777   distribution of digital certificates containing the public keys of the cardholder, and management and
778   dissemination of certificate status information. The key management component is used throughout the
779   life cycle of PIV Cards—from generation and loading of authentication keys and PKI credentials, to
780   usage of these keys for secure operations, to eventual renewal, reissuance, or termination of the card. The
781   key management component is also responsible for the provisioning of publicly accessible repositories
782   and services (such as PKI directories and certificate status responders) that provide information to the
783   requesting application about the status of the PKI credentials.

784   ### 3.1.3   PIV Relying Subsystem

785   The PIV Relying subsystem includes components responsible for determining a particular PIV
786   cardholder's access to a physical or logical resource. A physical resource is the secured facility (e.g.,
787   building, room, parking garage) that the cardholder wishes to access. The logical resource is typically a
788   network or a location on the network (e.g., computer workstation, folder, file, database record, software
789   program) to which the cardholder wants to gain access.

790   The authorization data component comprises information that defines the privileges (authorizations)
791   possessed by entities requesting to access a particular logical or physical resource. An example of this is
792   an access control list (ACL) associated with a file on a computer system.

793   The physical and logical access control system grants or denies access to a particular resource and
794   includes an identification and authentication (I&A) component as well as an authorization component.
795   The I&A component interacts with the PIV Card and uses mechanisms discussed in Section 6 to identify
796   and authenticate cardholders. Once authenticated, the authorization component interacts with the
797   authorization data component to match the cardholder-provided information to the information on record.

---

[5] For more information on the terms "something you know," "something you have," and "something you are," see [SP800-63].

798 The access control components typically interface with the card reader, the authorization component, the
799 PIN input device, the biometric reader, and any certificate status service (if available).

800 **3.2   PIV Card Life Cycle Activities**

801 The PIV Card life cycle consists of seven activities. The activities that take place during fabrication and
802 pre-personalization of the card at the manufacturer are not considered a part of this life cycle model.
803 Figure 3-2 presents these PIV activities and depicts the PIV Card request as the initial activity and PIV
804 Card termination as the end of life.
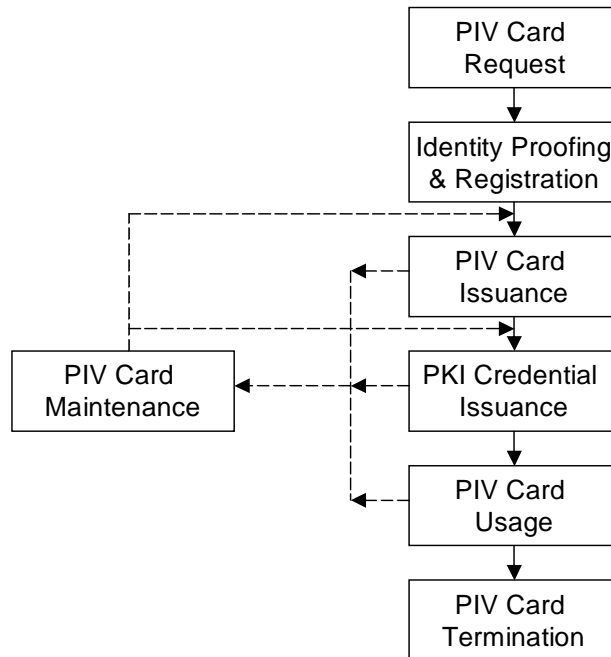
805

806
807   **Figure 3-2. PIV Card Life Cycle Activities**

808 Descriptions of the seven card life cycle activities are as follows:

809   +   **PIV Card Request.** This activity applies to the initiation of a request for the issuance of a PIV
810   Card to an applicant and the validation of this request.

811   +   **Identity Proofing and Registration.** The goal of this activity is to verify the claimed identity of
812   the applicant and that the entire set of identity source documents presented at the time of
813   registration is valid.

814   +   **PIV Card Issuance.** This activity deals with the personalization (physical and logical) of the
815   card and the issuance of the card to the intended applicant.

816   +   **PKI Credential Issuance.** This activity deals with generating logical credentials and loading
817   them onto the PIV Card.

818   +   **PIV Card Usage.** During this activity, the PIV Card is used to perform cardholder authentication
819   for access to a physical or logical resource. Access authorization decisions are made after
820   successful cardholder identification and authentication.

821   +   **PIV Card Maintenance.** This activity deals with the maintenance or update of the physical card
822   and the data stored thereon. Such data includes various card applications, PIN, PKI credentials,
823   and biometrics.

824   +   **PIV Card Termination.** The termination process is used to permanently destroy or invalidate
825   the PIV Card and the data and keys needed for authentication so as to prevent any future use of
826   the card for authentication.

4.   PIV Front-End Subsystem

828 This section identifies the requirements for the components of the PIV front-end subsystem. Section 4.1
829 provides the physical and logical card specifications. The logical PIV Cardholder Unique Identifier
830 (CHUID) object is described in Section 4.2. Cryptographic keys associated with the cardholder are
831 described in Section 4.3. Formats for mandatory biometric information are defined in Section 4.4.
832 Section 4.5 discusses card readers.

4.1   Physical PIV Card Characteristics

834 References to the PIV Card in this section and Sections 4.1.1 through 4.1.5 pertain to the physical
835 characteristics only. References to the front of the card apply to the side of the card that contains the
836 electronic contacts; references to the back of the card apply to the opposite side from the front side.

837 The PIV Card's physical appearance and other characteristics should balance the need to have the PIV
838 Card commonly recognized as a Federal identification card while providing the flexibility to support
839 individual department and agency requirements. Having a common look for PIV Cards is important in
840 meeting the objectives of improved security and interoperability. In support of these objectives,
841 consistent placement of printed components and technology is generally necessary.

842 The PIV Card shall comply with physical characteristics as described in International Organization for
843 Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 [ISO7810], ISO/IEC 10373
844 [ISO10373], ISO/IEC 7816 for contact cards [ISO7816], and ISO/IEC 14443 for contactless cards
845 [ISO14443].

4.1.1   Printed Material

847 The printed material shall not rub off during the life of the PIV Card, nor shall the printing process
848 deposit debris on the printer rollers during printing and laminating. Printed material shall not interfere
849 with the contact and contactless ICC(s) and related components, nor shall it obstruct access to machine-
850 readable information.

4.1.2   Tamper Proofing and Resistance

852 The PIV Card shall contain security features that aid in reducing counterfeiting, are resistant to tampering,
853 and provide visual evidence of tampering attempts. At a minimum, a PIV Card shall incorporate one such
854 security feature. Examples of these security features include the following:

855 + Optical varying structures

856 + Optical varying inks

857 + Laser etching and engraving

858 + Holograms

859 + Holographic images

860 + Watermarks.

861 Incorporation of security features shall—

862   **+**   Be in accordance with durability requirements [ISO7810]

863   **+**   Be free of defects, such as fading and discoloration

864   **+**   Not obscure printed information

865   **+**   Not impede access to machine-readable information.

866 Departments and agencies may incorporate additional tamper-resistance and anti-counterfeiting methods.
867 As a generally accepted security procedure, Federal departments and agencies are strongly encouraged to
868 periodically review the viability, effectiveness, and currency of employed tamper resistance and anti-
869 counterfeiting methods.

870 **4.1.3   Physical Characteristics and Durability**

871 The following list describes the physical requirements for the PIV Card.

872   **+**   The PIV Card shall contain a contact and a contactless ICC interface.

873   **+**   The card body shall be white in accordance with color representation in Section 4.1.5. Only a
874   security feature, as in Section 4.1.2, may modify the perceived color slightly. Presence of a
875   security feature shall not prevent the recognition of white as the principal card body color by a
876   person with normal vision (corrected or uncorrected) at a working distance of 50 cm to 200 cm.

877   **+**   The card body structure shall consist of card material(s) that satisfy the card characteristics in
878   [ISO7810] and test methods in American National Standards Institute (ANSI) 322. [ANSI322]
879   Although the [ANSI322] test methods do not currently specify compliance requirements, the tests
880   shall be used to evaluate card material durability and performance. The [ANSI322] tests
881   minimally shall include card flexure, static stress, plasticizer exposure, impact resistance, card
882   structural integrity, surface abrasion, temperature and humidity-induced dye migration, ultraviolet
883   light exposure, and a laundry test. Cards shall not malfunction or delaminate after hand cleaning
884   with a mild soap and water mixture. The reagents called out in Section 5.4.1.1 of [ISO10373]
885   shall be modified to include a two percent soap solution.

886   **+**   The card shall be subjected to actual, concentrated, or artificial sunlight to appropriately reflect
887   2000 hours of southwestern United States' sunlight exposure in accordance with [ISO10373],
888   Section 5.12. Concentrated sunlight exposure shall be performed in accordance with [G90-98]
889   and accelerated exposure in accordance with [G155-00]. After exposure, the card shall be
890   subjected to the [ISO10373] dynamic bending test and shall have no visible cracks or failures.
891   Alternatively, the card may be subjected to the [ANSI322] tests for ultraviolet and daylight fading
892   resistance and subjected to the same [ISO10373] dynamic bending test.

893   **+**   Departments and agencies shall ensure that the card meets the requirements of Section 508 of the
894   Rehabilitation Act. There are methods by which proper card orientation can be correctly detected
895   by touch. One method is adherence of a raised surface (for example, an adhesive Braille letter).
896   Section 4.1.4.3 defines Zone 21F, where raised surface may be placed.

897   **+**   The card shall be 27- to 33-mil thick (before lamination) in accordance with [ISO7810].

898   **+**   The PIV Card shall not be embossed.

899
900
+ Decals shall not be adhered to the card except as described in support of the Section 508 requirement.

901
902
903
904
905
+ Departments and agencies may choose to punch an opening in the card body to enable the card to be oriented by touch or to be worn on a lanyard. Departments and agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity and printing process is not adversely impacted. Departments and agencies are strongly encouraged to ensure such alterations do not—

906
– Compromise card body durability requirements and characteristics

907
– Invalidate card manufacturer warranties or other product claims

908
– Alter or interfere with printed information, including the photo

909
– Damage or interfere with machine-readable technology, such as the embedded antenna.

910
911
912
913
914
+ The card material shall withstand the effects of temperatures required by the application of a polyester laminate on one or both sides of the card by commercial off-the-shelf (COTS) equipment. The thickness added due to a laminate layer shall not interfere with the smart card reader operation. The card material shall allow production of a flat card in accordance with [ISO7810] after lamination of one or both sides of the card.

915
The PIV Card may be subjected to additional testing.

916
4.1.4 Visual Card Topography

917
918
919
920
The information on a PIV Card shall be in visual printed and electronic form. This section covers the placement of visual and printed information. It does not cover information stored in electronic form, such as stored data elements, and other possible machine-readable technologies. Logically stored data elements are discussed in Section 4.1.6.

921
922
923
As noted in Section 4.1.3, the PIV Card shall contain a contact and a contactless ICC interface. This standard does not specify whether a single chip is used or multiple chips are used to support the mandated contact and contactless interfaces.

924
925
926
927
928
To achieve a common PIV Card appearance, yet provide departments and agencies the flexibility to augment the card with department or agency-specific requirements, the card shall contain mandated and optional printed information and mandated and optional machine-readable technologies. Mandated and optional items shall generally be placed as described and depicted. Printed data shall not interfere with machine-readable technology.

929
930
931
932
933
934
Areas that are marked as reserved should not be used for printing. The reason for the recommended reserved areas is that placement of the embedded contactless ICC module may vary from manufacturer to manufacturer, and there are constraints that prohibit printing over the embedded contactless module. The PIV Card topography provides flexibility for placement of the embedded module, either in the upper right-hand corner or in the lower bottom portion. Printing restrictions apply only to the area where the embedded module is located (i.e., upper right-hand corner, lower bottom portion).

935
936
Because technological developments may obviate the need to have a restricted area, or change the size of the restricted area, departments and agencies are encouraged to work closely with card vendors and

937 manufacturers to ensure current printing procedures and methods are applied as well as potential
938 integration of features that may improve tamper resistance and anti-counterfeiting of the PIV Card.

939 **4.1.4.1 Mandatory Items on the Front of the PIV Card**
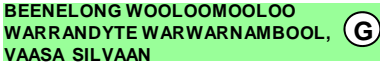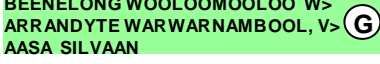
940 *Zone 1F—Photograph.* The photograph shall be placed in the upper left corner, as depicted in Figure 4-1,
941 and be a full frontal pose from top of the head to shoulder. A minimum of 300 dots per inch (dpi)
942 resolution shall be used. The background should follow recommendations set forth in SP 800-76.

943 *Zone 2F—Name.* The full name[6] shall be printed directly under the photograph in capital letters. The full
944 name shall be composed of a Primary Identifier (i.e., surnames or family names) and a Secondary
945 Identifier (i.e., pre-names or given names). The full name shall be printed in the <Primary Identifier>,
946 <Secondary Identifier> format. The entire full name should be printed on available lines of Zone 2F and
947 either identifier could be wrapped. The wrapped identifier shall be indicated with ">" character at the end
948 of the line. The identifiers may be confined to their lines if each fits on one line. Table 4-1 provides
949 examples of separate Primary and Secondary Identifier lines, single line with identifiers, wrapped full
950 names, and full name in three lines. Note that the truncation should only occur if the full name cannot be
951 printed in 7 point font.

952 **Table 4-1. Name Examples**

Name: Anna Maria Eriksson Characteristics: simple full name, two lines sufficient with 10 points.	**ERIKSSON,** **ANNA MARIA** Ⓖ
Name: Anna Maria Eriksson Characteristics: simple full name, one line sufficient for full name with 10 points.	**ERIKSSON, ANNA MARIA** Ⓖ
Name: Susie Margaret Smith-Jones Characteristics: longer full name in two lines, sufficient space in 10 points.	**SMITH-JONES,** **SUSIE MARGARET** Ⓖ
Name: Susie Margaret Smith-Jones Characteristics: longer full name wrapped, two lines sufficient with 10 points.	**SMITH-JONES, SUSIE MA>**Ⓖ **RGARET**
Name: Chayapa Dejthamrong Krusuang Nilavadhanananda Characteristics: longer full name wrapped, two lines NOT sufficient with 10 points. Reduce the font size to 8 points.	**NILAVADHANANANDA, CHAYA>** Ⓖ **PA DEJTHAMRONG KRUSUANG**

---

[6] Alternatively, pseudonyms as provided under the law as discussed in Section 2.6.4.

Name: Vaasa Silvaan Bennelong Wooloomooloo Warrandyte Warnambool Characteristics: longer full name, two lines NOT sufficient with 8 point, 7 point allows sufficient space for three lines in Zone 2F.	BEENELONG WOOLOOMOOLOO WARRANDYTE WARWARNAMBOOL, (G) VAASA SILVAAN
Name: Vaasa Silvaan Bennelong Wooloomooloo Warrandyte Warnambool Characteristics: same as previous but full name is wrapped.	BEENELONG WOOLOOMOOLOO W> ARRANDYTE WARWARNAMBOOL, V> (G) AASA SILVAAN

953

954 Names in the Primary Identifier and the first name in the Secondary Identifier shall not be abbreviated.
955 Other names and conventional prefixes and suffixes may be abbreviated. The special character "."
956 (period) shall indicate such abbreviations, as shown in Figure 4-2. Other uses of special symbols (e.g.,
957 "O'BRIEN") are at the discretion of the issuer.

958 Departments and agencies shall use the largest font size of 8 to 10 points that allows the full name to be
959 printed. The font size 7 point allows space for 3 lines and shall only be used if the full name is greater
960 than 45 characters.

961 *Zone 8F—Employee Affiliation.* An employee affiliation shall be printed on the card. Some examples of
962 employee affiliation are "Employee", "Contractor," "Active Duty," and "Civilian."

963 *Zone 10F—Agency, Department, or Organization.* The Organizational Affiliation shall be printed as
964 depicted in Figure 4-1.

965 *Zone 14F—Expiration Date.* The card expiration date shall be printed in a YYYYMMMDD format.

966 **4.1.4.2 Mandatory Items on the Back of the Card**

967 *Zone 1B—Agency Card Serial Number.* This item shall be printed as depicted in Figure 4-6 and contain
968 the unique serial number from the issuing department or agency. The format shall be at the discretion of
969 the issuing department or agency.

970 *Zone 2B—Issuer Identification Number.* This item shall be printed as depicted in Figure 4-6 and consist
971 of six characters for the department code and four characters for the agency code that uniquely identifies
972 the department or agency.

973 **4.1.4.3 Optional Items on the Front of the Card**

974 This section contains a description of the optional information and machine-readable technologies that
975 may be used and their respective placement. The storage capacity of all optional technologies is as
976 prescribed by individual departments and agencies and is not addressed in this standard. Although the
977 items discussed in this section are optional, if used they shall be placed on the card as designated in the
978 examples provided and as noted.

