

---

3 **A Recommendation for the Use of PIV**  
4 **Credentials in Physical Access Control**  
5 **Systems (PACS)**

---

7 Hildegard Ferraiolo  
8 David Cooper  
9 Nabil Ghadiali  
10 Jason Mohler  
11 Vincent Johnson  
12 Steven Brady

13  
14  
15 This publication is available free of charge  
16  
17  
18

---

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

---

22 **Draft NIST Special Publication 800-116**  
23 **Revision 1**

24  
25 **A Recommendation for the Use of PIV**  
26 **Credentials in Physical Access Control**  
27 **Systems (PACS)**

28 Hildegard Ferraiolo  
29 David Cooper  
30 *Computer Security Division*  
31 *Information Technology Laboratory*

32  
33 Nabil Ghadiali  
34 *National Gallery of Art*  
35 *Washington, DC*

36  
37 Jason Mohler  
38 Vincent Johnson  
39 Steven Brady  
40 *Electrosoft Services, Inc.*  
41 *Reston, Virginia*

42  
43 This publication is available free of charge

44  
45  
46 December 2015  
47



48  
49  
50 U.S. Department of Commerce  
51 Penny Pritzker, Secretary

52  
53 National Institute of Standards and Technology  
54 Willie May, Under Secretary of Commerce for Standards and Technology and Director

55

**Authority**

56 This publication has been developed by NIST in accordance with its statutory responsibilities under the  
57 Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law  
58 (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines,  
59 including minimum requirements for federal information systems, but such standards and guidelines shall  
60 not apply to national security systems without the express approval of appropriate federal officials  
61 exercising policy authority over such systems. This guideline is consistent with the requirements of the  
62 Office of Management and Budget (OMB) Circular A-130.

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

69 National Institute of Standards and Technology Special Publication 800-116 Revision 1  
70 Natl. Inst. Stand. Technol. Spec. Publ. 800-116 Revision 1, 85 pages (December 2015)  
71 CODEN: NSPUE2

72 This publication is available free of charge  
73

74 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an  
75 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or  
76 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best  
77 available for the purpose.

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

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

87 **Public comment period: *December 28, 2015 through February 1, 2016***

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

89 National Institute of Standards and Technology  
90 Attn: Computer Security Division, Information Technology Laboratory  
91 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930  
92 Email: [piv\\_comments@nist.gov](mailto:piv_comments@nist.gov)

93

94

## Reports on Computer Systems Technology

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

105

### Abstract

106 This recommendation provides a technical guideline to use Personal Identity Verification (PIV)  
107 Cards in physical access control systems (PACS); enabling federal agencies to operate as  
108 government-wide interoperable enterprises. This recommendation covers the risk-based strategy  
109 to select appropriate PIV authentication mechanisms as expressed within [\[FIPS201\]](#).

110

111

112

### Keywords

113 credential; e-authentication; identity assurance level; identity credential; issuance; PACS; PIV  
114 authentication mechanisms; PIV cards; PKI; validation

115

116

## Acknowledgements

117 The authors of SP 800-116 Revision 1 (Hildegard Ferraiolo and David Cooper of NIST; Nabil  
118 Ghadiali of the National Gallery of Art; and Jason Mohler, Vincent Johnson, and Steven Brady  
119 of Electrosoft Services, Inc.) wish to thank William MacGregor, Ketan Mehta, and Karen  
120 Scarfone for their substantial contribution towards the original version of this publication. The  
121 authors also gratefully acknowledge and appreciate the support and contributions by many others  
122 in the public and private sectors whose helpful and beneficial comments greatly enhance the  
123 utility of this publication. Special thanks to the Interagency Security Committee (ISC), the  
124 General Services Administration, the Department of Homeland Security, the Department of  
125 Defense, and the Office of Management and Budget for their review and contributions to this  
126 document.

127

128

129

## Audience

130 This document is intended for government officials responsible for implementing Homeland  
131 Security Presidential Directive-12 (HSPD-12) compliant physical access control systems  
132 (PACS). This document will also aid government executives (i.e., decision makers) in evaluating  
133 business cases and developing strategies for their departments or agencies. Information in this  
134 document is also useful to government contractors and physical security vendors that provide  
135 HSPD-12 systems, products, and integration services.

136

## 137 **Executive Summary**

138 Prior to Homeland Security Presidential Directive-12 [\[HSPD-12\]](#), the physical access control  
139 systems (PACS) deployed in many federal buildings were facility-centric rather than enterprise-  
140 centric and utilized proprietary PACS architectures. Therefore, many issued identification (ID)  
141 cards operated only with the PACS for which they were issued. The technologies used in these  
142 systems typically offered little or no authentication assurance, because the issued ID cards could  
143 be easily cloned or counterfeited. Many agencies continue to operate legacy PACS systems. In  
144 addition to the lack of interoperability, these PACS technologies present the following  
145 challenges:

- 146 + Scalability. Some legacy systems are limited in their capability to process the longer  
147 credential numbers necessary for government-wide interoperability.
- 148 + Security. Legacy PACS readers can read an identifying number from a card, but in  
149 most cases they do not perform a cryptographic challenge/response exchange. Most  
150 bar code, magnetic stripe, and proximity cards can be copied easily. The technologies  
151 used in these systems offer little or no authentication assurance.
- 152 + Validity. Legacy PACS control expiration of credentials through an expiration date  
153 stored in a site database. There is no simple way to synchronize the expiration or  
154 revocation of credentials for a federal employee or contractor across multiple sites.
- 155 + Efficiency. Use of personal identification numbers (PIN), public key infrastructure,  
156 and biometrics with some deployed PACS are managed on a site-specific basis.  
157 Individuals must enroll PINs, keys, and biometrics at each site. Since PINs, keys, and  
158 biometrics are often stored in a site database, they may not be technically  
159 interoperable with PACS at other sites.