979 *Zone 3F—Signature.* If used, the department or agency shall place the cardholder signature below the
980 photograph and cardholder name as depicted in Figure 4-3. The space for the signature shall not interfere
981 with the contact and contactless placement. Because of card surface space constraints, placement of a
982 signature may limit the size of the optional two-dimensional bar code.

983 *Zone 4F—Agency Specific Text Area.* If used, this area can be used for printing agency specific
984 requirements, such as employee status.

985 *Zone 5F—Rank.* If used, the cardholder's rank shall be printed in the area as illustrated. Data format is at
986 the department or agency's discretion.

987 *Zone 6F—Portable Data File (PDF) Two-Dimensional Bar Code.* If used, the PDF bar code placement
988 shall be as depicted in Figure 4-2 (i.e., left side of the card). If Zone 3F (a cardholder signature) is used,
989 the size of the PDF bar code may be affected. The card issuer should confirm that a PDF used in
990 conjunction with a PIV Card containing a cardholder signature will satisfy the anticipated PDF data
991 storage requirements.

992 *Zone 9F— Header.* If used, the text *"United States Government"* shall be placed as depicted in Figure 4-
993 1. Departments and agencies may also choose to use this zone for other department or agency-specific
994 information, such as identifying a Federal emergency responder role, as depicted in Figure 4-2.

995 *Zone 11F—Agency Seal.* If used, the seal selected by the issuing department, agency, or organization
996 shall be printed in the area depicted. It shall be printed using the guidelines provided in Figure 4-2 to
997 ensure information printed on the seal is legible and clearly visible.

998 *Zone 12F—Footer.* The footer is the preferred location for the *Emergency Response Official*
999 *Identification* label. If used, a department or agency may print "Emergency Response Official" as
1000 depicted in Figure 4-2, preferably in white lettering on a red background. Departments and agencies may
1001 also use Zone 9F to further identify the Federal emergency respondent's official role. Some examples of
1002 official roles are "Law Enforcement", "Fire Fighter", and "Emergency Response Team (ERT)".

1003 *Zone 13F—Issue Date.* If used, the card issuance date shall be printed above the expiration date in
1004 YYYYMMMDD format as depicted in Figure 4-2.

1005 *Zone 15F—Color-Coding for Employee Affiliation.* Color-coding may be used for additional
1006 identification of employee affiliation (see Section 4.1.5 for Color Representation). If color-coding is
1007 used, it shall be used as a background color for Zone 2F (name) as depicted in Figure 4-4. The following
1008 color scheme shall be used for the noted categories:

1009   **+**   Blue—foreign nationals

1010   **+**   Red—emergency response officials

1011   **+**   Green—contractors.

1012 These colors shall be reserved and shall not be employed for other purposes. Also, these colors shall be
1013 printed in accordance to the color specifications provided in Section 4.1.5. Zone 15F may be a solid or
1014 patterned line at the department or agency's discretion.

1015 *Zone 16F—Photo Border for Employee Affiliation.* A border may be used with the photo to further
1016 identify employee affiliation, as depicted in Figure 4-3. This border may be used in conjunction with

1017   Zone 15F to enable departments and agencies to develop various employee categories. The photo border
1018   shall not obscure the photo. The border may be a solid or patterned line. For solid and patterned lines, red
1019   shall be reserved for emergency response officials, blue for foreign nationals, and green for contractors.
1020   All other colors may be used at the department or agency's discretion.

1021   *Zone 17F—Agency Specific Data.* In cases in which other defined optional elements are not used, Zone
1022   17F may be used for other department or agency-specific information, as depicted in Figure 4-5.

1023   *Zone 18F—Affiliation Color Code.* The affiliation color code "B" for Blue, "G" for Green, or "R" for
1024   Red shall be printed in a white circle in Zone 15F. The diameter of the circle shall not be more than 5
1025   mm. Note that the lettering shall correspond to the printed color in Zone 15F. If Zone 16F photo border
1026   coloring is used to identify employee affiliation of emergency response officials, foreign nationals, or
1027   contractors, the lettering shall correspond to the printed color.

1028   *Zone 19F—Expiration Date.* If used, the card expiration date shall be printed in a MMMYYYY format in
1029   the upper right hand corner. The Zone 19F expiration date shall be printed in Arial 12pt Bold.

1030   *Zone 20F—Organizational Affiliation Abbreviation.* The organizational affiliation abbreviation may be
1031   printed in the upper right hand corner below the Zone 19F expiration date as shown in Figure 4-1. If
1032   printed, the organizational affiliation abbreviation shall be printed in Arial 12pt Bold.

1033   *Zone 21F—Section 508 Compliance*. A raised surface may be created so a card orientation can be
1034   determined by touch. The thickness of the PIV Card after the raised surface is applied shall not exceed 54
1035   mil. See Figure 4-2 for the placement of the raised surface.

1036   **4.1.4.4   Optional Items on the Back of the Card**

1037   *Zone 3B—Magnetic Stripe.* If used, the magnetic stripe shall be high coercivity and placed in accordance
1038   with [ISO7811], as illustrated in Figure 4-7.

1039   *Zone 4B—Return Address.* If used, the "return if lost" language shall be generally placed on the back of
1040   the card as depicted in Figure 4-7.

1041   *Zone 5B—Physical Characteristics of Cardholder.* If used, the cardholder physical characteristics (e.g.,
1042   height, eye color, hair color) shall be printed in the general area illustrated in Figure 4-7. Additional
1043   information such as Gender and Date of Birth required for Transportation Security Administration (TSA)
1044   checkpoint may also be printed as shown in Figure 4-7.

1045   *Zone 6B—Additional Language for Emergency Response Officials.* Departments and agencies may
1046   choose to provide additional information to identify emergency response officials or to better identify the
1047   cardholder's authorized access. If used, this additional text shall be in the general area depicted and shall
1048   not interfere with other printed text or machine-readable components. An example of a printed statement
1049   is provided in Figure 4-7.

1050   *Zone 7B—Standard Section 499, Title 18 Language*. If used, standard Section 499, Title 18, language
1051   warning against counterfeiting, altering, or misusing the card shall be printed in the general area depicted
1052   in Figure 4-7.

1053   *Zone 8B—Linear 3 of 9 Bar Code*. If used, a linear 3 of 9 bar code shall be generally placed as depicted
1054   in Figure 4-7. It shall be in accordance with Association for Automatic Identification and Mobility (AIM)
1055   standards. Beginning and end points of the bar code will be dependent on the embedded contactless

PERSONAL IDENTITY VERIFICATION (PIV) OF FEDERAL EMPLOYEES AND CONTRACTORS

1056   module selected. Departments and agencies are encouraged to coordinate placement of the bar code with
1057   the card vendor.

1058   *Zone 9B—Agency-Specific Text.* In cases in which other defined optional elements are not used, Zone 9B
1059   may be used for other department or agency-specific information, as depicted in Figure 4-8. For example,
1060   emergency response officials may use this area to provide additional details.

1061   *Zone 10B—Agency-Specific Text.* Zone 10B is similar to Zone 9B in that it is another area for providing
1062   department or agency-specific information.

1063   For Zones 9B and 10B, departments and agencies are encouraged to use this area prudently and minimize
1064   printed text to that which is absolutely necessary.

1065   In the case of the Department of Defense, the back of the card will have a distinct appearance. This is
1066   necessary to display information required by the Geneva Accord and to facilitate legislatively mandated
1067   medical entitlements.

DRAFT   27

1068

Zone 9F – Header (Optional)

2.5   30.25   51.5
       30.75

2.5

4.5   [United States Government]   MMMYYYY   4.5
                                                8

Zone 1F - Photograph
Recommended dimensions:
37.0 x 27.75 (.75 aspect)

**Zone 19F –
Expiration Date**
Arial 12pt Bold
Format: MMMYYYY

Color
Photograph

AGENCY   14.5
          18

**Zone 20F –
Organizational
Affiliation
Abbreviation**
Arial 12pt Bold

20

Affiliation
[Affiliation 6pt Bold]   **Zone 8F – Employee
                           affiliation**

Agency/Department
[Agency 6pt Bold]   **Zone 10F –
[Optional 2ⁿᵈ line]   Agency,
                       Department, or
                       Organization**

Expires
[YYYYMMMDD]   **Zone 14F –
               Expiration date**
               Format YYYYMMMDD

41.5   [LAST NAME,]
        [FIRST NAME]

Zone 2F – Name
Arial 7-10pt Bold, use
largest font size possible

50

57.5

Contact
Chip   65.5

**Zone 7F – Circuit
chip**
ISO 7816 compliant. No
printing allowed.

Area for additional optional data. Agency-specific data may be printed in this area. See other examples for required placement of additional optional data elements.

Area likely to be needed by card manufacturer. Optional data may be printed in this area but may be subject to restrictions imposed by card and/or printer manufacturers.

1069

1070   **Figure 4-1. Card Front—Printable Areas**

1071
1072

Zone 9F - Header
Example of emergency responder title.

30.75

Zone 21F – Section 508 Compliance

Zone 11F - Agency Seal
20 x 20 mm
Must not impair readability of text. Start with 65% brightness and 25% contrast.

Zone 13F - Issue date
Format YYYYMMMDD

Zone 4F – Agency Specific Text Area
60

Zone 5F - Rank

Zone 6F - PDF417 bar code

50

Zone 12F - Footer
(Emergency Response example shown)

1073
1074
1075

Figure 4-2. Card Front—Optional Data Placement—Example 1

1076

1077

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.
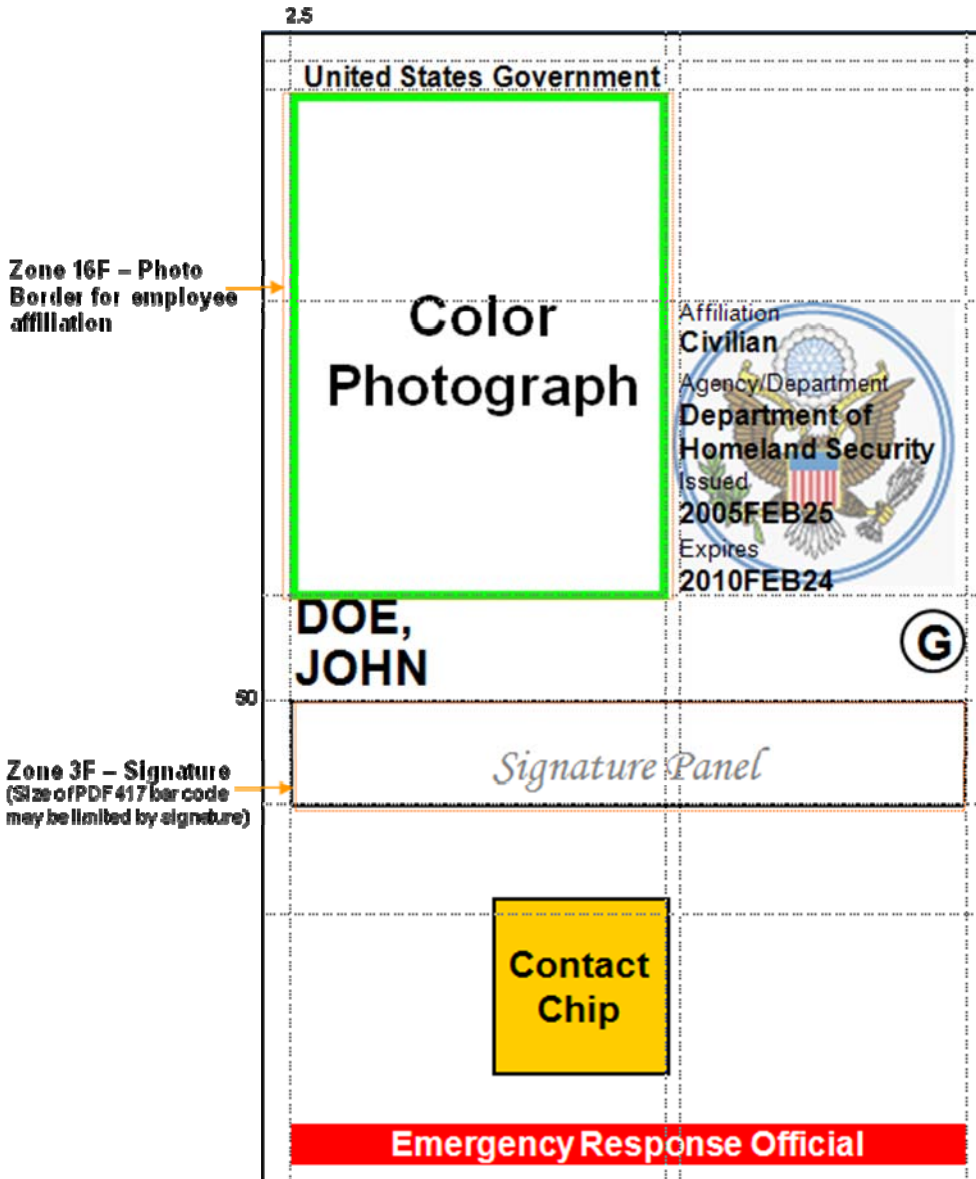
1078
1079
1080 **Figure 4-3. Card Front—Optional Data Placement—Example 2**

1081

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for
data.
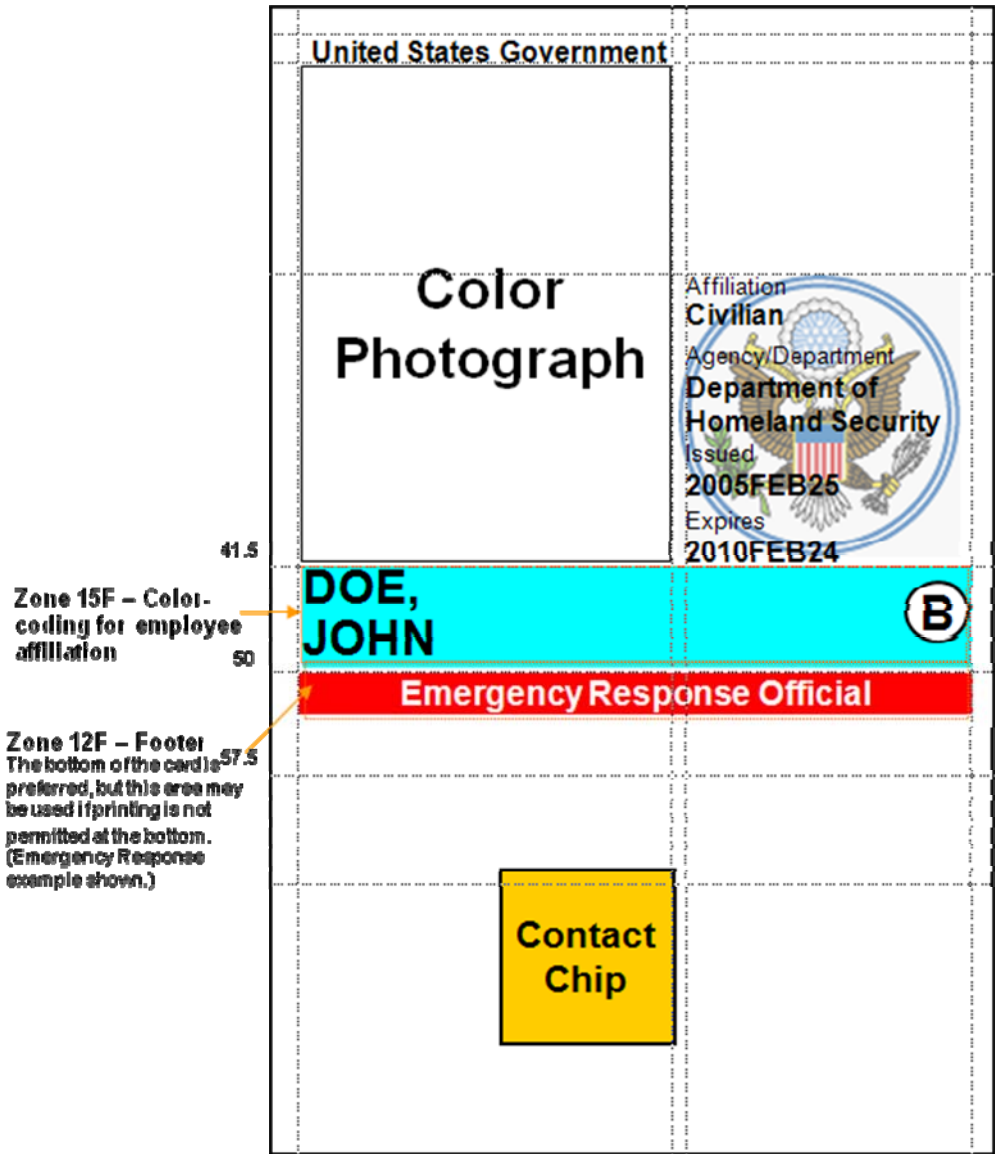
1082

1083   **Figure 4-4. Card Front—Optional Data Placement—Example 3**

1084

1085

1086

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.

1087

1088   **Figure 4-5. Card Front—Optional Data Placement—Example 4**

1089

1090

1091

All measurements are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.

1092
1093
1094

Figure 4-6. Card Back—Printable Areas and Required Data

1095

1096

All measurements are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.

Zone 3B – Magnetic Stripe
ISO 7811-6 standard

Zone 5B – Physical characteristics and TSA checkpoint information
Limit use of abbreviations. Use English units.

Hair: Brown
Eyes: Brown
D.O.B.: 01/01/1970
Height: 5'11"
Gender: Male

This credential is the property of the U.S. Government. Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code. The bearer of this card is a designated Emergency Responder. After Credential verification, bearer should be given access to controlled areas.

Return to:
Security Manager's Office
1800 F Street, N.W.
Washington, DC 20405

Issuer ID

Serial Number

Contact Chip

Zone 8B – 3 of 9 bar code
May use optional printing areas for ends of bar code. Must be positioned as shown for slot-reader compatibility.

Zone 7B – Section 499, Title 18 language
5pt Arial Normal

Zone 6B – Emergency Responder details
5pt Arial Normal

Zone 4B – Return Address
5pt Arial Normal

1097
1098
1099

Figure 4-7. Card Back—Optional Data Placement—Example 1

1100

All measurements are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.
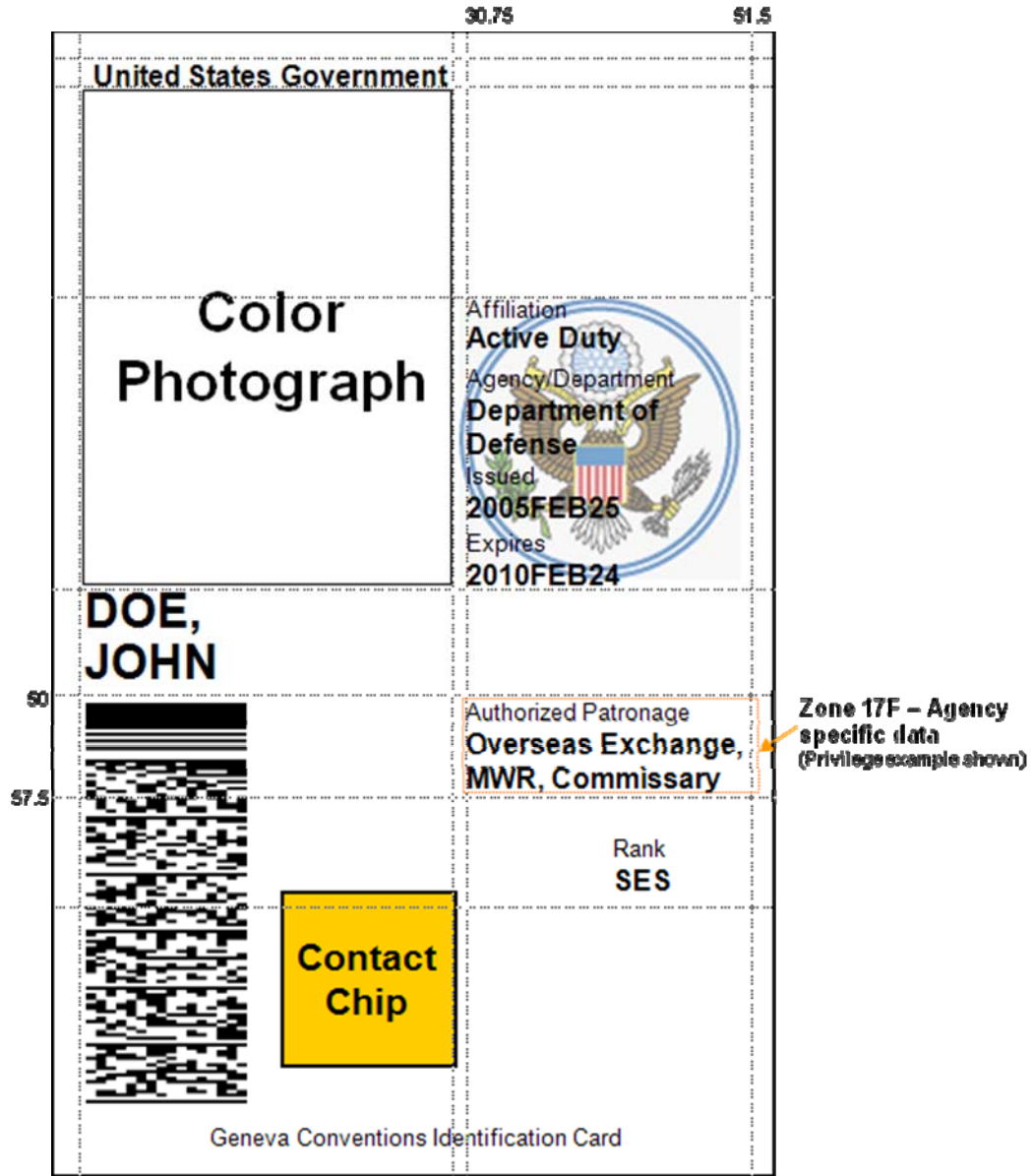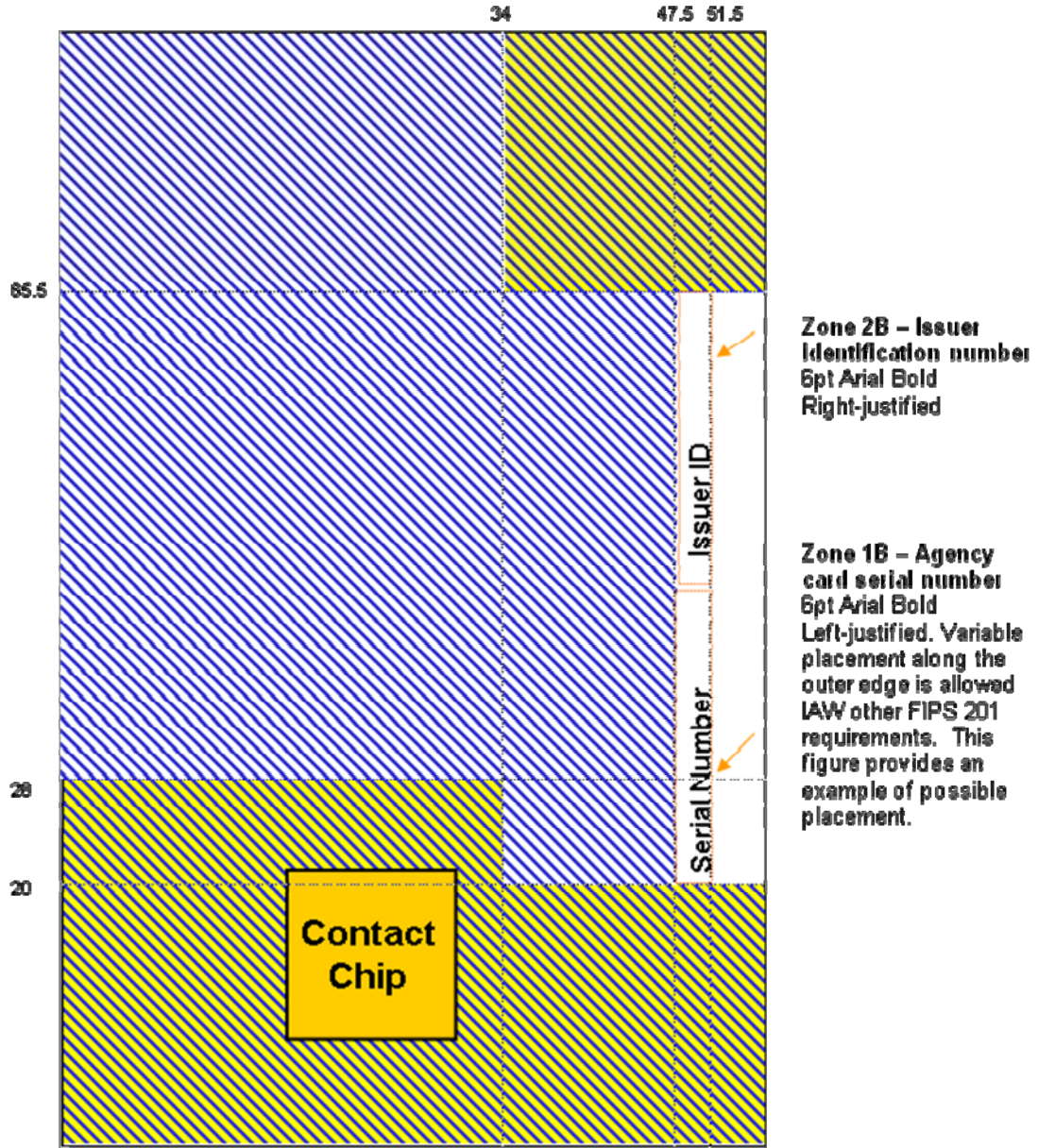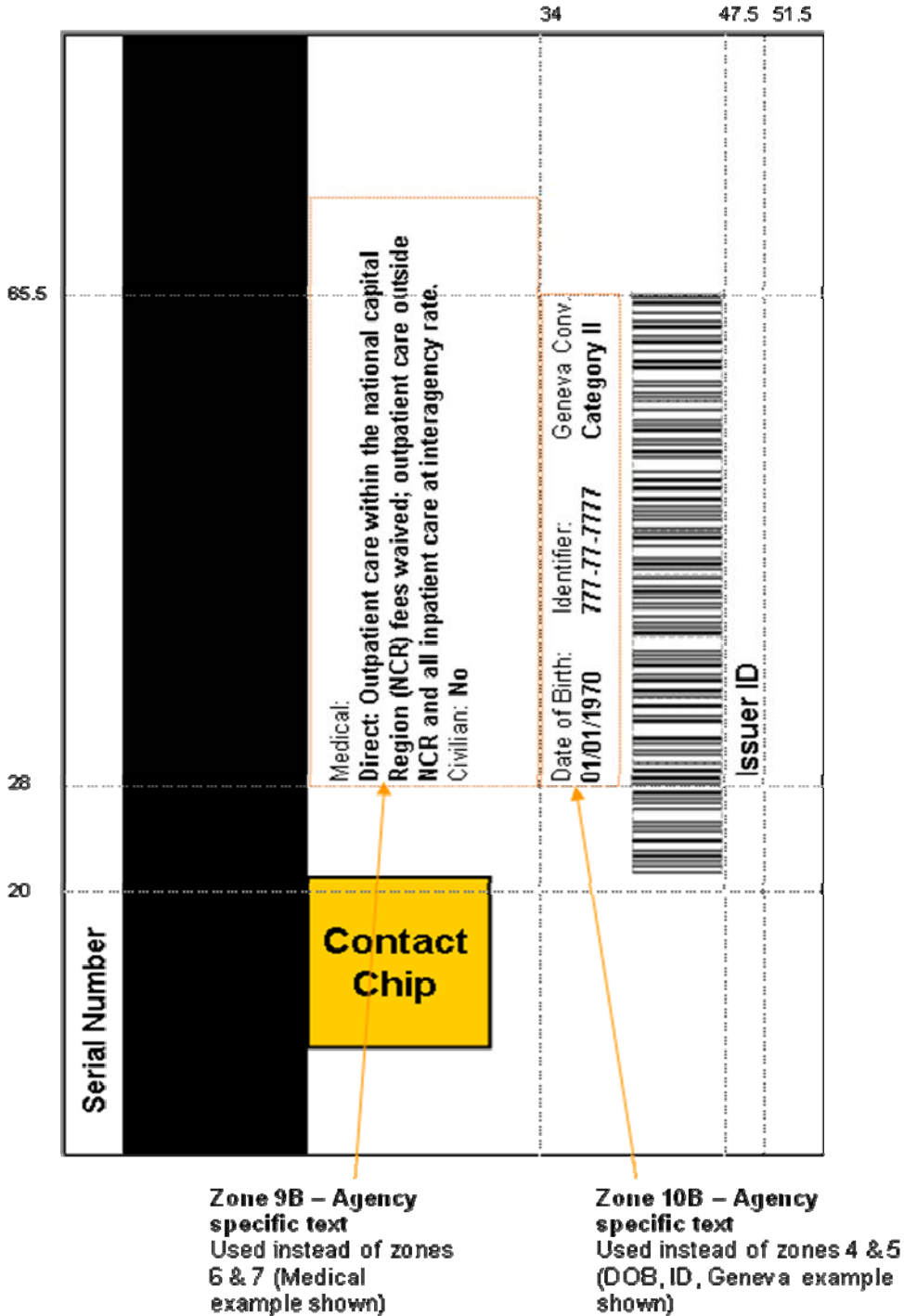

1101
1102
1103 **Figure 4-8. Card Back—Optional Data Placement—Example 2**

1104   **4.1.5 Color Representation**

1105   Table 4-1 provides quantitative specifications for colors in three different color systems: sRGB
1106   Tristimulus, sRGB ([IEC 61966], Color management – default RGB color space), and CMYK (Cyan,
1107   Magenta, Yellow and Key or 'blacK'). Since the card body is white, the white color-coding is achieved
1108   by the absence of printing. Note that presence of the security feature, which may overlap colored or
1109   printed regions, may modify the perceived color. In the case of colored regions, the effect of overlap
1110   shall not prevent the recognition of the principal color by a person with normal vision (corrected or
1111   uncorrected) at a working distance of 50 cm to 200 cm.

1112   **Table 4-2. Color Representation**

Color	Zone	sRGB Tristimulus Value (IEC 61966-2-1)	sRGB Value (IEC 61966-2-1)	CMYK Value {C,M,Y,K}
White	15F	{255, 255, 255}	{255, 255, 255}	{0, 0, 0, 0}
Green	15F	{153, 255, 153}	{203, 255, 203}	{40, 0, 40, 0}
Blue	15F	{0, 255, 255}	{0, 255, 255}	{100, 0, 0, 0}
Red	12F	{253, 27, 20}	{254, 92, 79}	{0, 90, 86, 0}

1113
1114   The colors in Table 4-2 can be mapped to the Pantone[7] color cue; however, note that this will not produce
1115   an exact match. An agency or department may use the following Pantone mappings in cases where Table
1116   4-2 scales are not available.
1117
1118   +   Blue—630C

1119   +   White—White

1120   +   Green—359C

1121   +   Red—032C

1122
1123   **4.1.6 Logical Credentials**

1124   This section defines logical identity credentials and the requirements for use of these credentials.

1125   **4.1.6.1 Logical Credential Data Model**

1126   To support a variety of authentication mechanisms, the PIV logical credentials shall contain multiple data
1127   elements for the purpose of verifying the cardholder's identity at graduated assurance levels. These
1128   mandatory data elements are part of the data model for PIV logical credentials, and include the following:

1129   +   A PIN

1130   +   A CHUID

1131   +   PIV authentication data (one asymmetric key pair and corresponding certificate)

1132   +   Two biometric fingerprints or if fingerprints are not collectible, two iris images

---

[7] Pantone is a registered name protected by law.

1133   **+**   Card authentication data (one asymmetric key pair and corresponding certificate)

1134 This standard also defines optional data elements for the PIV data model. These optional data elements
1135 include:

1136   **+**   An asymmetric key pair and corresponding certificate for digital signatures

1137   **+**   An asymmetric key pair and corresponding certificate for key management

1138   **+**   A symmetric card authentication key for supporting physical access applications

1139   **+**   A symmetric key associated with the card management system.

1140   **+**   Facial image

1141   **+**   One or two iris images

1142   **+**   On-card biometric comparison data

1143 In addition to the above, other data elements are specified in [SP 800-73].

1144 PIV logical credentials fall into the following three categories:

1145   1.   Credential elements used to prove the identity of the cardholder to the card (CTC authentication)

1146   2.   Credential elements used to prove the identity of the card management system to the card (CMTC
1147   authentication)

1148   3.   Credential elements used by the card to prove the identity of the cardholder to an external entity
1149   (CTE authentication) such as a host computer system.

1150 The PIN falls into the first category, the card management key into the second category, and the CHUID,
1151 biometric credential, symmetric keys, and asymmetric keys into the third.

1152 **4.1.7   PIV Card Activation**

1153 The PIV Card shall be activated[8] to perform privileged[9] operations such as reading biometric information
1154 and using the PIV authentication key, digital signature key, and key management key. The PIV Card
1155 shall be activated for privileged operations only after authenticating the cardholder or the appropriate card
1156 management system. Cardholder activation is described in Section 4.1.7.1, and card management system
1157 activation is described in Section 4.1.7.2.