160 [\[HSPD-12\]](#) sets a clear goal to improve PACS through the use of government-wide standards.  
161 Federal Information Processing Standard 201 [\[FIPS201\]](#) defines characteristics of the identity  
162 credential that can be interoperable government-wide. In the context of [\[HSPD-12\]](#), the term  
163 *interoperability* means the ability to use any Personal Identity Verification (PIV) Card with any  
164 application performing one or more PIV authentication mechanisms. [\[FIPS201\]](#) defines  
165 authentication mechanisms at four E-Authentication assurance levels (LITTLE or NO, SOME,  
166 HIGH, and VERY HIGH), and standardizes optional credential elements that extend trust in the  
167 PIV System to functions beyond authentication. A gap remains, however, between the concepts  
168 of authentication assurance levels and their application in many PACS environments. To close  
169 this gap, this document:

- 170 + Discusses the different PIV Card capabilities so that the risk-based assessment can be  
171 aligned with the appropriate PIV authentication mechanism.
- 172 + Uses the concept of “Controlled, Limited, Exclusion” areas to employ risk-based PIV  
173 authentication mechanisms for different areas within a facility.
- 174 + Proposes a PIV Implementation Maturity Model (PIMM) to measure the progress of  
175 facility and agency implementations.

176 + Recommends to federal agencies an overall strategy for the implementation of PIV  
 177 authentication mechanisms with agency facility PACS.

178 Since the areas accessible via different access points within a facility do not all have the same  
 179 security requirement, the PIV authentication mechanisms selected should be consistent with, and  
 180 integral to, the overall security requirements of the protected area. A single facility may need  
 181 multiple authentication mechanisms. Therefore, the designation of “Controlled, Limited,  
 182 Exclusion” areas, detailed in [Section 5.3](#), is applied to the protected area. Specifically, this  
 183 document recommends PIV authentication mechanisms for “Controlled, Limited, Exclusion” in  
 184 terms of authentication factors as shown in [Table ES-1](#). Some agencies may have different  
 185 names for their security areas, however each agency should establish their criteria to implement  
 186 authentication consistent with this document.

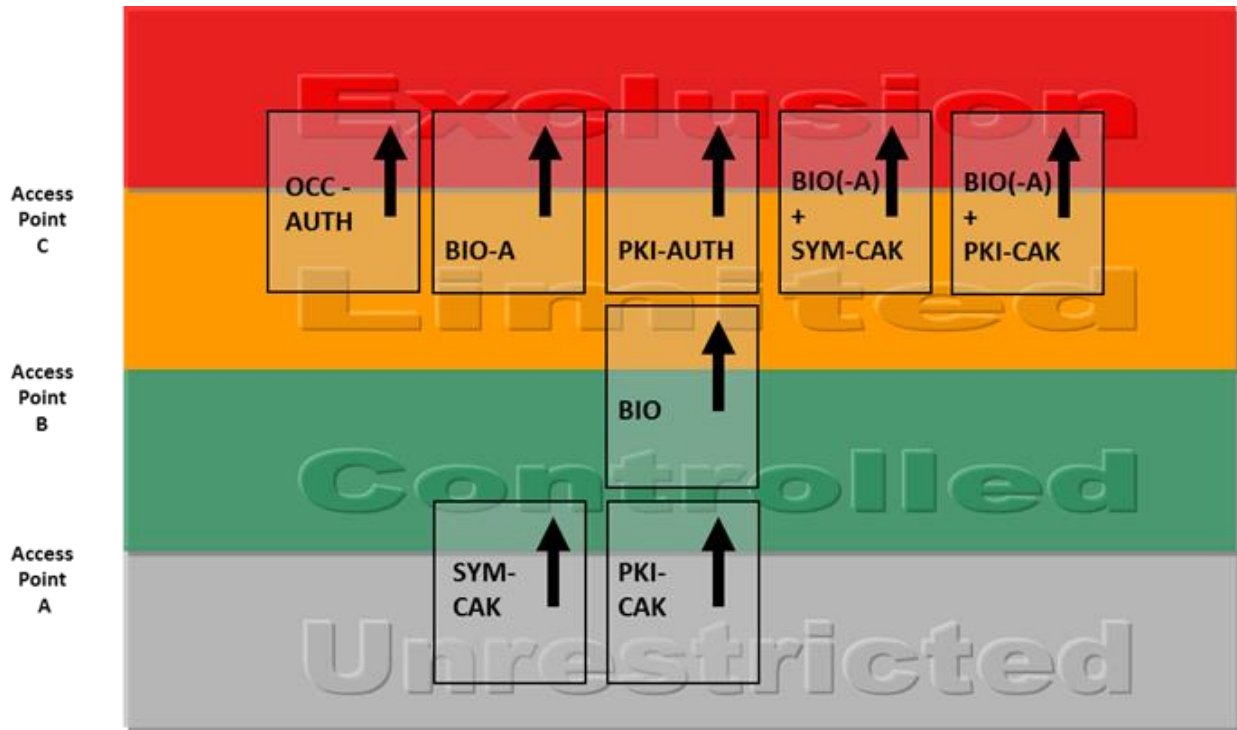
Security Areas	Number of Authentication Factors Required
Controlled	1
Limited	2
Exclusion	3

187

**Table ES-1 - Authentication Factors for Security Areas**

188 PIV authentication mechanisms should be implemented in accordance with [Table ES-1](#). [Figure](#)  
 189 [ES-1](#) illustrates the innermost perimeter at which each PIV authentication mechanism may be  
 190 used based on the authentication assurance level of the mechanism. The combined effect of  
 191 [Table ES-1](#) and [Figure ES-1](#) determines exactly what mechanisms may be used (see [Section 5.3](#)).  
 192 An exhaustive list of possible uses of PIV authentication mechanisms against protected areas is  
 193 provided in [Appendix D](#).

194 [\[FIPS201\]](#) identifies a number of authentication mechanisms supported by mandatory features of  
 195 PIV Cards. These mechanisms include Authentication using PIV Visual Credentials (VIS),  
 196 Authentication using the Cardholder Unique Identifier (CHUID), Authentication with the Card  
 197 Authentication Certificate Credential (PKI-CAK), Authentication Using Off-Card Biometric  
 198 Comparison (BIO), Attended Authentication Using Off-Card Biometric Comparison (BIO-A),  
 199 and Authentication with the PIV Authentication Certificate Credential (PKI-AUTH). In addition,  
 200 PIV Cards may optionally support a number of other authentication mechanisms; these include  
 201 Authentication with the Symmetric Card Authentication Key (SYM-CAK) and Authentication  
 202 Using On-Card Biometric Comparison (OCC-AUTH). Access points should not rely solely on an  
 203 authentication mechanism that requires optional card features as it is not guaranteed that the  
 204 optional features to be used for authentication are present on all cards. Both the authentication  
 205 mechanisms that are supported by all PIV Cards and the authentication mechanisms that require  
 206 optional card capabilities are described in [Section 5](#).