1158 **4.1.7.1   Activation by Cardholder**

1159 PIV Cards shall implement user-based cardholder activation to allow privileged operations using PIV
1160 credentials held by the card. At a minimum, the PIV Card shall implement PIN-based cardholder
1161 activation in support of interoperability across departments and agencies. Other card activation
1162 mechanisms, only as specified in [SP 800-73], may be implemented and shall be discoverable. For PIN-
1163 based cardholder activation, the cardholder shall supply a numeric PIN. The verification data shall be

---

[8] Activation in this context refers to the unlocking of the PIV Card application so privileged operations can be performed.
[9] A read of a PIV CHUID or use of the card authentication key is not considered a privileged operation.

1164   transmitted to the PIV Card and checked by the card. If the verification data check is successful, the PIV
1165   Card is activated. The PIV Card shall include mechanisms to block activation of the card after a number
1166   of consecutive failed activation attempts.

1167   The PIN should not be easily-guessable or otherwise individually-identifiable in nature (e.g., part of a
1168   Social Security Number, phone number). The required PIN length shall be a minimum of six digits.

1169   **4.1.7.2   Activation by Card Management System**

1170   PIV Cards may support card activation by the card management system to support card personalization
1171   and post-issuance card update. To activate the card for personalization or update, the card management
1172   system shall perform a challenge response protocol using cryptographic keys stored on the card in
1173   accordance with [SP 800-73]. When cards are personalized, card management keys shall be set to be
1174   specific to each PIV Card. That is, each PIV Card shall contain a unique card management key. Card
1175   management keys shall meet the algorithm and key size requirements stated in Special Publication 800-
1176   78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP 800-78]

1177   **4.2   Cardholder Unique Identifier (CHUID)**

1178   The PIV Card shall include the CHUID as defined in [SP 800-73]. The CHUID includes the Federal
1179   Agency Smart Credential Number (FASC-N), which uniquely identifies each card as described in [SP
1180   800-73]. CHUID elements specific to this standard are described below in Section 4.2.1. The format of
1181   the CHUID signature element is described in Section 4.2.2.

1182   The PIV CHUID shall be accessible from both the contact and contactless interfaces of the PIV Card
1183   without card activation. The PIV FASC-N shall not be modified post-issuance.

1184   The CHUID may be read and used by the relying systems, but it should be treated as if it were a password
1185   (since the digital signature provides entropy equivalent to a password) for purposes of retention. A stored
1186   CHUID presents risks similar to a stored password; it can be copied and used to gain access. It is strongly
1187   recommended that a complete CHUID should not be stored in relying systems.

1188   **4.2.1   PIV CHUID Data Elements**

1189   In addition to the mandatory FASC-N that identifies a PIV Card, the CHUID shall include an expiration
1190   date data element in machine readable format that specifies when the card expires. The expiration date
1191   format and encoding rules are as specified in [SP 800-73]. For PIV Cards, the format of the asymmetric
1192   signature field is specified in Section 4.2.2.

1193   **4.2.2   Asymmetric Signature Field in CHUID**

1194   This standard requires inclusion of the asymmetric signature field in the CHUID container. The
1195   asymmetric signature data element of the PIV CHUID shall be encoded as a Cryptographic Message
1196   Syntax (CMS) external digital signature, as defined in RFC 5652 [RFC5652]. The digital signature shall
1197   be computed in accordance with [SP 800-73]. Algorithm and key size requirements for the asymmetric
1198   signature are detailed in [SP 800-78].

1199   The issuer asymmetric signature file is implemented as a *SignedData* type, as specified in [RFC5652],
1200   and shall include the following information:
1201
1202   +   The message shall include a *version* field specifying version v3

1203   +   The *digestAlgorithms* field shall be as specified in [SP 800-78]

1204   +   The *encapContentInfo* shall:

1205   –   Specify an *eContentType* of id-PIV-CHUIDSecurityObject

1206   –   Omit the *eContent* field

1207   +   The *certificates* field shall include only a single X.509 certificate, which can be used to verify the
1208   signature in the *SignerInfo* field

1209   +   The *crls* field shall be omitted

1210   +   *signerInfo*s shall be present and include only a single *SignerInfo*

1211   +   The *SignerInfo* shall:

1212   –   Use the *issuerAndSerialNumber* choice for *SignerIdentifier*

1213   –   Specify a *digestAlgorithm* in accordance with [SP 800-78]

1214   –   Include, at a minimum, the following signed attributes:

1215   •   A *MessageDigest* attribute containing the hash computed in accordance with [SP 800-73]

1216   •   A *pivSigner-DN* attribute containing the subject name that appears in the PKI certificate
1217   for the entity that signed the CHUID

1218   –   Include the digital signature.

1219   The public key required to verify the digital signature shall be provided in the *certificates* field in an
1220   X.509 digital signature certificate issued under the id-fpki-common-devices, id-fpki-common-hardware,
1221   or id-fpki-common-High policy of [COMMON].[10] The X.509 digital signature certificate issued under
1222   the id-fpki-common-devices, id-fpki-common-hardware, or id-fpki-common-High policy of [COMMON]
1223   shall also include an extended key usage (*extKeyUsage)* extension asserting id-PIV-content-signing.
1224   Additional descriptions for the PIV object identifiers are provided in Appendix D.

1225   ### 4.3   Cryptographic Specifications

1226   The PIV Card shall implement the cryptographic operations and support functions as defined in [SP 800-
1227   78] and [SP 800-73].

1228   The PIV Card must store private keys and corresponding public key certificates, and perform
1229   cryptographic operations using the asymmetric private keys. At a minimum, the PIV Card must store two
1230   asymmetric private keys and the corresponding public key certificates, namely the *PIV authentication key*
1231   and the *asymmetric card authentication key*. With the exception of the *card authentication key and keys*
1232   *used to establish a secure messaging*, the cryptographic private key operations shall be performed only
1233   through the contact interface.

---

[10] For legacy PKIs, as defined in Section 5.4, the certificates may be issued under a department or agency-specific policy that has
been cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level.

1234 The PIV Card may include additional asymmetric keys and PKI certificates. This standard defines
1235 requirements for digital signature and key management keys. Where digital signature keys are supported,
1236 the PIV Card is not required to implement a secure hash algorithm. Message hashing may be performed
1237 off card. Symmetric cryptographic operations are not mandated for the contactless interface, but
1238 departments and agencies may choose to supplement the basic functionality with storage for a symmetric
1239 card authentication key and support for a corresponding set of cryptographic operations. For example, if
1240 a department or agency wants to utilize Advanced Encryption Standard (AES) based challenge/response
1241 for physical access, the PIV Card must contain storage for the AES key and support AES operations
1242 through the contactless interface. Algorithms and key sizes for each PIV key type are specified in [SP
1243 800-78].

1244 The PIV Card has both mandatory keys and optional keys:

1245 + The *PIV authentication key* shall be an asymmetric private key that is accessible from the contact
1246 interface and supports card authentication for an interoperable environment. This is a mandatory
1247 key for each PIV Card.

1248 + The *asymmetric card authentication key* shall be a private key that is accessible over the
1249 contactless and contact interface and supports card authentication for an interoperable
1250 environment. This is a mandatory key for each PIV Card.

1251 + The *symmetric (secret) card authentication key* supports card authentication for physical access,
1252 and it is optional.

1253 + The *digital signature key* is an asymmetric private key supporting document signing, and it is
1254 optional.

1255 + The *key management key* is an asymmetric private key supporting key establishment and
1256 transport, and it is optional. This can also be used as an encryption key. Optionally, up to twenty
1257 retired key management keys may also be stored on the PIV Card.

1258 + The *card management key* is a symmetric key used for personalization and post-issuance
1259 activities, and it is optional.

1260 + The PIV Card may include additional key(s) for use with secure messaging to enable protocols
1261 such as on-card biometric comparison. These keys are defined in [SP 800-73] or [SP 800-78].

1262 All PIV cryptographic keys shall be generated within a FIPS 140 validated cryptographic module with
1263 overall validation at Level 2 or above. In addition to an overall validation of Level 2, the PIV Card shall
1264 provide Level 3 physical security to protect the PIV private keys in storage.

1265 Requirements specific to storage and access for each key are detailed below. Where applicable, key
1266 management requirements are also specified.

1267 + **PIV Authentication Key.** This key shall be generated on the PIV Card. The PIV Card shall not
1268 permit exportation of the PIV authentication key. The PIV authentication key must be available
1269 only through the contact interface of the PIV Card. Private key operations may be performed
1270 using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for
1271 each operation).

1272   The PIV Card shall store a corresponding X.509 certificate to support validation of the public
1273   key. The X.509 certificate shall include the FASC-N in the subject alternative name extension
1274   using the pivFASC-N attribute to support physical access procedures. The expiration date of the
1275   certificate must be no later than the expiration date of the PIV Card. Issued PIV Authentication
1276   certificates shall also include a PIV NACI indicator extension, until such time that OMB
1277   approves a government-wide operational system for distribution of Background Investigation
1278   status information (see Section 2.5). After OMB approves such an operational system, the
1279   inclusion of the PIV NACI indicator extension in issued PIV Authentication certificates is
1280   optional and deprecated. Section 5 of this document specifies the certificate format and the key
1281   management infrastructure for PIV authentication key.

1282   +   **Asymmetric Card Authentication Key.** The asymmetric card authentication key shall be
1283   generated on the PIV Card. The PIV Card shall not permit exportation of the card authentication
1284   key. The card authentication key shall be available through the contact and the contactless
1285   interface of the PIV Card. Private key operations may be performed using this key without card
1286   activation (e.g., the PIN need not be supplied for operations with this key).

1287   The PIV Card shall store a corresponding X.509 certificate to support validation of the
1288   asymmetric card authentication key. The X.509 certificate shall include the FASC-N in the
1289   subject alternative name extension using the pivFASC-N attribute to support physical access
1290   procedures. The expiration date of the certificate must be no later than the expiration date of the
1291   PIV Card. Section 5 of this document specifies the certificate format and the key management
1292   infrastructure for asymmetric PIV Card authentication keys.

1293   +   **Symmetric Card Authentication Key.** The symmetric card authentication key is imported onto
1294   the card by the issuer. The PIV Card shall not permit exportation of this key. If present**,**
1295   cryptographic operations using this key may be performed without card activation (e.g., the PIN
1296   need not be supplied for operations with this key). The card authentication key shall be available
1297   through the contact and the contactless interface of the PIV Card. This standard does not specify
1298   key management protocols or infrastructure requirements.

1299   **+**   **Digital Signature Key.** The PIV digital signature key shall be generated on the PIV Card. The
1300   PIV Card shall not permit exportation of the digital signature key. If present, cryptographic
1301   operations using the digital signature key may only be performed using the contact interface of
1302   the PIV Card. Private key operations may not be performed without explicit user action.

1303   The PIV Card shall store a corresponding X.509 certificate to support validation of the digital
1304   signature key. Section 5 of this document specifies the certificate format and the key
1305   management infrastructure for PIV digital signature keys.

1306   **+**   **Key Management Key.** This key may be generated on the PIV Card or imported to the card. If
1307   present, the key management key must only be accessible using the contact interface of the PIV
1308   Card. Private key operations may be performed using an activated PIV Card without explicit user
1309   action (e.g., the PIN need not be supplied for each operation).

1310   The PIV Card shall import and store a corresponding X.509 certificate to support validation of the
1311   key management key. Section 5 of this document specifies the certificate format and the key
1312   management infrastructure for key management keys.

1313
1314
1315

    +   **Card Management Key.** The card management key is imported onto the card by the issuer. If present, the card management key must only be accessible using the contact interface of the PIV Card.

1316   **4.4   PIV Biometric Data Specifications**

1317   The PIV biometric data shall consist of the following:

1318
1319

    +   A full set of fingerprints used to perform law enforcement checks as part of the identity proofing and registration process.

1320
1321

    +   An electronic facial image used for printing the facial image on the card and for performing visual authentication during card usage. The facial image is not required to be stored on the card.

1322
1323
1324

    +   Two electronic fingerprints to be stored on the card for automated authentication during card usage. If no fingerprints can be collected, two electronic iris images shall be stored on the PIV Card.

1325   The PIV biometric data may optionally include:

1326   +   One or two iris images

1327   +   On-card biometric comparison data

1328
1329

All biometric data enumerated above are collected during the identity proofing and registration process. PIV biometric data shall be stored on PIV Cards as specified in [SP 800-76] and [SP 800-73].

1330
1331
1332
1333
1334
1335
1336
1337

The PIV biometric data, except for on-card biometric comparison data, stored on the card shall be only accessible through the contact interface and after the presentation of a valid PIN. No contactless access is permitted for the PIV biometric data, except for on-card biometric comparison data, specified to be stored on the PIV Card under this standard. The on-card biometric comparison data may be available through the contact and the contactless interface of the PIV Card to support card activation (section 4.1.7.1) and cardholder authentication (section 6.2.5). The PIV Card shall not permit exportation of the on-card biometric comparison data. If implemented, PIV on-card biometric comparison data shall be implemented and used in accordance with [SP 800-73] and [SP 800-76].

1338   **4.4.1   Biometric Data Collection and chain-of-trust**

1339
1340
1341
1342
1343
1344
1345

A card issuer shall maintain, for each PIV Card issued, a documentary chain-of-trust for the identification data it collects. The chain-of-trust is a sequence of related enrollment data records, and shall be created and maintained through the methods of contemporaneous acquisition of data within each enrollment data record, and biometric matching of samples between enrollment data records[11]. An enrollment data record shall describe the circumstances of biometric acquisition including the name and role of the acquiring agent, the office and organization, time, place, and acquisition method. An enrollment data record may or may not contain historical biometric data[12]. A card issuer shall retain a biometric record, for example two

---

[11] For example, ten fingerprints for law enforcement checks may be collected at one time and place, and two fingerprints for PIV Card templates may be collected at a later time and different place, provided that the two fingerprints are verified as among the ten original fingerprints.

[12] An enrollment data set will always include biometric data immediately after it is created, but the biometric data itself may be deleted from the enrollment data set when it is no longer needed. The most recent biometric data shall be retained in the chain of trust. This enables extending and reconnecting the chain of trust.

1346   fingerprint templates, from the most recent enrollment to extend the chain-of-trust when necessary.[13] If
1347   the card issuer cannot collect and retain two fingerprints templates, two iris images shall be retained as the
1348   biometric data for the chain-of-trust and used in 1:1 biometric match to reconnect to the chain-of-trust.
1349   The biometric data in the chain-of-trust shall be valid for at most 12 years.

1350   A card issuer shall be able to import and export a chain-of-trust in the manner and representation
1351   described in [TBD].

1352   The chain-of-trust will be applied in several situations to include:

1353   +   Extended enrollment: a PIV applicant enrolls ten fingerprints for background investigations at
1354   one place and time (e.g., at a police station), and two fingerprints for on-card templates at another
1355   place and time (e.g., at the PIV enrollment station). The chain-of-trust would contain identifiers
1356   and two enrollment data records, one with a ten fingerprint transaction, and one with two
1357   fingerprint templates. The two fingerprint templates would be matched against the corresponding
1358   fingers in the ten fingerprint data set to link the chain.

1359   +   Reissuance: a PIV cardholder loses his/her card. Since the card issuer has biometric enrollment
1360   data records, the cardholder can perform a 1:1 biometric match to reconnect to the card issuer's
1361   chain-of-trust. The card issuer need not repeat the background investigation. The card issuer
1362   proceeds to issue a new card as described in Section 2.5.2.

1363   +   Interagency transfer: a Federal employee is transferred from one agency to another. When the
1364   employee leaves the old agency, he/she surrenders the PIV Card and it is destroyed. When the
1365   employee arrives at new agency and is processed in, the card issuer in the new agency requests
1366   the employee's chain-of-trust from the card issuer in the old agency, and receives the chain-of-
1367   trust. The employee performs a 1:1 biometric match against the chain-of-trust, and the interaction
1368   proceeds as a PIV Card Reissuance as described in Section 2.5.2.

1369   The technical specifications for the collection and formatting of the ten fingerprints and other biometric
1370   information are contained in [SP 800-76]. The fingerprints shall be used for one-to-many matching with
1371   the database of fingerprints maintained by the FBI. The fingerprints should be captured using FBI-
1372   certified scanners and transmitted using FBI standard transactions. This one-to-many matching is called
1373   biometric identification. The requirement for ten fingerprints is based on matching accuracy data
1374   obtained by NIST in large-scale trials and reported in NISTIR 7123 [NISTIR7123]. Because biometric
1375   identification using fingerprints is the primary means for law enforcement checks, agencies shall seek
1376   OPM guidance for alternative means for performing law enforcement checks in cases where obtaining ten
1377   fingerprints is impossible.

1378   In cases where the collection of fingerprints for the PIV Card is not possible, two iris images shall be
1379   collected from the PIV applicant. The technical specifications for the electronic iris images are contained
1380   in [SP 800-76]. The electronic iris images may be used for biometric authentication as defined in Section
1381   6.2.3. This approach is required when the PIV Card does not contain fingerprint templates because the
1382   card issuer could not collect usable fingerprint images from the cardholder.

1383   A facial image shall be collected from all PIV applicants. The technical specifications for an electronic
1384   facial image are contained in [SP 800-76]. The electronic facial image may be used for the following
1385   purposes:

---

[13] If an agency is unable to collect fingerprint biometric data or iris images biometric data, a circumstance requiring PIV Card reissuance would force a new chain-of-trust to be created, implying a new FBI National Criminal History Check.

1386   **+**   For generating the printed image on the card

1387   **+**   For generating a visual image on the monitor of a guard workstation for augmenting the visual
1388   authentication process defined in Section 6.2.1. This approach may be required in the following
1389   situations:

1390   –   A good live sample of fingerprints or iris cannot be collected from the PIV cardholder due to
1391   damage or injury.

1392   –   Fingerprint or iris matching equipment failure

1393   –   Authenticating PIV cardholders covered under Section 508.

1394   Two electronic fingerprints shall be collected from all PIV applicants, who can provide them, for storing
1395   on the card. Alternatively, these two electronic fingerprints can also be extracted from the ten fingerprints
1396   collected earlier for law enforcement checks. The technical specifications for the two electronic
1397   fingerprints are contained in [SP 800-76]. The right and left index fingers shall normally be designated as
1398   the primary and secondary finger, respectively. However, if those fingers cannot be imaged, the primary
1399   and secondary designations shall be taken from the following fingers, in decreasing order of priority:

1400   1. Right thumb

1401   2. Left thumb

1402   3. Right middle finger

1403   4. Left middle finger

1404   5. Right ring finger

1405   6. Left ring finger

1406   7. Right little finger

1407   8. Left little finger

1408   These fingerprint templates shall be used for 1:1 biometric verification against live samples collected
1409   from the PIV cardholder (see Section 6.2.3). Even though two fingerprints are available on the card, a
1410   department or agency has the option to use one or both of them for the purpose of PIV cardholder
1411   authentication. If only one fingerprint is used for authentication, then the primary finger shall be used
1412   first. In cases where there is difficulty in collecting even a single live scan sample fingerprint of
1413   acceptable quality, the department or agency shall perform authentication using asymmetric cryptography
1414   as described in Section 6.2.4.1.

1415   **4.4.2   Biometric Data Representation and Protection**

1416   Biometric data shall be formatted using the standardized records specified in [SP 800-76]. The integrity
1417   of the mandatory fingerprint and optional iris and facial data records shall be protected using digital
1418   signatures as follows. The records shall be prepended with a Common Biometric Exchange Formats
1419   Framework (CBEFF) header (referred to as CBEFF_HEADER) and appended with the CBEFF signature
1420   block (referred to as the CBEFF_SIGNATURE_BLOCK) [CBEFF].

1421   The format for CBEFF_HEADER is specified in [SP 800-76].

1422 The CBEFF_SIGNATURE_BLOCK contains the digital signature of the biometric data and thus
1423 facilitates the verification of integrity of the biometric data. The process of generating a
1424 CBEFF_SIGNATURE_BLOCK is described as follows. The CBEFF_SIGNATURE_BLOCK shall be
1425 encoded as a CMS external digital signature as defined in [RFC5652]. The digital signature shall be
1426 computed over the entire CBEFF structure except the CBEFF_SIGNATURE_BLOCK itself (which
1427 means that it includes the CBEFF_HEADER and the biometric records). The algorithm and key size
1428 requirements for the digital signature are detailed in [SP 800-78].

1429 The CMS encoding of the CBEFF_SIGNATURE_BLOCK is as a *SignedData* type, and shall include the
1430 following information:

1431   +   The message shall include a *version* field specifying version v3

1432   +   The *digestAlgorithms* field shall be as specified in [SP 800-78]

1433   +   The *encapcontentInfo* shall

1434   –   Specify an *eContentType* of id-PIV-biometricObject

1435   –   Omit the *eContent* field

1436   +   If the signature on the biometric was generated with the same key as the signature on the CHUID,
1437   the *certificates* field shall be omitted

1438   +   If the signature on the biometric was generated with a different key than the signature on the
1439   CHUID, the *certificates* field shall include only a single certificate, which can be used to verify
1440   the signature in the *SignerInfo* field

1441   +   The *crls* field shall be omitted

1442   +   *signerInfo*s shall be present and include only a single *SignerInfo*

1443   +   The *SignerInfo* shall

1444   –   Use the *issuerAndSerialNumber* choice for *SignerIdentifier*

1445   –   Specify a *digestAlgorithm* in accordance with [SP 800-78]

1446   –   Include at a minimum the following signed attributes:

1447   •   A *MessageDigest* attribute containing the hash of the concatenated CBEFF_HEADER +
1448   Biometric Record

1449   •   A *pivFASC-N* attribute containing the FASC-N of the PIV Card (to link the biometric
1450   data and PIV Card)

1451   •   A *pivSigner-DN* attribute containing the subject name that appears in the PKI certificate
1452   for the entity that signed the biometric data

1453   –   Include the digital signature.

1454 The X.509 certificate containing the public key required to verify the digital signature shall be issued
1455 under the id-fpki-common-devices, id-fpki-common-hardware, or id-fpki-common-High policy of

1456 [COMMON].[14] The certificate shall also include an extended key usage (*extKeyUsage)* extension
1457 asserting id-PIV-content-signing. Additional descriptions for the PIV object identifiers are provided in
1458 Appendix D.

4.4.3 Biometric Data Content

1460 Matching accuracy and data interoperability are the driving factors in specifying the biometric data on the
1461 PIV Card. These data characteristics include the image parameters (e.g., pixel density, pixel depth) in the
1462 image records as well as the fields in the encapsulating standard biometric record. As already stated, the
1463 biometric data content collected over the PIV life cycle shall conform to the specifications outlined in [SP
1464 800-76].

4.5 Card Reader Requirements

1466 This section provides minimum requirements for the contact and contactless card readers. Also, this
1467 section provides requirements for PIN input devices. Further requirements are specified in [SP 800-96].

4.5.1 Contact Reader Requirements

1469 Contact card readers shall conform to the [ISO7816] standard for the card-to-reader interface. These
1470 readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-
1471 to-host system interface in general desktop computing environment. Specifically, the contact card readers
1472 shall conform to the requirements specified in [SP 800-96]. In physical access control systems where the
1473 readers are not connected to general purpose desktop computing systems, the reader-to-host system
1474 interface is not specified in this standard.

4.5.2 Contactless Reader Requirements

1476 Contactless card readers shall conform to [ISO14443] standard for the card-to-reader interface and data
1477 transmitted over the [ISO14443] link shall conform to [ISO7816]. In cases where these readers are
1478 connected to general purpose desktop computing systems, they shall conform to [PCSC] for the reader-to-
1479 host system interface. Specifically, the contact card readers shall conform to the requirements specified
1480 in [SP 800-96]. In physical access control systems where the readers are not connected to general
1481 purpose desktop computing systems, the reader-to-host system interface is not specified in this standard.
1482 This is necessary to allow retrofitting of PIV readers into existing physical access control systems that use
1483 a variety of non-standard card reader communication interfaces.

4.5.3 Reader Resilience and Flexibility

1485 The international standard ISO/IEC 24727 [ISOIEC 24727] enables a high degree of interoperability
1486 between electronic credentials and relying subsystems by means of a firmware-defined adaptation layer.
1487 To make interoperability among PIV System middleware, card readers, and credentials more resilient and
1488 flexible, the Department of Commerce will evaluate ISO/IEC 24727 and propose an optional profile of
1489 ISO/IEC 24727 in [SP 800-73]. The profile will explain how profile-conformant middleware, card
1490 readers, and PIV Cards can be used interchangeably with middleware, card readers, and PIV Cards
1491 currently deployed.

---

[14] For legacy PKIs, as defined in Section 5.4.4, the certificates may be issued under a department or agency-specific policy that
has been cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level.

1492   Specifications of the profile will become effective, as a means to implement PIV System readers and
1493   middleware, when OMB determines that the profile specifications are complete and ready for
1494   deployment.

1495   **4.5.4   PIN Input Device Requirements**

1496   PIN input devices shall be used for implementing PIN-based PIV Card activation. When the PIV Card is
1497   used with a PIN for physical access, the PIN input device shall be integrated with the reader. When the
1498   PIV Card is used with a PIN for logical access (e.g., to authenticate to a Web site or other server), the PIN
1499   input device may be integrated with the reader or entered using the computer's keyboard. If the PIN input
1500   device is not integrated with the reader, the PIN shall be transmitted securely and directly to the PIV Card
1501   for card activation.

1502

5. PIV Key Management Requirements

PIV Cards consistent with this specification will have two or more asymmetric private keys. To manage the public keys associated with the asymmetric private keys, departments and agencies shall issue and manage X.509 public key certificates as specified below.

5.1 Architecture

The CA that issues certificates to support PIV Card authentication shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI. Self-signed, self-issued, and CA certificates issued by these CAs shall conform to *Worksheet 1: Self-Signed Certificate Profile*, *Worksheet 2: Self-Issued CA Certificate Profile*, and *Worksheet 3: Cross Certificate Profile,* respectively, in *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program* [PROF]. The requirements for legacy PKIs are defined in Section 5.4.

5.2 PKI Certificate

All certificates issued to support PIV Card authentication shall be issued under the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* [COMMON]. The requirements in this certificate policy cover identity proofing and the management of CAs and registration authorities. CAs and registration authorities may be operated by departments and agencies, or may be outsourced to PKI service providers. For a list of PKI service providers that have been approved to operate under [COMMON], see http://www.idmanagement.gov/fpkipa/cpl.cfm.

[COMMON] requires FIPS 140 Level 2 validation for the subscriber cryptographic module (i.e., the PIV Card). In addition, this standard requires the cardholder to authenticate to the PIV Card each time it performs a private key computation with the digital signature key.

5.2.1 X.509 Certificate Contents

The required contents of X.509 certificates associated with PIV private keys are based on [PROF]. The relationship is described below:

+ Certificates containing the public key associated with an asymmetric Card Authentication Key shall conform to *Worksheet 8: Card Authentication Certificate Profile* in [PROF].

+ Certificates containing the public key associated with a digital signature private key shall conform to *Worksheet 5: End Entity Signature Certificate Profile* in [PROF] and shall specify either the id-fpki-common-hardware or id-fpki-common-High policy in the certificate policies extension.

+ Certificates containing the public key associated with a PIV authentication private key shall conform to *Worksheet 9: PIV Authentication Certificate Profile* in [PROF].

+ Certificates containing the public key associated with a key management private key shall conform to *Worksheet 6: Key Management Certificate Profile* in [PROF].[15]

---

[15] Note that Key Management certificates may assert the id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High policy in the certificate policies extension. Applications / relying systems sensitive to the assurance level may choose not to accept certificates that only assert id-fpki-common-policy.

1537   **+**   Requirements for algorithms and key sizes for each type of PIV asymmetric key are given in [SP
1538   800-78].

1539
1540 ## 5.3   X.509 CRL Contents

1541   CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a
1542   minimum. The contents of X.509 CRLs shall conform to *Worksheet 4: CRL Profile* in [PROF].

1543 ## 5.4   Migration from Legacy PKIs

1544   For the purposes of this standard, legacy PKIs are the PKIs of departments and agencies that have cross-
1545   certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level. PIV
1546   Authentication Certificates and Card Authentication Certificates issued by legacy PKIs shall meet the
1547   requirements specified in Section 5.2.1. Departments and agencies may assert department or agency-
1548   specific policy OIDs in PIV Authentication Certificates and Card Authentication Certificates in addition
1549   to the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth OID, respectively.
1550   This specification imposes no requirements on digital signature or key management certificates issued by
1551   legacy PKIs.

1552 ## 5.5   PKI Repository and OCSP Responder(s)

1553   The PIV PKI Repository and Online Certificate Status Protocol (OCSP) responder provides PIV Card and
1554   key status information across departments, agencies, and other organizations, to support high-assurance
1555   interagency PIV Card interoperation. Departments and agencies will be responsible for notifying
1556   Certification Authorities (CA) when cards or certificates need to be revoked. CAs shall maintain the
1557   status of servers and responders needed for PIV Card and certificate status checking.

1558   The expiration date of the authentication certificates (PIV authentication certificate and Card
1559   authentication certificate) shall not be after the expiration date of the PIV Card. If the card is revoked, the
1560   authentication certificates shall be revoked. However, an authentication certificate (and its associated key
1561   pair) may be revoked without revoking the PIV Card and may then be replaced. The presence of a valid,
1562   unexpired, and unrevoked authentication certificate on a card is proof that the card was issued and is not
1563   revoked.

1564   Because an authentication certificate typically is valid several years, a mechanism to distribute certificate
1565   status information is necessary. CRL and OCSP are the two commonly used mechanisms. CAs that issue
1566   authentication certificates shall maintain an LDAP directory server that holds the CRLs for the certificates
1567   it issues, as well as any CA certificates issued to or by it.

1568   PIV Authentication key certificates and Card Authentication key certificates shall contain the
1569   *crlDistributionPoints* and *authorityInfoAccess* extensions needed to locate CRLs and the authoritative
1570   OCSP responder, respectively. In addition, every CA that issues these authentication certificates shall
1571   operate an OCSP server that provides certificate status for every authentication certificate the CA issues.

1572 ### 5.5.1   Certificate and CRL Distribution

1573   This standard requires distribution of CA certificates and CRLs using LDAP and Hypertext Transport
1574   Protocol (HTTP). Specific requirements are found in the Shared Service Provider Repository Service
1575   Requirements [SSP REP].

1576   Certificates that contain the FASC-N in the subject alternative name extension, such as PIV
1577   Authentication certificates and Card Authentication certificates, shall not be distributed publicly (e.g., via
1578   LDAP or HTTP accessible from the public Internet). Individual departments and agencies can decide
1579   whether other user certificates (digital signature and key management) can be distributed via LDAP.
1580   When user certificates are distributed, the requirements in Table IV—End-Entity Certificate Repository
1581   Service Requirements of [SSP REP] shall be satisfied.

1582   **5.5.2   OCSP Status Responders**

1583   OCSP [RFC2560] status responders shall be implemented as a supplementary certificate status
1584   mechanism. The OCSP status responders must be updated at least as frequently as CRLs are issued. The
1585   definitive OCSP responder for each certificate shall be specified in the AIA extension as described in
1586   [PROF].

6. PIV Cardholder Authentication

1587

1588 This section defines a suite of identity authentication mechanisms that are supported by all the PIV Cards,
1589 and their applicability in meeting the requirements for a set of graduated levels of identity assurance.
1590 Specific implementation details of authentication mechanisms identified in this section are provided in
1591 [SP 800-73]. Moreover, while a wide range of authentication mechanisms is identified in this section,
1592 departments and agencies may adopt additional mechanisms that use the identity credentials on the PIV
1593 Card. In the context of the PIV Card Application, identity authentication is defined as the process of
1594 establishing confidence in the identity of the cardholder presenting a PIV Card. The authenticated
1595 identity can then be used to determine the permissions or authorizations granted to that identity for access
1596 to various physical and logical resources.

6.1 Identity Authentication Assurance Levels

1597

1598 This standard defines three levels of assurance for identity authentication supported by the PIV Card
1599 Application. Each assurance level sets a degree of confidence established in the identity of the holder of
1600 the PIV Card. The entity performing the authentication establishes confidence in the identity of the PIV
1601 cardholder through the following:

1602 1) The rigor of the identity proofing process conducted prior to issuing the PIV Card.

1603 2) The security of the PIV Card issuance and maintenance processes.

1604 3) The strength of the technical mechanisms used to verify that the cardholder is the owner of the
1605 PIV Card.

1606 Section 2 of this standard defines requirements for the identity proofing, registration, issuance, and
1607 maintenance processes for PIV Cards and establishes a common level of assurance in these processes.
1608 The PIV Card contains a number of visual and logical credentials. Depending on the specific PIV data
1609 used to authenticate the holder of the PIV Card to an entity that controls access to a resource, varying
1610 levels of assurance that the holder of the PIV Card is the owner of the card can be achieved. This is the
1611 basis for the following identity authentication assurance levels defined in this standard:

1612 **+** SOME Confidence—A basic degree of assurance in the identity of the cardholder

1613 **+** HIGH Confidence—A strong degree of assurance in the identity of the cardholder

1614 **+** VERY HIGH Confidence—A very strong degree of assurance in the identity of the cardholder.