207

208

**Figure ES- 1: Innermost Use of PIV Authentication Mechanisms**

209

A risk-based migration strategy should be planned and implemented to achieve PIV enabling. This document recommends a model that allows agencies to incrementally PIV-enable access points. The model is defined in terms of maturity levels as follows:

210

211

212

+ Maturity Level 1—Ad hoc PIV verification.

213

+ Maturity Level 2—Systematic PIV verification to Controlled areas. PIV Cards and currently deployed non-PIV PACS cards are accepted for access to the Controlled areas at this level.

214

215

216

+ Maturity Level 3—Access to Exclusion areas by PIV or exception only. Non-PIV cards are not accepted for access to the Exclusion areas at this level.

217

218

+ Maturity Level 4—Access to Limited areas by PIV or exception only. Non-PIV cards are not accepted for access to the Limited or Exclusion areas at this level.

219

220

+ Maturity Level 5—Access to Controlled areas by PIV or exception only. Non-PIV cards are not accepted for access to any areas at this level.

221

222



223

**Table of Contents**

224	<b>1. Introduction.....</b>	<b>1</b>
225	1.1 Background.....	1
226	1.2 Purpose and Scope.....	2
227	<b>2. Threat Environment .....</b>	<b>4</b>
228	2.1 Identifier Collisions .....	4
229	2.2 Revoked PIV Cards .....	5
230	2.3 Visual Counterfeiting .....	5
231	2.4 Skimming.....	6
232	2.5 Sniffing .....	6
233	2.6 Social Engineering.....	7
234	2.7 Electronic Cloning.....	7
235	2.8 Electronic Counterfeiting .....	8
236	2.9 Other Threats .....	8
237	<b>3. Limitations of Legacy Physical Access Control Systems.....</b>	<b>9</b>
238	3.1 Cardholder Identification.....	9
239	3.2 Door Reader Interface .....	9
240	3.3 Authentication Capability.....	9
241	3.4 Wiring.....	10
242	3.5 Software Upgrades .....	10
243	3.6 Legacy PACS Cards and PIV Card Differences .....	11
244	<b>4. The PIV Vision .....</b>	<b>12</b>
245	4.1 Interoperability .....	12
246	4.2 Qualities of the Complete Implementation.....	14
247	4.3 Benefits of the Complete Implementation.....	15
248	4.4 Infrastructure Requirements .....	16
249	<b>5. PIV Authentication Mechanisms.....</b>	<b>18</b>
250	5.1 Authentication Factors.....	18
251	5.1.1 Authentication using PIV Visual Credentials (VIS).....	20
252	5.1.2 Authentication using the Cardholder Unique Identifier (CHUID) .....	20
253	5.1.3 Authentication with the Card Authentication Certificate (PKI-CAK) .....	21
254	5.1.4 Authentication with the Symmetric Card Authentication Key (SYM-CAK). 21	
255	5.1.5 Unattended Authentication Using Off-Card Biometric Comparison (BIO)... 21	

289           5.1.6   Attended Authentication Using Off-Card Biometric Comparison (BIO-A)... 22

290           5.1.7   Authentication with the PIV Authentication Certificate (PKI-AUTH) ..... 22

291 |         5.1.8   Authentication Using On-Card Biometric Comparison (OCC-AUTH) ..... 23

292           5.1.9   (PKI-CAK | SYM-CAK) + BIO(-A) Authentication..... 23

293         5.2   Multi-Factor Authentication .....23

294 |         5.3   Selection of PIV Authentication Mechanisms..... 24

295           5.3.1   Migrating Away from the Legacy CHUID Authentication Mechanism ..... 28

296         5.4   PIV Identifiers .....30

297         5.5   PACS Registration.....31

298         5.6   Credential Validation and Path Validation .....32

299         5.7   Lost PIV Card or Suspicion of Fraudulent Use .....34

300   **6.   PACS Use Cases ..... 35**

301         6.1   Single-Tenant Facility .....36

302         6.2   Multi-Tenant Facility.....36

303         6.3   Mixed-Multi-Tenant Facility .....37

304         6.4   Single-Tenant Campus .....38

305           6.4.1   FSL I or II Campus Facility ..... 38

306           6.4.2   FSL III Campus Facility ..... 39

307           6.4.3   FSL IV or V Campus Facility ..... 40

308         6.5   Multi-Tenant Campus.....40

309         6.6   Role-Based Access Control .....41

310         6.7   Temporary Badges.....41

311         6.8   Disaster Response and Recovery Incidents .....42

312   **7.   Migration Strategy ..... 43**

313         7.1   Project Planning.....43

314         7.2   Risk Assessment .....43

315         7.3   Business and Functional Requirements .....44

316         7.4   Develop Migration Plan.....44

317         7.5   Migration Strategy & Tactics .....45

318         7.6   PIV Implementation Maturity Model (PIMM).....46

319         7.7   PIV-in-PACS Best Practices .....47

Deleted

Deleted

353 **List of Appendices**

354 **Appendix A— Improving Authentication Transaction Times ..... 49**

355 **Appendix B— Recommendations..... 51**

356 **Appendix C— FASC-N Uniqueness..... 55**

357     C.1 Full FASC-N Comparison .....55

358     C.2 FASC-N Identifier Comparison.....57

359     C.3 Partial FASC-N Comparison .....57

360     C.4 Isomorphic FASC-N Comparison .....58

361 **Appendix D— Possible PIV Authentication Mechanisms in PACS..... 59**

362 **Appendix E— References..... 62**

363 **Appendix F— Terminology ..... 65**

364 **Appendix G— Abbreviations and Acronyms ..... 73**

365

366 **List of Figures**

367 Figure 5-1: Innermost Use of PIV Authentication Mechanisms ..... 25

368 Figure 5-2: Examples of Mapping PIV Authentication Mechanisms..... 27

369 Figure 6-1: Single-Tenant Facility ..... 36

370 Figure 6-2: Multi-Tenant Facility ..... 37

371 Figure 6-3: FSL I or II Campus Facility ..... 39

372 Figure 6-4: FSL III Campus Facility ..... 39

373 Figure 6-5: FSL IV or V Campus Facility ..... 40

374 Figure 7-1: Migration Strategy ..... 43

375

376 **List of Tables**

377 | Table 5-1 - PIV Authentication Mechanisms on the Contact Interface ..... 20

378 | Table 5-2 - PIV Authentication Mechanisms on the Contactless Interface ..... 20

379 | Table 5-3 - Authentication Factors for Security Areas ..... 25

380 | Table 5-4 - PIV Identifiers ..... 30

381

Deleted

Deleted

## 384 1. Introduction

### 385 1.1 Background

386 Homeland Security Presidential Directive-12 [\[HSPD-12\]](#) mandated the establishment of a  
387 government-wide standard for identity credentials to improve physical security in federally-  
388 controlled facilities.<sup>1</sup> To that end, [\[HSPD-12\]](#) required all government employees and contractors  
389 be issued a new identity credential based on [\[FIPS201\]](#), *Personal Identity Verification (PIV) for*  
390 *Federal Employees and Contractors*. Following [\[FIPS201\]](#), this credential is referred to herein as  
391 the PIV Card.<sup>2</sup>

392 [\[HSPD-12\]](#) explicitly requires the use of PIV credentials “in gaining physical access to  
393 Federally-controlled facilities and logical access to Federally-controlled information systems.”  
394 The PIV Card employs microprocessor-based smart card technology, and is designed to be  
395 counterfeit-resistant, tamper-resistant, and interoperable across Federal Government facilities.  
396 Additionally, the [\[FIPS201\]](#) standards suite defines the authentication mechanisms as  
397 transactions between a PIV Card and a relying party. [\[FIPS201\]](#) does not, however, elaborate on  
398 the uses and applications of the PIV Card. This document provides guidelines on the uses of PIV  
399 Cards with physical access control systems (PACS).

400 Legacy PACS technologies deployed in some federal buildings are facility-centric rather than  
401 enterprise-centric and often utilize proprietary PACS architectures. Historically, a security  
402 advantage was seen in not having the design of the security system published or readily  
403 accommodating substitution. For this and other reasons, many legacy PACS are not  
404 interoperable. Moreover, lack of agency card technology standards and use of local credential  
405 numbering systems are key factors that limit interoperability of legacy PACS across agencies. In  
406 other words, an identity credential issued for use with one legacy PACS may not have the  
407 capability to be used by another. To enhance security and promote interoperability, it is essential  
408 to develop an efficient and cost-effective strategy to migrate legacy PACS to standardized  
409 methods as defined in [\[FIPS201\]](#). The application of cryptographic authentication and integrity  
410 methods allows the security of authentication to be improved, the design of authentication to rely  
411 on open standards, and the need for secrecy regarding authentication to be concentrated on  
412 cryptographic keys.

413 Full compliance with [\[HSPD-12\]](#), and the use of PIV authentication mechanisms for access to  
414 federal facilities and systems as required by [\[HSPD-12\]](#), should be the principal goals of a  
415 department or agency implementation plan. Recognizing that implementation will take time,  
416 migration goals and plans should be developed to PIV-enable PACS installations, while meeting  
417 continuity of operations and resource constraints. Plans may include change management  
418 strategies such as:

419 + Retrofit or upgrade the existing PACS to use PIV Cards.

---

<sup>1</sup> Federally controlled facilities as defined in Section 1D of OMB Memorandum [\[M-05-24\]](#)

<sup>2</sup> Federal agencies may refer to PIV Cards by other names, for example, “Common Access Cards (CAC),” “LincPass,” “identity badges,” or “access cards.” In this document, all such credentials issued by an accredited PIV Card Issuer are called PIV Cards.

420 + Coexistence of PIV-enabled and existing PACS in leased multi-tenant facilities.

## 421 **1.2 Purpose and Scope**

422 The purpose of this document is to describe a strategy allowing agencies to PIV-enable their  
 423 PACS, and migrate to government-wide interoperability. Specifically, the document  
 424 recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to  
 425 manage physical access to Federal Government facilities and assets. With the intent to facilitate  
 426 and encourage greater use of PIV Cards, this document:

427 + Describes the desired characteristics of a target implementation of PIV-enabled PACS.

428 + Describes trust and infrastructure challenges that must be overcome to achieve  
 429 government-wide credential interoperability.

430 + Discusses the PIV Card capabilities so that a risk-based assessment can be aligned with  
 431 the appropriate PIV authentication mechanism.

432 + Recommends to federal agencies an overall strategy for the implementation of PIV  
 433 authentication mechanisms with agency facility PACS.

434 + Proposes a PIV Implementation Maturity Model (PIMM) to measure the progress of  
 435 facility and agency implementations.

436 As stated above, this document focuses on the use of PIV Cards to gain access to federal  
 437 buildings and facilities. This document does not address non-PIV authentication mechanisms.

438 Although the ergonomic design of PACS components is outside the scope of this publication, the  
 439 1998 Amendment to Section 508 of the Rehabilitation Act has special relevance to PACS  
 440 components [\[SECTION508\]](#). PACS access controls are intended to be unavoidable.  
 441 [\[SECTION508\]](#) should be considered early during projects that integrate the PIV System with  
 442 PACS. [\[SECTION508\]](#) should be considered as it applies to enrollment software, smart card and  
 443 biometric readers, monitoring systems, and access control point sensors and actuators. Note  
 444 [\[FIPS201\]](#), Section 6.2.1 footnote 31, states “when biometric authentication cannot be  
 445 performed, PKI-AUTH is the recommended alternate authentication mechanism.” Further  
 446 information can be found at [\[SECTION508\]](#), in [\[FIPS201\]](#), and in [\[SP800-76\]](#), *Biometric*  
 447 *Specifications for Personal Identity Verification*.

448 Many other aspects of physical access control are outside the scope of this publication.  
 449 Authorization (i.e., granting permission within a PACS for an identified person to pass access  
 450 control points) is a critical security function, but is out of scope for the PIV System. Other out-  
 451 of-scope functions include area protection, intrusion detection, egress, monitoring and tracking  
 452 (other than at access control points), and enforcement of access control decisions. It is  
 453 understood that PACS may also be integrated with surveillance systems, fire control systems,  
 454 evacuation systems, etc., within a facility. This document does not address the integration of  
 455 PACS with other facility-centric information technology (IT) systems, although it has been  
 456 written to minimize conflicts during such integration. Therefore, if the integration of the  
 457 measures outlined in this document creates a life-safety risk, organizations will need to mitigate  
 458 these risks before applying the measures.