1615 Parties responsible for controlling access to Federal resources (both physical and logical) shall determine
1616 the appropriate level of identity assurance required for access, based on the harm and impact to
1617 individuals and organizations as a result of errors in the authentication of the identity of the PIV
1618 cardholder. Once the required level of assurance has been determined, the authentication mechanisms
1619 specified within this section may be applied to achieve the required degree of confidence in the identity of
1620 the PIV cardholder.

6.1.1 Relationship to OMB's E-Authentication Guidance

1621

1622 The levels of identity authentication assurance defined within this standard are closely aligned with
1623 Section 2 of OMB's E-Authentication Guidance for Federal Agencies, M-04-04 [OMB404]. Specifically,

1624 Table 6-1 shows the notional relationship between the PIV identity authentication assurance levels and
1625 the [OMB404] identity authentication assurance levels.

1626

Table 6-1. Relationship Between PIV and E-Authentication Assurance Levels

OMB E-Authentication Levels		Comparable PIV Assurance Levels
Level Number	**Description**	
Level 2	Some confidence in the asserted identity's validity	SOME confidence
Level 3	High confidence in the asserted identity's validity	HIGH confidence
Level 4	Very high confidence in the asserted identity's validity	VERY HIGH confidence

1627

1628 [OMB404] addresses "four levels of identity assurance for electronic transactions requiring
1629 authentication" and prescribes a methodology for determining the level of identity assurance required
1630 based on the risks and potential impacts of errors in identity authentication. In the context of the PIV
1631 Card, owners of logical resources shall apply the methodology defined in [OMB404] to identify the level
1632 of identity authentication assurance required for their electronic transaction. Parties that are responsible
1633 for access to physical resources may use a methodology similar to that defined in [OMB404] to determine
1634 the PIV identity authentication assurance level required for access to their physical resource; they may
1635 also use other applicable methodologies to determine the required level of identity assurance for their
1636 application.

1637 **6.2   PIV Card Authentication Mechanisms**

1638 The following subsections define the basic types of authentication mechanisms that are supported by the
1639 credential set hosted by the PIV Card Application. PIV Cards can be used for identity authentication in
1640 environments that are equipped with card readers as well as those that lack card readers. Card readers,
1641 when present, can be contact readers or contactless readers. The usage environment affects the PIV
1642 identity authentication mechanisms that may be applied to a particular situation.

1643 Each authentication mechanism described in this section is strengthened through the use of a back-end
1644 certificate status verification infrastructure. The status of the authentication certificates (i.e., PIV
1645 authentication certificate and Card authentication Certificate) is directly tied to the status of all other
1646 credential elements held by the card. Sections 6.2.1 through 6.2.4 define the basic types of authentication
1647 mechanisms that are supported by the core (mandatory) credential set on the PIV Card and are
1648 interoperable across agencies. Section 6.2.5 and section 6.2.6 define the authentication mechanisms that
1649 are available if the optional logical credential elements are present on the PIV Card.

1650 **6.2.1   Authentication Using PIV Visual Credentials (VIS)**

1651 Visual authentication of a PIV cardholder shall be used only to support access control to physical
1652 facilities and resources.

1653 The PIV Card has several mandatory topographical features on the front and back that support visual
1654 identification and authentication, as follows:

1655   **+**   Zone 1F – Photograph

1656   **+**   Zone 2F – Name

1657   **+**   Zone 8F – Employee affiliation

1658   **+**   Zone 10F – Agency, Department or Organization

1659   **+**   Zone 14F – Expiration date

1660   **+**   Zone 1B – Agency card serial number (back of card)

1661   **+**   Zone 2B – Issuer identification number (back of card).

1662   The PIV Card may also bear the following optional components:

1663   **+**   Zone 11F – Agency seal

1664   **+**   Zone 5B – Physical characteristics of cardholder

1665   **+**   Zone 3F –Signature.

1666 When a cardholder attempts to pass through an access control point for a Federally controlled facility, a
1667 human guard shall perform visual identity verification of the cardholder, and determine whether the
1668 identified individual should be allowed through the control point. The series of steps that shall be applied
1669 in the visual authentication process are as follows:

1670   1.   The human guard at the access control entry point determines whether the PIV Card appears to be
1671   genuine and has not been altered in any way.

1672   2.   The guard compares the cardholder's facial features with the picture on the card to ensure that
1673   they match.

1674   3.   The guard checks the expiration date on the card to ensure that the card has not expired.

1675   4.   The guard compares the cardholder's physical characteristic descriptions to those of the
1676   cardholder. (Optional)

1677   5.   The guard collects the cardholder's signature and compares it with the signature on the card.
1678   (Optional)

1679   6.   One or more of the other data elements on the card (e.g., name, employee affiliation, agency card
1680   serial number, issuer identification, agency name) are used to determine whether the cardholder
1681   should be granted access.

1682 Some characteristics of the visual authentication mechanism are as follows:

1683   **+**   Human inspection of card, which is not amenable for rapid or high volume access control

1684   **+**   Resistant to use of unaltered card by non-owner of card

1685   **+**   Low resistance to tampering and forgery

1686   +   Applicable in environments with and without card readers.

1687 **6.2.2 Authentication Using the PIV CHUID**

1688   The PIV Card provides a mandatory logical credential called the CHUID. As described in Section 4.2,
1689   the CHUID contains numerous data elements.

1690   The CHUID shall be used for PIV cardholder authentication using the following sequence:

1691   1. The CHUID is read electronically from the PIV Card.

1692   2. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted
1693   source and is unaltered.

1694   3. The expiration date on the CHUID is checked to ensure that the card has not expired.

1695   4. A unique identifier within the CHUID is used as input to the authorization check to determine
1696   whether the cardholder should be granted access.

1697   Some characteristics of the CHUID-based authentication mechanism are as follows:

1698   +   Can be used for rapid authentication for high volume access control

1699   +   Low resistance to use of unaltered card by non-owner of card

1700   +   Applicable with contact-based and contactless readers.

1701 **6.2.3 Authentication Using PIV Biometric**

1702   The PIV Card Application hosts the signed fingerprint templates and/or the signed iris image templates.
1703   Either biometric can be read from the card following cardholder-to-card (CTC) authentication using a PIN
1704   supplied by the cardholder. These PIV biometrics are designed to support a cardholder-to-external
1705   system (CTE) authentication mechanism through a match-off-card scheme. The following subsections
1706   define two authentication schemes that make use of the PIV biometrics. As noted in Section 4.4, neither
1707   the fingerprint template nor the iris images are guaranteed to be present on a PIV Card, since it may not
1708   be possible to collect fingerprints from some cardholders and iris images are only required to be collected
1709   from cardholders whom fingerprints could not be collected. In some rare cases, a PIV Card may have
1710   neither fingerprint templates nor iris images, if neither fingerprints nor iris images could be collected from
1711   the cardholder.

1712   Some characteristics of the PIV Biometrics authentication mechanisms (described below) are as follows:

1713   +   Slower mechanism, because it requires two interactions (e.g., presentation of PIN and biometric)
1714   with the cardholder

1715   +   Strong resistance to use of unaltered card by non-owner since PIN and cardholder biometric are
1716   required

1717   +   Digital signature on biometric, which is checked to further strengthen the mechanism

1718   +   Applicable only with contact-based card readers.

6.2.3.1 Unattended Authentication Using PIV Biometric (BIO)

The following sequence shall be followed for unattended authentication of the PIV biometric:

1. The CHUID is read from the card.

2. The expiration date in the CHUID is checked to ensure the card has not expired.

3. The cardholder is prompted to submit a PIN, activating the PIV Card.

4. The PIV biometric is read from the card.

5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source.

6. The cardholder is prompted to submit a live biometric sample.

7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.

8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.

9. FASC-N is used as input to the authorization check to determine whether the cardholder should be granted access.

6.2.3.2 Attended Authentication of PIV Biometric (BIO-A)

The following sequence shall be followed for attended authentication of the PIV biometrics:

1. The CHUID is read from the card.

2. The expiration date in the CHUID is checked to ensure that the card has not expired.

3. The cardholder is prompted to submit a PIN. The PIN entry is done in the view of an attendant.

4. The submitted PIN is used to activate the card. The PIV biometric is read from the card.

5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source.

6. The cardholder is prompted to submit a live biometric sample. The biometric sample is submitted in the view of an attendant.

7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.

8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.

9. FASC-N is used as input to the authorization check to determine whether the cardholder should be granted access.

1750 This authentication mechanism is similar to the unattended biometrics authentication mechanism; the only
1751 difference is that an attendant (e.g., security guard) supervises the use of the PIV Card and the submission
1752 of the PIN and the biometric by the cardholder.

1753 **6.2.4   Authentication Using PIV Asymmetric Cryptography**

1754 The PIV Card contains two mandatory asymmetric authentication private keys and corresponding
1755 certificates, as described in Section 4. The following subsections shall be used to perform authentication
1756 using the authentication keys. The PKI-Auth shall be the alternative authentication mechanism, in cases
1757 where neither the fingerprints nor its alternative iris images could be collect for on-card storage.

1758 **6.2.4.1   Authentication with the PIV authentication certificate credential (PKI-AUTH)**

1759   1. The reader reads the PIV Authentication Key certificate from the PIV Card Application.

1760   2. The cardholder is prompted to submit a PIN.

1761   3. The submitted PIN is used to activate the card.

1762   4. The reader issues a challenge string to the card and requests an asymmetric operation in response.

1763   5. The card responds to the previously issued challenge by signing it using the PIV authentication
1764   private key.

1765   6. The response signature is verified and standards-compliant PKI path validation is conducted. The
1766   related digital certificate is checked to ensure that it is from a trusted source. The revocation
1767   status of the certificate is checked to ensure current validity.

1768   7. The response is validated as the expected response to the issued challenge.

1769   8. The Subject Distinguished Name (DN) and unique identifier from the authentication certificate
1770   are extracted and passed as input to the access control decision.

1771 Some of the characteristics of the PKI-based authentication mechanism are as follows:

1772   +   Requires the use of online certificate status checking infrastructure

1773   +   Highly resistant to credential forgery

1774   +   Strong resistance to use of unaltered card by non-owner since PIN is required to activate card

1775   +   Applicable with contact-based card readers.

1776

1777 **6.2.4.2   Authentication with the Card authentication certificate credential (PKI-CAK)**

1778   1. The reader reads the Card Authentication Key (CAK) certificate from the PIV Card Application.

1779   2. The reader issues a challenge string to the card and requests an asymmetric operation in response.

1780   3. The card responds to the previously issued challenge by signing it using the card authentication
1781   private key.

1782   4. The response signature is verified and standards-compliant PKI path validation is conducted. The
1783   related digital certificate is checked to ensure that it is from a trusted source. The revocation
1784   status of the certificate is checked to ensure current validity.

1785   5. The response is validated as the expected response to the issued challenge.

1786   6. The FASC-N from the card authentication certificate is extracted and passed as input to the
1787   access control decision.

1788   Some of the characteristics of the PKI-CAK authentication mechanism are as follows:

1789   + Requires the use of online certificate status checking infrastructure

1790   + Highly resistant to credential forgery

1791   + Applicable with contact-based and contactless readers.

1792   **6.2.5 Authentication Using On-Card Biometric Comparison**

1793 The PIV Card Application may host the optional on-card biometric comparison algorithm. In this case,
1794 fingerprint templates are stored on the card, which cannot be read, but could be used for identity
1795 verification. A live-scan biometric is supplied to the card to perform cardholder-to-card (CTC)
1796 authentication and the card with an indication of the success of the on-card biometric comparison. The
1797 response includes information that allows the reader to authenticate the card. The cardholder PIN is not
1798 required for this operation. The PIV Card shall include mechanism to block this authentication
1799 mechanism after a number of consecutive failed authentication attempts as stipulated by department or
1800 agency. As with authentication using PIV biometric, aIf agencies choose to implement On-card biometric
1801 comparison it shall be implemented as defined in [SP 800-73] and [SP 800-76].

1802   **6.2.6 Authentication with the Symmetric Card Authentication Key**

1803 The PIV Card Application may host the optional symmetric card authentication key. In this case, the
1804 symmetric card authentication key shall be used for PIV cardholder authentication using the following
1805 sequence:

1806   1. The CHUID is read electronically from the PIV Card.

1807   2. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted
1808   source and is unaltered.

1809   3. The expiration date on the CHUID is checked to ensure that the card has not expired.

1810   4. The reader issues a challenge string to the card and requests a response.

1811   5. The card responds to the previously issued challenge by signing it using the symmetric card
1812   authentication key.

1813   6. The response is validated as the expected response to the issued challenge.

1814   7. A unique identifier within the CHUID is used as input to the authorization check to determine
1815   whether the cardholder should be granted access.

6.3   PIV Support of Graduated Assurance Levels for Identity Authentication

1817 The PIV Card supports a set of authentication mechanisms that can be used to implement graduated
1818 assurance levels for identity authentication. The following subsections specify the basic PIV
1819 authentication mechanisms that may be used to support the various levels of identity authentication
1820 assurance as defined in Section 6.1. Two or more complementing identity authentication mechanisms
1821 may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder.
1822 For example, PKI-AUTH and BIO may be applied in unison to achieve a higher degree of assurance in
1823 cardholder identity.

1824 Adequately designed and implemented relying systems can achieve the PIV Card authentication
1825 assurance levels stated in Tables 6-2 and 6-3. Less adequately designed or implemented relying systems
1826 may only achieve lower authentication assurance levels. The design of components of relying systems,
1827 including card readers, biometric readers, cryptographic modules, and key management systems, involves
1828 many factors not fully specified by FIPS 201, such as correctness of the functional mechanism, physical
1829 protection of the mechanism, and environmental conditions at the authentication point. Additional
1830 standards and best practice guidelines apply to the design and implementation of relying systems, e.g.,
1831 FIPS 140 and SP 800-116.

6.3.1 Physical Access

1833 The PIV Card may be used to authenticate the identity of the cardholder in a physical access control
1834 environment. For example, a Federal facility may have physical entry doors that have human guards at
1835 checkpoints, or may have electronic access control points. The PIV-supported authentication mechanisms
1836 for physical access control systems are summarized in Table 6-2. An authentication mechanism that is
1837 suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance
1838 level.

Table 6-2. Authentication for Physical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
SOME confidence	VIS, CHUID, PKI-CAK
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, PKI-AUTH

6.3.2 Logical Access

1848 The PIV Card may be used to authenticate the cardholder in support of decisions concerning access to
1849 logical information resources. For example, a cardholder may log in to his or her department or agency
1850 network using the PIV Card; the identity established through this authentication process can be used for
1851 determining access to file systems, databases, and other services available on the network.

1852 Table 6-3 describes the authentication mechanisms defined for this standard to support logical access
1853 control. An authentication mechanism that is suitable for a higher assurance level can also be applied to
1854 meet the requirements for a lower assurance level.

1855

Table 6-3. Authentication for Logical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism	
	Local Workstation Environment	Remote/Network System Environment
SOME confidence	CHUID, PKI-CAK	PKI-CAK
HIGH confidence	BIO	
VERY HIGH confidence	BIO-A, PKI-AUTH	PKI-AUTH

1856

Appendix A—PIV Validation, Certification, and Accreditation

A.1   Accreditation of PIV Card Issuers (PCI)

[HSPD-12] requires that all cards be issued by providers whose reliability has been established by an official accreditation process. To that end, NIST developed a set of attributes as the basis of reliability assessment of PIV Card Issuers (PCIs) in SP 800-79 and published this document in July 2005. Subsequent lessons learned in implementation experience (in credential management and PIV Card issuance) of various agencies together with the evolution of PCI organizations motivated NIST to develop a new accreditation methodology that is objective, efficient, and will result in consistent and repeatable accreditation decisions and published the substantial revision as SP 800-79-1 in June 2008 [SP 800-79]. The new PCI accreditation methodology is built on a foundation of four major Accreditation Topics, 13 Accreditation Focus Areas and a total of 79 Control requirements distributed under the various Accreditation Focus Areas. Associated with each control requirement are a set of assessment methods, the exercise of the latter will result in outcomes that form the basis for accreditation decisions.

The four major Accreditation Topics identified in [SP 800-79] are:

+   Organizational Preparedness

+   Security Management and Data Protection

+   Infrastructure Elements

+   (PIV) Processes

The entire spectrum of activities in the PCI accreditation methodology is divided into the following four phases:

+   Initiation Phase

+   Assessment Phase

+   Accreditation Phase

+   Monitoring Phase

The initiation phase involves communicating the goals of the assessment/accreditation to the key personnel of the PCI organization and the review of documents such as the PCI operations plan. In the assessment phase, the appropriate assessment methods stipulated in the methodology for each PCI control are carried out and the individual results recorded. The accreditation phase involves aggregating the results of assessment, arriving at an accreditation decision, and issuing the appropriate notification – Authorization to Operate (ATO) or the Denial of Authorization to Operate (DATO), that is consistent with the accreditation decision.