459 The evaluation of specific PACS architectures or implementations is also outside the scope of  
460 this publication, as is the standardization of PACS. The creation of specific migration plans for  
461 each agency and facility is also not the intent of this document, although it offers advice on the  
462 construction of such plans. Unless normatively referenced, this document is a best practice  
463 guideline.

464 **Recommendation 1.1:** This document recommends a risk-based approach for  
465 selecting appropriate PIV authentication mechanisms to manage physical access to  
466 Federal Government facilities and assets. Agencies should seek recommendations  
467 on PACS architectures, authorization, and facility protection from other sources.

## 468 **2. Threat Environment**

469 The PIV System is intended to enhance security and trust in identity credentials, but no practical  
470 system can guarantee perfect security. This section discusses known technical threats to PIV  
471 authentication mechanisms, especially the CHUID authentication mechanism, which has been  
472 downgraded in [\[FIPS201\]](#) to indicate that it provides “LITTLE or NO” confidence in the identity  
473 of the cardholder because of these threats. Methods of attack are described in general terms, and  
474 this is not an exhaustive list of possible attacks. Attackers often succeed by exploiting  
475 overlooked or newly introduced vulnerabilities in operational systems.

476 The PIV System protects the trustworthiness of the PIV Card data objects through PIV Card  
477 access rules and digital signatures. Overall trust in the execution of a PIV authentication  
478 mechanism is also dependent on correct operation of the PIV Card, the PACS, and the PIV Card  
479 validation infrastructure, and, to a degree, on protecting the confidentiality, integrity, and  
480 availability of the communication channels among them. Attacks may, therefore, be directed  
481 against any of these components, with varying difficulty and potential impact.

482 The factors critical to sustained trust in the PIV System are:

- 483 + The strength of cryptographic operations.
- 484 + The protection of private and secret keys by system components.
- 485 + The successful decryption and/or signature verification of data objects at expected  
486 times.
- 487 + The continuous implementation of access rules by the PIV Card.
- 488 + The dependable operation of other system elements in the PIV System and the PACS.

489 To execute a PIV authentication mechanism, the cardholder presents his or her card to the PACS.  
490 The presentation of the PIV Card occurs outside the security perimeter to which access is  
491 requested. When the presentation occurs at the outermost perimeter of a facility, the cardholder is  
492 in an Unrestricted area, and various technical attacks on PACS are easily carried out. Special  
493 security precautions must be taken to ensure protection of these devices at the outermost  
494 perimeters of the facility. Even at interior perimeters, the degree of protection provided by  
495 enclosing perimeters may be modest when the means of attack can be easily concealed. Possible  
496 attack vectors include identifier collisions, revoked PIV Cards, visual counterfeiting, skimming,  
497 sniffing, social engineering, electronic cloning, and electronic counterfeiting. These methods of  
498 attack, as well as others, are discussed below.

### 499 **2.1 Identifier Collisions**

500 By definition, a unique identifier for a PIV Card is a data artifact with a fixed value unique to  
501 one particular PIV Card. PIV Card Issuers (PCIs) create unique identifiers during the card  
502 issuance process. The presence of unique identifiers allows a PIV Card to be uniquely identified  
503 by a relying system, such as a PACS. If the unique identifier is ever truncated, compressed,  
504 hashed, or modified, information could be lost. If information is lost from the unique identifier  
505 before it is compared against access control list (ACL) entries, multiple cards may generate the

506 same reduced identifier. This is called an *identifier collision*. A collision means that multiple PIV  
507 Cards will appear to belong to the same person, and will all be granted the same access  
508 privileges.

509 *The PIV Card mitigates the risk of collision by defining a unique FASC-N Identifier for*  
510 *the purposes of physical access control decisions. To prevent collisions, all access*  
511 *control decisions based on the FASC-N should be made by comparing the 14 decimal*  
512 *digit FASC-N Identifier, and optionally the values of additional FASC-N fields, against*  
513 *the ACL entries. [\[FIPS201\]](#) added the mandatory Card UUID, which is also a unique*  
514 *identifier that can be used reliably in access control decisions. See [Section 5.4](#) for PIV*  
515 *identifiers.*

## 516 **2.2 Revoked PIV Cards**

517 PIV Cards may be revoked for a number of reasons, including a lost or stolen card. A revoked  
518 PIV Card could continue to open doors with the CHUID authentication mechanism long after the  
519 card has been revoked. As described in [\[FIPS201\]](#), the check for revocation should be performed  
520 by a status check, using either the Online Certificate Status Protocol (OCSP) or certificate  
521 revocation lists (CRL), on the PIV Authentication certificate or the Card Authentication  
522 certificate. Credential validation (see [Section 5.5](#)) is required by [\[FIPS201\]](#) for all PIV  
523 authentication mechanisms, however, validation of the CHUID and biometric credentials do not  
524 include a revocation check. If a PIV Card is reported as lost and then revoked by the issuer, a  
525 PACS relying on the CHUID authentication mechanism will continue to accept the CHUID until  
526 the user is de-authorized in each of those systems. If a PACS caches the status of PIV Cards, the  
527 cached status of a revoked PIV Card will remain “valid” until the cache is refreshed. The process  
528 for PACS de-authorization is not required or defined by [\[FIPS201\]](#), raising the possibility that  
529 online credential validation may not be implemented, or not effectively implemented, where the  
530 CHUID authentication mechanism is employed.

531 *The PIV System mitigates the risk of use of a misappropriated PIV Card (which has been*  
532 *successfully reported and revoked) through the process of credential validation. Section*  
533 *5.5 of [\[FIPS201\]](#) states that “the presence of a valid, unexpired, and unrevoked*  
534 *authentication certificate on a card is proof that the card was issued and is not revoked.”*  
535 *In the CHUID authentication mechanism, only the CHUID data object is read from the*  
536 *PIV Card, and a reader cannot check the status of a PIV Authentication certificate on the*  
537 *basis of the CHUID alone. Therefore, it is recommended that path validation of the PIV*  
538 *Authentication certificate or the Card Authentication certificate be done at PIV*  
539 *registration, and periodically repeated by the PACS as long as registration is maintained.*  
540 *Implementation methods are further discussed in [Section 5.5](#) and [Section 5.6](#).*

## 541 **2.3 Visual Counterfeiting**

542 PIV Cards used in the VIS authentication mechanism are visually inspected by a security guard.  
543 A visual counterfeit mimics the appearance, but not the electronic behavior, of an actual PIV  
544 Card. A PIV replica may be created by color photocopying or graphic illustration methods and  
545 color printing to blank stock. Because of the required presence of one or more security features  
546 on the PIV Card, a visual counterfeit is unlikely to pass close examination, provided guards are  
547 trained to recognize security features. However, ID cards may receive only cursory examination



548 when used as “flash passes.”

549 *The PIV Card mitigates the risk of visual counterfeiting through its capability for rapid*  
550 *electronic authentication, and to a lesser degree, by the presence of one or more security*  
551 *features on the surface of the card. Given the ready availability of high-quality scanners,*  
552 *graphic editing software, card stock, and smart card printers, electronic verification is*  
553 *strongly recommended, either in place of the VIS authentication mechanism or in*  
554 *combination with it. (Note that [\[FIPS201\]](#) downgraded the VIS Authentication mechanism*  
555 *to indicate that it provides “LITTLE or NO” confidence in the identity of the cardholder.)*

## 556 **2.4 Skimming**

557 A contactless PIV Card reader with a sensitive antenna can be concealed in a briefcase, and is  
558 capable of reading [\[ISO/IEC 14443\]](#) contactless smart cards like the PIV Card at a distance of at  
559 least 25 cm, as demonstrated in [\[SKIMMER\]](#). The range of a skimmer is limited primarily by the  
560 requirement for the skimmer to supply power to the PIV Card by inductive coupling. A  
561 concealed skimmer could immediately obtain the free-read data from the PIV Card through the  
562 contactless interface. [\[FIPS201\]](#) introduced the concept of an optional virtual contact interface  
563 (VCI), which allows all data on the PIV Card that is not protected by a PIN to be read once this  
564 interface is established. [\[SP 800-73\]](#), *Interfaces for Personal Identity Verification*, specifies an  
565 optional pairing code that can be used to authenticate the card reader to a PIV Card before the  
566 card establishes a VCI session. If agencies deploy PIV Cards that support establishing a VCI  
567 without requiring the submission of a pairing code, all data on these cards that is not protected by  
568 a PIN is vulnerable to skimming.

569 *The PIV Card mitigates the risk of skimming by implementing access rules that prevent the*  
570 *release of biometric and other data over the contactless interface when a VCI has not been*  
571 *established, by requiring the use of a pairing code in order to establish a VCI. The risk of*  
572 *skimming can also be mitigated by employing shielding techniques that positively*  
573 *deactivate the PIV Card when not in use. The electromagnetically opaque holder*  
574 *mentioned in Section 2.11 of [\[FIPS201\]](#) is one such technique.*

## 575 **2.5 Sniffing**

576 When a PIV Card is presented to a contactless reader at an access point, the reader supplies  
577 power to the PIV Card through inductive coupling and a series of messages is exchanged  
578 between the PIV Card and reader using radio frequency (RF) communications. A sniffer is a  
579 passive receiver that does not supply power to the smart card. A sniffer can operate at greater  
580 distance than a skimmer (sniffing at a distance of about 10 m has been reported), because a  
581 legitimate reader powers the PIV Card at the nominal distance of a few centimeters, while the  
582 sniffer’s RF receiver is farther away. Potentially, a sniffer could capture the entire message  
583 transaction between the contactless reader and the PIV Card.

584 *The PIV Card mitigates the risk of sniffing by the same access rules that prevent the*  
585 *release of biometric and other data over the contactless interface. The CHUID can be*  
586 *sniffed, however, when used over a contactless interface. Shielding techniques that*  
587 *positively deactivate a PIV Card when not in use cannot mitigate the risk of sniffing,*  
588 *because a PIV Card must be activated to perform a legitimate authentication transaction.*

589 *When a PIV Card that supports secure messaging<sup>3</sup> communicates with a contactless card*  
590 *reader, the card reader can leverage the secure channel, which would protect data objects*  
591 *being read from the risk of a sniffing attack.*

## 592 **2.6 Social Engineering**

593 If an attacker persuaded the cardholder to give them possession of the PIV Card, the attacker  
594 could quickly copy all of the information that was not protected by the PIN. An attacker could  
595 also attempt a remote attack similar to well-known phishing attacks by creating a web page that  
596 asks the subject to “insert PIV Card and enter PIN” for an apparently legitimate purpose. If the  
597 cardholder complies, under some assumptions the attacker could capture the cardholder’s PIN  
598 and all of the PIV data objects.

599 *The PIV Card mitigates the risk of social engineering attacks by blocking the release of all*  
600 *private and secret keys, and by requiring two-factor authentication (PIV Card and PIN) to*  
601 *perform cryptographic operations with the PIV Authentication key. Moreover, the PIV*  
602 *Card is blocked upon exceeding the allocated number of bad PIN tries. Additional*  
603 *technical and procedural controls may be needed to counter PIV phishing.*

## 604 **2.7 Electronic Cloning**

605 If an attacker has successfully conducted a skimming, sniffing, or social engineering attack, he or  
606 she possesses verbatim copies of some of the data objects from an issued PIV Card. The objects  
607 that are signed (e.g., the certificates and CHUID) retain their signatures, and the signatures are  
608 valid if the original card is valid. The attacks described, however, cannot copy the private or  
609 secret keys needed for cryptographic authentication methods. The attacker is thus able to create a  
610 partial clone of the PIV Card that would succeed in a CHUID authentication, but is not able to  
611 create a clone that would succeed in the PKI-CAK or PKI-AUTH authentication mechanisms.