A.2   Security Certification and Accreditation of IT System(s) Supporting PCI

The accreditation of the capability and reliability of a PCI using the methodology outlined in [SP 800-79] depends upon adequate security for the information systems that are used for PCI functions. The assurance that such a security exists in a PCI is obtained through security certification and accreditation of IT systems performed using the methodology specified in SP 800-37. [SP 800-37] The methodology in

1893 [SP 800-37] in turn was created in pursuant to a mandate in Appendix III of Office of Management and
1894 Budget (OMB) Circular A-130. An accreditation decision granted under [SP 800-37] signifies that a PCI
1895 organization's official accepts responsibility for the security (in terms of confidentiality, integrity, and
1896 availability of information) of the information systems that will be involved in carrying out the PCI
1897 functions. Hence accreditation under [SP 800-37] is mandatory for issuing PCI accreditation using SP
1898 800-79.

1899 **A.3   Conformance of PIV Card Application and Middleware Testing to Specifications**
1900   **Based on this Standard**

1901 Assurance of conformance of the PIV Card Application and PIV Middleware interfaces to this standard
1902 and its associated technical specifications is needed in order to meet the security and interoperability
1903 goals of HSPD-12. To facilitate this, NIST has established the NIST Personal Identity Verification
1904 Program (NPIVP). Under this program NIST has developed test procedures in SP 800-85A, *PIV Card*
1905 *Application and Middleware Interface Test Guidelines (SP800-73 compliance)*, and an associated toolkit
1906 for conformance testing of PIV Card Application and PIV Middleware. [SP 800-85A] Commercial
1907 products under these two categories are tested by the set of accredited test laboratories, accredited under
1908 National Voluntary Laboratory Accreditation Program (NVLAP) program, using the NIST supplied test
1909 procedures and toolkit. The outcomes of the test results are validated by NIST, which then issues
1910 validation certificates. Information about NPIVP is available at
1911 http://csrc.nist.gov/groups/SNS/piv/npivp.

1912
1913 **A.4   Cryptographic Testing and Validation (FIPS 140 and algorithm standards)**

1914 All on-card cryptographic modules hosting the PIV Card Application and cryptographic modules of Card
1915 Issuance and Maintenance Systems shall be validated to FIPS 140 with an overall Security Level 2 (or
1916 higher). [FIPS140-2] The facilities for FIPS 140 testing are the Cryptographic and Security Testing
1917 (CST) laboratories accredited by the NVLAP program of NIST. Vendors wanting to supply
1918 cryptographic modules can select any of the accredited laboratories. The tests conducted by these
1919 laboratories for all vendor submissions are validated and a validation certificate for each vendor module is
1920 issued by the Cryptographic Module Validation Program (CMVP), a joint program run by NIST and
1921 Communications Security Establishment (CSE) of the Government of Canada. The details of the CMVP
1922 and NVLAP programs and the list of CMT laboratories can be found at the CMVP Web site at
1923 http://csrc.nist.gov/groups/STM/index.html.

1924 **A.5   FIPS 201 Evaluation Program**

1925 In order to evaluate the conformance of different families of products that support the PIV processes to
1926 this standard and its associated technical specifications, the Office of Government-wide Policy (OGP)
1927 under GSA set up the FIPS 201 Evaluation Program. The product families include Card Personalization
1928 products, Card Readers, Products involved in Credential enrollment functions such as Fingerprint and
1929 Facial Image Capture equipments, Biometric fingerprint template generators etc. Products evaluated and
1930 approved under this program are placed on the FIPS 201 Approved Products List (APL) to enable
1931 procurement of conformant products by implementing agencies. The details of the program are available
1932 at http://fips201ep.cio.gov/.

1933

1934 ## Appendix B—Background Check Descriptions

1935 The following describes the details of a National Agency Check with Inquiries (NACI).

1936   **+**   **NACI.** The basic and minimum investigation required on all new Federal employees consisting
1937 of a National Agency Check (NAC) with written inquiries and searches of records covering
1938 specific areas of an individual's background during the past five years (inquiries sent to current
1939 and past employers, schools attended, references, and local law enforcement authorities).
1940 Coverage includes:

1941   – Employment, 5 years

1942   – Education, 5 years and highest degree verified

1943   – Residence, 3 years

1944   – References

1945   – Law Enforcement, 5 years

1946   – NACs

1947 **Appendix C—PIV Card Processes**

1948 The following table is a summary of the requirements described in Section 2.4 and Section 2.5. The
1949 summary is provided as an overview of the requirements and is only intend to be a quick reference.

1950

FIPS 201-2 Card Processes and Their Requirements							
	Issuance	Maintenance					
	Issuance	Renewal		Reissuance		Re-Key	Post Issuance Updates
		Data Change	No Data Change	Data Change	No Data Change		
Sponsor Approval	●	●	●	● (if expiration date is extended)	● (if expiration date is extended)		
Identity Proofing	●						
Biometric Collection	●	Good for 12 years	Good for 12 years	Good for 12 years	Good for 12 years		
Enroll in Chain-of-trust	●	Record change		Record change			
NCHC	●						
NACI	●	●	●	● (if expiration date is extended)	● (if expiration date is extended)		
Chain-of-trust verification (CV)	●	●	●	●	●		● (if biometric data change)
Valid PIV Card in Possession		●	●	● (unless lost/stolen)		●	●
New Physical Card issued (new FASC-N)	●	●	●	●	●		
Re-enrollment if CV not available		●	●	●	●		
Expiration Date	Maximum 6 yrs	Maximum 6 yrs	Maximum 6 yrs	Maximum 6 yrs	Maximum 6 yrs	No Change	No Change

1951

Appendix D—PIV Object Identifiers and Certificate Extension

1953 **D.1   PIV Object Identifiers**

1954 Table D-1 lists details for PIV object identifiers.

1955   **Table D-1. PIV Object Identifiers**

ID	Object Identifier	Description
PIV eContent Types		
id-PIV-CHUIDSecurityObject	2.16.840.1.101.3.6.1	The associated content is the concatenated contents of the CHUID, excluding the authentication key map and the asymmetric signature field.
id-PIV-biometricObject	2.16.840.1.101.3.6.2	The associated content is the concatenated CBEFF_HEADER + STD_BIOMETRIC_RECORD.
PIV Attributes		
pivCardholder-Name	2.16.840.1.101.3.6.3	The attribute value is of type DirectoryString and specifies the PIV cardholder's name.
pivCardholder-DN	2.16.840.1.101.3.6.4	The attribute value is an X.501 type Name and specifies the DN associated with the PIV cardholder in the PIV certificate(s).
pivSigner-DN	2.16.840.1.101.3.6.5	The attribute value is an X.501 type Name and specifies the subject name that appears in the PKI certificate for the entity that signed the biometric or CHUID.
pivFASC-N	2.16.840.1.101.3.6.6	The pivFASC-N OID may appear as a name type in the otherName field of the subjectAltName extension of X.509 certificates or a signed attribute in CMS external signatures. Where used as a name type, the syntax is OCTET STRING. Where used as an attribute, the attribute value is of type OCTET STRING. In each case, the value specifies the FASC-N of the PIV Card.
PIV Extended Key Usage		
id-PIV-content-signing	2.16.840.1.101.3.6.7	This specifies that the public key may be used to verify signatures on PIV CHUIDs and PIV biometrics.
id-PIV-cardAuth	2.16.840.1.101.3.6.8	This specifies that the public key is used to authenticate the PIV Card rather than the PIV cardholder.

1956
1957 **D.2   PIV Certificate Extension**

1958 The PIV NACI indicator is a non-critical extension that may appear in PIV authentication certificates and
1959 card authentication certificates. The PIV NACI indicator extension indicates the status of the subject's
1960 background investigation at the time of credential issuance. The value of this extension is asserted as
1961 follows:

1962   +   TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint
1963   Check has completed successfully, and (2) a NACI has been initiated but has not completed.

1964   +   FALSE if, at the time of credential issuance, the subject's NACI has been completed and
1965   successfully adjudicated.

1966 The PIV NACI indicator extension is identified by the id-piv-NACI object identifier. The syntax for this
1967 extension is defined by the following ASN.1 module.

1968

```
1969     PIV-Cert-Extensions { 2 16 840 1 101 3 6 10 1  }
1970
1971     DEFINITIONS EXPLICIT TAGS ::=
1972
1973     BEGIN
1974
1975     -- EXPORTS ALL --
1976
1977     -- IMPORTS NONE --
1978
1979     id-piv-NACI OBJECT IDENTIFIER  ::= { 2 16 840 1 101 3 6 9 1 }
1980
1981     NACI-indicator ::= BOOLEAN
1982
1983     END
1984
```

1985 **Appendix E—Glossary of Terms, Acronyms, and Notations**

1986 **E.1 Glossary of Terms**

1987 The following terms are used throughout this standard.

1988 **Access Control:** The process of granting or denying specific requests: 1) obtain and use information and
1989 related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings,
1990 military establishments, border crossing entrances).

1991 **Applicant:** An individual applying for a PIV Card/credential. The Applicant may be a current or
1992 prospective Federal hire, a Federal employee, or a contractor.

1993 **Application:** A hardware/software system implemented to satisfy a particular set of requirements. In
1994 this context, an application incorporates a system used to satisfy a subset of requirements related to the
1995 verification or identification of an end user's identity so that the end user's identifier can be used to
1996 facilitate the end user's interaction with the system.

1997 **Approved:** FIPS approved or NIST recommended. An algorithm or technique that is either (1) specified
1998 in a FIPS or a NIST recommendation or (2) adopted in a FIPS or NIST recommendation.

1999 **Architecture:** A highly structured specification of an acceptable approach within a framework for
2000 solving a specific problem. An architecture contains descriptions of all the components of a selected,
2001 acceptable solution while allowing certain details of specific components to be variable to satisfy related
2002 constraints (e.g., costs, local environment, user acceptability).

2003 **Assurance Level (or E-Authentication Assurance Level):** A measure of trust or confidence in an
2004 authentication mechanism defined in OMB Memorandum M-04-04 and NIST Special Publication (SP)
2005 800-63, in terms of four levels: [M-04-04]

2006 • Level 1: LITTLE OR NO confidence

2007 • Level 2: SOME confidence

2008 • Level 3: HIGH confidence

2009 • Level 4: VERY HIGH confidence

2010 **Asymmetric Keys:** Two related keys, a public key and a private key, that are used to perform
2011 complementary operations, such as encryption and decryption or signature generation and signature
2012 verification.

2013 **Authentication:** The process of establishing confidence of authenticity; in this case, in the validity of a
2014 person's identity and the PIV Card.

2015 **Biometric:** A measurable, physical characteristic or personal behavioral trait used to recognize the
2016 identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris scan samples
2017 are all examples of biometrics.

2018 **Biometric Information:** The stored electronic information pertaining to a biometric. This information
2019 can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns).

2020 **Biometric System:** An automated system capable of the following:

2021   **+**   Capturing a biometric sample from an end user

2022   **+**   Extracting biometric data from that sample

2023   **+**   Comparing the extracted biometric data with data contained in one or more references

2024   **+**   Deciding how well they match

2025   **+**   Indicating whether or not an identification or verification of identity has been achieved.

2026   **Capture:** The method of taking a biometric sample from an end user. [INCITS/M1-040211]

2027   **Cardholder:** An individual possessing an issued PIV Card.

2028   **Certificate Revocation List:** A list of revoked public key certificates created and digitally signed by a
2029   Certification Authority. [RFC 5280]

2030   **Certification:** The process of verifying the correctness of a statement or claim and issuing a certificate as
2031   to its correctness.

2032   **Certification Authority:** A trusted entity that issues and revokes public key certificates.

2033   **Chain-of-trust:** The chain-of-trust is a sequence of related enrollment data sets that is created and
2034   maintained by PIV Card issuers.

2035   **Claimant:** A party whose identity is to be verified using an authentication protocol.

2036   **Comparison:** The process of comparing a biometric with a previously stored reference. See also
2037   "Identification" and "Identity Verification". [INCITS/M1-040211]

2038   **Component:** An element of a large system, such as an identity card, PIV Issuer, PIV Registrar, card
2039   reader, or identity verification support, within the PIV system.

2040   **Conformance Testing:** A process established by NIST within its responsibilities of developing,
2041   promulgating, and supporting FIPS for testing specific characteristics of components, products, and
2042   services, as well as people and organizations for compliance with a FIPS.

2043   **Credential:** Evidence attesting to one's right to credit or authority; in this standard, it is the PIV Card
2044   and data elements associated with an individual that authoritatively binds an identity (and, optionally,
2045   additional attributes) to that individual.

2046   **Cryptographic Key (Key):** A parameter used in conjunction with a cryptographic algorithm that
2047   determines the specific operation of that algorithm.

2048   **Enrollment data set:** A record including information about a biometric enrollment: name and role of the
2049   acquiring agent, office and organization, time, place, and acquisition method.

2050   **Federal Agency Smart Credential Number (FASC-N):** As required by FIPS 201, the primary
2051   identifier on the PIV Card for physical access control. The FASC-N is a fixed length (25 byte) data
2052   object, specified in [SP 800-73], and included in several data objects on a PIV Card.

2053 **FASC-N Identifier:** The FASC-N shall be in accordance with [SP 800-73]. A subset of FASC-N, a
2054 FASC-N Identifier, is a unique identifier as described in [SP 800-73].

2055 **Federal Information Processing Standards (FIPS):** A standard for adoption and use by Federal
2056 departments and agencies that has been developed within the Information Technology Laboratory and
2057 published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in
2058 information technology to achieve a common level of quality or some level of interoperability.

2059 **Framework:** A structured description of a topic of interest, including a detailed statement of the
2060 problem(s) to be solved and the goal(s) to be achieved. An annotated outline of all the issues that must be
2061 addressed while developing acceptable solutions to the problem(s). A description and analysis of the
2062 constraints that must be satisfied by an acceptable solution and detailed specifications of acceptable
2063 approaches to solving the problems(s).

2064 **Graduated Security:** A security system that provides several levels (e.g., low, moderate, high) of
2065 protection based on threats, risks, available technology, support services, time, human concerns, and
2066 economics.

2067 **Hash Function:** A function that maps a bit string of arbitrary length to a fixed length bit string.
2068 Approved hash functions satisfy the following properties:

2069 1. **One-Way.** It is computationally infeasible to find any input that maps to any pre-specified
2070 output.

2071 2. **Collision Resistant.** It is computationally infeasible to find any two distinct inputs that map to
2072 the same output.

2073 **Identification:** The process of discovering the true identity (i.e., origin, initial history) of a person or
2074 item from the entire collection of similar persons or items.

2075 **Identifier:** Unique data used to represent a person's identity and associated attributes. A name or a card
2076 number are examples of identifiers.

2077 **Identity:** The set of physical and behavioral characteristics by which an individual is uniquely
2078 recognizable.

2079 **Identity Authentication Assurance Level:** A degree of confidence established in the identity of the
2080 holder of the PIV Card.

2081 **Identity Binding** – Binding of the vetted claimed identity to the individual (through biometrics)
2082 according to the issuing authority. Represented by an identity assertion from the issuer that is carried by a
2083 *PIV credential.*

2084 **Identity Management System (IDMS)** – Identity management system comprised of one or more
2085 systems or applications that manages the identity verification, validation, and issuance process.

2086 **Identity Proofing:** The process of providing sufficient information (e.g., identity history, credentials,
2087 documents) to a PIV Registrar when attempting to establish an identity.

2088 **Identity Registration:** The process of making a person's identity known to the PIV system, associating a
2089 unique identifier with that identity, and collecting and recording the person's relevant attributes into the
2090 system.

2091   **Identity Verification:** The process of confirming or denying that a claimed identity is correct by
2092   comparing the credentials (something you know, something you have, something you are) of a person
2093   requesting access with those previously proven and stored in the PIV Card or system and associated with
2094   the identity being claimed.

2095   **Information in Identifiable Form (IIF):** Any representation of information that permits the identity of
2096   an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
2097   [E-Gov]

2098   **Interoperability:** For the purposes of this standard, interoperability allows any government facility or
2099   information system, regardless of the PIV Issuer, to verify a cardholder's identity using the credentials on
2100   the PIV Card.

2101   **Issuer:** The organization that is issuing the PIV Card to an Applicant. Typically this is an organization
2102   for which the Applicant is working.

2103   **Key:** See "Cryptographic Key".

2104   **Match/Matching:** The process of comparing biometric information against a previously stored biometric
2105   data and scoring the level of similarity.

2106   **Model:** A very detailed description or scaled representation of one component of a larger system that can
2107   be created, operated, and analyzed to predict actual operational characteristics of the final produced
2108   component.