612 *The PIV Card mitigates the risk of electronic cloning by providing alternative*  
613 *authentication mechanisms. It is strongly recommended that agencies use an*  
614 *authentication mechanism other than the CHUID authentication mechanism (e.g., PKI-*  
615 *CAK), since [\[FIPS201\]](#) deprecates the use of the CHUID authentication mechanism as it*  
616 *provides ‘LITTLE or NO’ confidence in the identity of the cardholder. Relying systems*  
617 *currently implementing the CHUID authentication mechanism should phase out the*  
618 *mechanism as soon as possible.<sup>4</sup> See [Section 5.3.1](#) for recommendations on a transition*  
619 *strategy.*

---

<sup>3</sup> Secure messaging is an optional mechanism specified in [\[SP 800-73\]](#) that provides confidentiality and integrity protection for the card commands that are sent to the card as well as for the responses received from the PIV Card.

<sup>4</sup> Using the transition strategies described in [Section 5.3.1](#) will result in use of the CHUID authentication mechanism being gradually decreased until it is entirely eliminated by September 2019 once all valid PIV Cards issued without Card Authentication certificates have completed their five-year life cycle and have been replaced with cards containing Card Authentication certificates.

## 620 **2.8 Electronic Counterfeiting**

621 An attacker could construct a battery-powered, microprocessor-based device that emulates a PIV  
622 Card for purposes of the CHUID authentication mechanism. The attacker could program the  
623 microprocessor to generate and test CHUIDs repetitively against a PACS reader, changing the  
624 FASC-N credential identifier on each trial. This approach would not require prior capture of a  
625 valid CHUID, but since the counterfeit CHUIDs would not possess valid issuer signatures, a  
626 successful exploit depends on the absence of signature verification in the CHUID processing  
627 done by the reader.

628 *The PIV Card mitigates the risk of electronic counterfeiting by storing a CHUID with a*  
629 *digital signature field. Electronic counterfeiting will be extremely difficult if CHUID*  
630 *signature verification is performed as required in [\[FIPS201\]](#). Moreover, since many*  
631 *CHUIDs may be presented while an attacker probes for a valid CHUID, the PACS should*  
632 *employ methods to detect, alarm, and block repeated unsuccessful CHUID presentations.*

## 633 **2.9 Other Threats**

634 The PIV and PACS systems are complex, and this brief discussion has focused on properties of  
635 the PIV Card. A number of other attack vectors have not been discussed in detail, including  
636 sophisticated technical attacks against the integrity of the PIV Card, PIV System, or PACS  
637 components, and cryptanalysis of the PIV cryptographic algorithms. While the impact of  
638 successful attacks such as these could be moderate to high, the probability of success is believed  
639 to be extremely low.

640 **Recommendation 2.1:** *This section emphasizes the technical risks associated with*  
641 *the legacy CHUID authentication mechanism. If the CHUID authentication*  
642 *mechanism is used without restriction, operational risk increases as the value of*  
643 *targets and the availability of cloning and counterfeiting tools increase. [\[FIPS201\]](#)*  
644 *deprecates the use of the CHUID authentication mechanism since it provides*  
645 *'LITTLE or NO' confidence in the identity of the cardholder, and so relying systems*  
646 *should phase out use of this authentication mechanism as soon as possible. NIST*  
647 *recommends transitioning away from the CHUID authentication mechanism using*  
648 *the strategy described in [Section 5.3.1](#).*

649

### 650 **3. Limitations of Legacy Physical Access Control Systems**

651 [\[FIPS201\]](#) and its supporting special publications impose specific requirements on PACS  
652 interfaces with PIV Card and PIV System. These requirements will present technical challenges  
653 in migrating to PIV Card use in the areas of cardholder identification, card-to-reader interface,  
654 and authentication protocol. The following sections explore how [\[FIPS201\]](#) requirements differ  
655 from the capabilities of PACS that are not PIV-enabled.

#### 656 **3.1 Cardholder Identification**

657 Legacy PACS use cards with data formats that are often proprietary to the specific enterprise.  
658 Many of the legacy PACS use an ID number based on a 26-bit standard, which is comprised of  
659 an 8-bit site code and a 16-bit unique card ID number with 2 bits assigned to parity (the parity  
660 bits add confidence that the data transmission has no errors). The 8-bit site code accommodates  
661 256 unique sites and the 16-bit card ID number accommodates 65 536 unique users for that site.  
662 Larger ID numbers are used by some legacy systems but they are not necessarily interoperable.

663 A PACS based on the 26-bit format is deployed as a standalone solution at a dedicated site.  
664 Typically, these solutions are managed locally, and an individual with an access card for one site  
665 cannot use the same card at a second site and must obtain a second card. [\[FIPS201\]](#) changes this  
666 dynamic because the credential is issued through a separate process instead of as part of the  
667 PACS deployment. Legacy PACS need to be upgraded or re-provisioned to support at least a  
668 14-decimal-digit FASC-N Identifier or a 16-byte Card UUID (see [Appendix C](#)).

#### 669 **3.2 Door Reader Interface**

670 PACS readers come in varying configurations and offer multiple interface options for the card  
671 and the controller. [\[FIPS201\]](#) standardizes the use of the [ISO/IEC 14443](#) interface for the  
672 contactless reader to card communication. Note that the card reader may require additional  
673 conformance testing for federal acquisition. An authority for such conformance testing is the  
674 General Services Administration (GSA) FIPS 201 Evaluation Program [\[FIPS 201 EP\]](#), which  
675 defines tests and maintains a list of approved products. Not all existing PACS use this interface,  
676 so some agencies may have to plan to migrate from their legacy environment to the [ISO/IEC](#)  
677 [14443](#) conformant interface. Alternatively, an agency may use the PIV Card's contact interface  
678 based on [ISO/IEC 7816](#).

679 The interface from the door reader to the controller also comes in different configurations.  
680 [\[FIPS201\]](#) does not specify which protocols can be used for this interface, as long as the  
681 necessary data can be communicated to the controller. Typical deployed implementations  
682 support transmitting a small amount of data (on the order of 10 to 15 bytes), but [\[FIPS201\]](#)  
683 defines data elements that are much larger. Therefore, depending on the agency's  
684 implementation strategy, an upgrade to the door reader to controller interface may also be  
685 required. At a minimum, a 14-decimal-digit FASC-N Identifier or the full 16-byte Card UUID  
686 will be supported. Note that any change to this interface may also necessitate changes to the  
687 physical wiring and cabling infrastructures.