2109   **Off-Card:** Refers to data that is not stored within the PIV Card or to a computation that is not performed
2110   by the Integrated Circuit Chip (ICC) of the PIV Card.

2111   **On-Card:** Refers to data that is stored within the PIV Card or to a computation that is performed by the
2112   Integrated Circuit Chip (ICC) of the PIV Card.

2113   **One-to-Many:** Synonym for "Identification". [INCITS/M1-040211]

2114   **Online Certificate Status Protocol (OCSP):** An online protocol used to determine the status of a public
2115   key certificate. [RFC 2560]

2116   **Path Validation:** The process of verifying the binding between the subject identifier and subject public
2117   key in a certificate, based on the public key of a trust anchor, through the validation of a chain of
2118   certificates that begins with a certificate issued by the trust anchor and ends with the target certificate.
2119   Successful path validation provides strong evidence that the information in the target certificate is
2120   trustworthy.

2121   **Personal Identification Number (PIN):** A secret that a claimant memorizes and uses to authenticate his
2122   or her identity.

2123   **Personal Identity Verification (PIV) Card:** A physical artifact (e.g., identity card, "smart" card) issued
2124   to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized
2125   fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored
2126   credentials by another person (human readable and verifiable) or an automated process (computer
2127   readable and verifiable).

2128 **PIV Issuer:** An authorized identity card creator that procures FIPS-approved blank identity cards,
2129 initializes them with appropriate software and data elements for the requested identity verification and
2130 access control application, personalizes the cards with the identity credentials of the authorized subjects,
2131 and delivers the personalized cards to the authorized subjects along with appropriate instructions for
2132 protection and use.

2133 **PIV Registrar:** An entity that establishes and vouches for the identity of an Applicant to a PIV Issuer.
2134 The PIV Registrar authenticates the Applicant's identity by checking identity source documents and
2135 identity proofing, and ensures a proper background check has been completed, before the credential is
2136 issued.

2137 **PIV Sponsor:** An individual who can act on behalf of a department or agency to request a PIV Card for
2138 an Applicant.

2139 **Population:** The set of users for the application. [INCITS/M1-040211]

2140 **Pseudonyms:** a name assigned by a Federal Department or Agency through a formal process to a Federal
2141 employee for the purpose of the employee's protection (i.e., the employee might be placed at risk if their
2142 actual name were known) or for other purposes.

2143 **Public Key:** The public part of an asymmetric key pair that is typically used to verify signatures or
2144 encrypt data.

2145 **Public Key Infrastructure (PKI):** A support service to the PIV system that provides the cryptographic
2146 keys needed to perform digital signature-based identity verification and to protect communications and
2147 storage of sensitive verification system data within identity cards and the verification system.

2148 **PKI-Card Authentication Key (PKI-CAK):** A PIV authentication mechanism that is implemented by
2149 an asymmetric key challenge/response protocol using the Card authentication key of the PIV card and a
2150 contact or contactless reader.

2151 **PKI-PIV Authentication Key (PKI-AUTH):** A PIV authentication mechanism that is implemented by
2152 an asymmetric key challenge/response protocol using the PIV authentication key of the PIV card and a
2153 contact reader.

2154 **Recommendation:** A special publication of the ITL stipulating specific characteristics of technology to
2155 use or procedures to follow to achieve a common level of quality or level of interoperability.

2156 **Reference Implementation:** An implementation of a FIPS or a recommendation available from
2157 NIST/ITL for demonstrating proof of concept, implementation methods, technology utilization, and
2158 operational feasibility.

2159 **Registration:** See "Identity Registration".

2160 **Secret Key:** A cryptographic key that must be protected from unauthorized disclosure to protect data
2161 encrypted with the key. The use of the term "secret" in this context does not imply a classification level;
2162 rather, the term implies the need to protect the key from disclosure or substitution.

2163 **Standard:** A published statement on a topic specifying the characteristics, usually measurable, that must
2164 be satisfied or achieved to comply with the standard.

2165 **Trustworthiness** – Security decision with respect to extended investigations to determine and confirm
2166 qualifications, and suitability to perform specific tasks and responsibilities.

2167 **Validation:** The process of demonstrating that the system under consideration meets in all respects the
2168 specification of that system. [INCITS/M1-040211]

2169 **Verification:** See "Identity Verification".

2170
2171 **E.2   Acronyms**

2172 The following acronyms and abbreviations are used throughout this standard:

2173	**ACL**	Access Control List
2174	**AES**	Advanced Encryption Standard
2175	**AIA**	Authority Information Access
2176	**AIM**	Association for Automatic Identification and Mobility
2177	**ANSI**	American National Standards Institute
2178		
2179	**CA**	Certification Authority
2180	**CAK**	**Card Authentication Key**
2181	**CBEFF**	Common Biometric Exchange Formats Framework
2182	**CFR**	Code of Federal Regulations
2183	**CHUID**	Cardholder Unique Identifier
2184	**CMS**	Cryptographic Message Syntax
2185	**CMT**	Cryptographic Module Testing
2186	**CMTC**	Card Management System to the Card
2187	**CMVP**	Cryptographic Module Validation Program
2188	**COTS**	Commercial Off-the-Shelf
2189	**CRL**	Certificate Revocation List
2190	**CSE**	Communication Security Establishment
2191	**CTC**	Cardholder to Card
2192	**CTE**	Cardholder to External System
2193	**CVS**	Clearance Verification System
2194		
2195	**DHS**	Department of Homeland Security
2196	**DN**	Distinguished Name
2197	**dpi**	Dots Per Inch
2198		
2199	**ECC**	Elliptic Curve Cryptography
2200	**ERT**	Emergency Response Team
2201		
2202	**FASC-N**	Federal Agency Smart Credential Number
2203	**FBCA**	Federal Bridge Certification Authority
2204	**FBI**	Federal Bureau of Investigation
2205	**FICC**	Federal Identity Credentialing Committee
2206	**FIPS**	Federal Information Processing Standards
2207	**FIPS PUB**	FIPS Publication
2208	**FISMA**	Federal Information Security Management Act
2209		
2210	**HSPD**	Homeland Security Presidential Directive

2211	**HTTP**	Hypertext Transfer Protocol
2212		
2213	**I&A**	Identification and Authentication
2214	**IAB**	Interagency Advisory Board
2215	**ICC**	Integrated Circuit Chip
2216	**ID**	Identification
2217	**IDMS**	Identity Management System
2218	**IEC**	International Electrotechnical Commission
2219	**IETF**	Internet Engineering Task Force
2220	**IIF**	Information in Identifiable Form
2221	**INCITS**	International Committee for Information Technology Standards
2222	**ISO**	International Organization for Standardization
2223	**IT**	Information Technology
2224	**ITL**	Information Technology Laboratory
2225		
2226	**LDAP**	Lightweight Directory Access Protocol
2227		
2228	**NAC**	National Agency Check
2229	**NACI**	National Agency Check with Inquiries
2230	**NCHC**	National Criminal History Check
2231	**NIST**	National Institute of Standards and Technology
2232	**NISTIR**	National Institute of Standards and Technology Interagency Report
2233	**NPIVP**	NIST Personal Identity Verification Program
2234	**NVLAP**	National Voluntary Laboratory Accreditation Program
2235		
2236	**OCSP**	Online Certificate Status Protocol
2237	**OID**	Object Identifier
2238	**OMB**	Office of Management and Budget
2239	**OPM**	Office of Personnel Management
2240		
2241	**PCI**	PIV Card Issuer
2242	**PC/SC**	Personal Computer/Smart Card
2243	**PDF**	Portable Data File
2244	**PIA**	Privacy Impact Assessment
2245	**PIN**	Personal Identification Number
2246	**PIV**	Personal Identity Verification
2247	**PKI**	Public Key Infrastructure
2248		
2249	**RFC**	Request for Comments
2250	**RSA**	Rivest Shamir Adleman
2251		
2252	**SAVE**	Systematic Alien Verification for Entitlements
2253	**SF**	Standard Form
2254	**SP**	Special Publication
2255		
2256	**TSA**	Transportation Security Administration
2257		
2258	**USCIS**	U.S. Citizenship and Immigration Services
2259		

2260 **E.3   Notations**

2261   This standard uses the following typographical conventions in text:

2262   **+**   ASN.1 data types are represented in *italics*. For example, *SignedData* and *SignerInfo* are data
2263   types defined for digital signatures.

2264   **+**   Letters or words in CAPITALS separated with underscore represent CBEFF-compliant data
2265   structures. For example, CBEFF_HEADER is a header field in the CBEFF structure.

2266

Appendix F—References

[ANSI322] ANSI INCITS 322 Information Technology, *Card Durability Test Methods*, ANSI, 2002.

[CBEFF] NISTIR 6529-A, *Common Biometric Exchange Formats Framework (CBEFF)*, NIST, 2003.

[COMMON] *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Version 3647 – 1.12, October 15, 2010, or as amended. Available at http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf.

[E-Gov] *E-Government Act of 2002,* U.S. Public Law 107-347, 2002.

[EO10450] Executive Order 10450, *Security Requirements for Government Employees*, April 17, 1953. Available at http://www.dss.mil/nf/adr/10450/eo10450T.htm.

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

[G155-00] ASTM G155-00, *Standard Practice for Operating Xenon Arc Light Apparatus for Exposure of Non-metallic Materials*, Vol. 14.04, ASTM, July 2000.

[G90-98] ASTM G90-98, *Standard Practice for Performing Accelerated Outdoor Weathering of Non-metallic Materials Using Concentrated Natural Sunlight*, Vol. 14.04, ASTM, 2003.

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

[INCITS/M1-040211] ANSI/INCITS M1-040211, *Biometric Profile—Interoperability and Data Interchange—Biometrics-Based Verification and Identification of Transportation Workers*, ANSI, April 2004.

[ISO10373] ISO/IEC 10373, *Identification Cards—Test Methods.* Part 1—*Standard for General Characteristic Test of Identification Cards*, ISO, 1998. Part 3—*Standard for Integrated Circuit Cards with Contacts and Related Interface Devices*, ISO, 2001. Part 6—*Standard for Proximity Card Support in Identification Cards*, ISO, 2001.

[ISO14443] ISO/IEC 14443-1:2000, *Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards*, ISO, 2000.

[ISO7810] ISO/IEC 7810:2003, *Identification Cards—Physical Characteristics*, ISO, 2003.

[ISO7816] ISO/IEC 7816, *Identification Cards—Integrated Circuits with Contacts*, Parts 1-6, ISO.

[MRTD] International Civil Aviation Organization. *PKI for Machine Readable Travel Documents offering ICC Read-Only Access.* Version – 1.1, October 2004.

2302 [NISTIR7123] NISTIR 7123, *Fingerprint Vendor Technology Evaluation 2003: Summary of*
2303 *Results and Analysis Report*, NIST, June 2004.

2304 [OMB322] OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of*
2305 *the E-Government Act of 2002*, OMB, September 26, 2003.

2306 [OMB404] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies,*
2307 OMB, December 2003.

2308 [PCSC] Personal Computer/Smart Card Workgroup Specifications. Available at
2309 http://www.pcscworkgroup.com.

2310 [PRIVACY] *Privacy Act of 1974*, U.S. Public Law 93-579, 1974.

2311 [PROF] *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the*
2312 *Shared Service Provider (SSP) Program*, Version 1.5, January 7, 2008 or as amended. Available
2313 at http://www.idmanagement.gov/fpkipa/documents/CertCRLprofileForCP.pdf.

2314 [RFC2560] RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status*
2315 *Protocol - OCSP*, Internet Engineering Task Force (IETF), June 1999. Available at
2316 http://www.ietf.org/rfc/rfc2560.txt.

2317 [RFC5280] RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate*
2318 *Revocation List (CRL) Profile*, IETF, May 2008. Available at http://www.ietf.org/rfc/rfc5280.txt.

2319 [RFC5652] RFC 5652, *Cryptographic Message Syntax (CMS)*, IETF, September 2009. Available
2320 at http://www.ietf.org/rfc/rfc5652.txt.

2321 [SP 800-37] NIST Special Publication 800-37-1, *Guide for Applying the Risk Management*
2322 *Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST, February
2323 2010 or as amended.

2324 [SP 800-53] NIST Special Publication 800-53-3, *Recommended Security Controls for Federal*
2325 *Information Systems and Organizations*, NIST, August 2009 or as amended.

2326 [SP 800-63] NIST Special Publication 800-63 Version 1.0.2, *Electronic Authentication*
2327 *Guideline,* Appendix A, NIST, April 2006 or as amended.

2328 [SP 800-73] NIST Special Publication 800-73-3, *Interfaces for Personal Identity Verification*,
2329 NIST, February 2010 or as amended.

2330 [SP 800-76] NIST Special Publication 800-76-1, *Biometric Data Specification for Personal*
2331 *Identity Verification*, NIST, January 2007 or as amended

2332 [SP 800-78] NIST Special Publication 800-78-2, *Cryptographic Algorithms and Key Sizes for*
2333 *Personal Identity Verification,* NIST, February 2010 or amended.

2334 [SP 800-79] NIST Special Publication 800-79-1, *Guidelines for the Accreditation of Personal*
2335 *Identity Verification Card Issuers,* NIST, June 2008 or amended.

2336 [SP 800-85A] NIST Special Publication 800-85A-2, *PIV Card Application and Middleware*
2337 *Interface Test Guidelines (SP800-73-3 compliance),* NIST, August 2010 or amended.

2338   [SP 800-87] NIST Special Publication 800-87 Revision 1, *Codes for the Identification of Federal*
2339   *and Federally-Assisted Organizations,* NIST, April 2008 or amended.

2340   [SP 800-96] NIST Special Publication 800-96, *PIV Card to Reader Interoperability Guidelines,*
2341   NIST, September 2006 or amended.

2342   [SP 800-116] NIST Special Publication 800-116, *A Recommendation for the use of PIV*
2343   *Credentials in Physical Access Control Systems (PACS),* NIST, November 2008 or amended.

2344   [SP 800-122] NIST Special Publication 800-122, Guide to Protecting the Confidentiality of
2345   Personally Identifiable Information (PII)*,* NIST, April 2010 or amended.

2346   [SPRINGER MEMO] Final Credentialing Standards for Issuing Personal Identity Verification
2347   Cards under HSPD-12, July 31, 2008.

2348   [SSP REP] Shared Service Provider Repository Service Requirements, June 28, 2007, or as
2349   amended. Available at
2350   http://www.idmanagement.gov/fpkipa/documents/SSPrepositoryRqmts.pdf.

2351
2352

2353

Appendix G—Revision History

2354

2355   The Revision History is a complete list of updates to FIPS 201 since its initial release.

Version	Release Date	Updates
FIPS 201	February 2005	Initial Release
FIPS 201-1	March 2006	Added the requirement for electronically distinguishable from identity credentials issued to individuals who have a completed investigation (NACI Indictor).
FIPS 201-1 Change Notice 1	March 2006	Added clarification for variable placement of Agency Card Serial Number along the outer edge of the back of the PIV Card is allowed. Also, updated ASN.1 encoding for NACI Indicator.
FIPS 201-2, Draft	March 2011	This version represents 5 year review of FISP 201 and change request inputs received from agencies. Following is the highlights of changes made in this version.
		Incorporated reference to the memo by Linda Springer, Director OPM, dated 31 Jul 2008 for Credentialing Requirements.
		Incorporated the content from the I-9 form that is relevant to FIPS 201.
		Introduced the concept of a "chain-of-trust" maintained by a PIV Card Issuer. The "chain-of-trust" allows the owner of a PIV Card to obtain a replacement for a compromised, lost, stolen, or damaged PIV Card through biometric authentication.
		Changed the maximum life of PIV Card from 5 years to 6 years.
		Introduced a special rule for pseudonyms.
		Introduced a grace period for the period between termination of an employee or contractor and re-employment by the US Government or a USG Federal contractor.
		Revised the PIV Card Issuance and Maintenance requirements based on above changes.
		Added requirements for post-issuance updates.
		Incorporated visual card topography zones and color specifications from SP 800-104 and added clarifications to some of the existing zones.
		Added optional requirements for Section 508 compliance.
		Introduced requirement to collect alternate iris images when an agency cannot capture reliable fingerprints.
		Made asymmetric card authentication key mandatory and symmetric card authentication key optional.
		Added optional On-card biometric comparison as a means of performing card activation and PIV authentication mechanism.
		Inserted hook for additional keys if they are needed for

		secure messaging.
		Modified card activation to allow for PIN or equivalent verification data (e.g., biometric data).
		Added an option to include country(ies) of citizenship of Foreign Nationals in the PIV Authentication Certificate.
		Require signature verification and certificate path validation in the CHUID, BIO, and BIO-A authentication mechanisms.
		Added support for On-card Biometric Comparison
		Removed Annex A which provided two examples of PIV Processes.

2356

2357