#### 688 **3.3 Authentication Capability**

689 Legacy PACS readers use proximity or magnetic stripe technology to interface with identity

690 cards and use proprietary protocols to communicate data. Some of these proprietary protocols  
 691 employ cryptography, but their use is limited to the local site. [\[FIPS201\]](#) specifies identity  
 692 credentials that can be used for a new generation of identity management technology for building  
 693 access. [\[FIPS201\]](#) and its supporting special publications define the credential data model and  
 694 the card-to-reader interface, and also provide requirements for implementing the digital  
 695 certificates.

696 [\[FIPS201\]](#) added a standardized contactless and contact interface, PIN, biometric fingerprints,  
 697 optional iris images, and cryptography to the card that could be used to attain a higher level of  
 698 identity authentication assurance. The capability to perform bi-directional data communication is  
 699 fundamental to the deployment of secure building access. Adding cryptography to the cards  
 700 permits agencies to validate the data objects on the card and authenticate the cardholder. Adding  
 701 credential expiration and credential validation requirements also strengthens access control  
 702 decisions. At the same time, [\[FIPS201\]](#) provided the opportunity to migrate building access  
 703 systems from LITTLE or NO confidence levels to VERY HIGH confidence levels. Legacy  
 704 PACS may need upgrades to take advantage of these features and functions, in coordination with  
 705 the following guidelines and authorities:

- 706 + [\[FIPS201\]](#) assurance levels.
- 707 + The Risk Management Process for Federal Facilities: An Interagency Security  
 708 Committee Standard [\[ISC-RMP\]](#).
- 709 + OMB M-04-04, E-Authentication Guidance for Federal Agencies [\[M-04-04\]](#).

710 [\[FIPS201\]](#) redefines the requirements for building access in a fundamental way: instead of each  
 711 facility issuing an access card solely for that facility's PACS architecture, a facility relies on the  
 712 PIV Card that was issued by the same, or a different, agency certified by the Federal  
 713 Government. The facility still has control over the user's access privileges, but the technology  
 714 has been standardized to optimize interagency interoperability and the credential has been issued  
 715 to the user as part of the [\[FIPS201\]](#) identity management process.

### 716 **3.4 Wiring**

717 Selecting a particular reader type and its interface with the controller requires careful attention to  
 718 wiring. Existing wiring should be assessed for its ability to meet the requirements of new readers  
 719 and controllers and take into consideration performance. The existing wiring may be a limiting  
 720 factor due to its capacity to transmit data and original specifications. Many recently installed  
 721 systems use higher bandwidth cables, which are typically sufficient for a PIV-based access  
 722 control system. In some environments, advanced signaling methods operating at higher speeds  
 723 with lower signal-to-noise margins can necessitate upgrades to the wiring.

### 724 **3.5 Software Upgrades**

725 Vendors may be able to upgrade their PACS software to minimize the hardware changes needed  
 726 for a legacy PACS to accept PIV Cards. Software or firmware upgrades to controllers or door  
 727 readers may be available to agencies. PACS suppliers should be asked if software or firmware  
 728 upgrades supporting PIV Cards are a possibility. If available, the agency should ensure that the  
 729 software upgrade will have no adverse effect on the PACS system or any interconnected

730 systems.

### 731 **3.6 Legacy PACS Cards and PIV Card Differences**

732 The list below compares the basic differences in the technology offerings between the legacy  
733 PACS cards and the PIV Card.

- 734 + Some legacy PACS use site-specific card technology, with the result that a card  
735 cannot be used at sites with incompatible PACS. For example, a magnetic stripe card  
736 cannot be used at a proximity card site, and a magnetic stripe card from one vendor  
737 cannot be used at a site with magnetic stripe equipment from another vendor.
  - 738 + Legacy PACS readers can read an identifying number from a card, but in most cases  
739 they do not perform a cryptographic challenge/response exchange. Many non-PIV  
740 PACS cards can be copied easily.
  - 741 + When two sites use compatible legacy card technology, the risk of duplicate site  
742 identifiers for cards is always present. Without government-wide coordination of  
743 identifiers, the same identifier could be used on multiple cards at different sites.
  - 744 + To achieve government-wide coordination of cardholder identifiers, enough  
745 identifiers must be available for all government-issued credentials. Many legacy  
746 PACS have a limit on the number of sites (256) and the number of users per site  
747 (65 536) that is too small for government-wide use and can lead to the same  
748 identifiers being issued to different individuals.
  - 749 + Legacy PACS control expiration of credentials through an expiration date stored in a  
750 site database, whereas with PIV Cards expiration dates can be obtained from the cards  
751 themselves. There is no simple way to synchronize the expiration of credentials for a  
752 federal employee or contractor with access to multiple sites unless all sites are tied  
753 into a centralized enterprise-wide PACS (e-PACS).
  - 754 + Use of PINs, public key infrastructure, and biometrics with legacy PACS is managed  
755 on a site-specific basis at the PACS server. Individuals must enroll PINs, keys, or  
756 biometrics at each site. Since PINs, keys, and biometrics are often stored in a site  
757 database, they may not be technically interoperable with the requirements of other  
758 sites.
- 759 [\[FIPS201\]](#)-conformant PIV-enabled PACS eliminate or substantially reduce each of these  
760 limitations, relative to legacy PACS installations.



761

## 4. The PIV Vision

762 [\[HSPD-12\]](#) begins, “Wide variations in the quality and security of forms of identification used to  
763 gain access to secure Federal and other facilities where there is potential for terrorist attacks need  
764 to be eliminated.” [\[HSPD-12\]](#) continues, in Paragraph 4, “As promptly as possible... the heads  
765 of executive departments and agencies shall, to the maximum extent practicable, require the use  
766 of identification by Federal employees and contractors that meets the Standard in gaining  
767 physical access to Federally controlled facilities.”

768 [\[HSPD-12\]](#) directs federal departments and agencies to improve identification and authentication  
769 of federal employees and contractors requiring access to federally controlled facilities through  
770 the widespread application of [\[FIPS201\]](#). The standard defines the characteristics of the PIV  
771 System. This section describes the benefits that are expected from the use of the PIV System, to  
772 the maximum extent practicable, for authenticating people to PACS managed by the United  
773 States Government.

774 This section focuses on the benefits of electronic verification and direct integration with an  
775 electronic PACS. The [\[FIPS201\]](#) authentication mechanisms that can be performed electronically  
776 are PKI-CAK, SYM-CAK, BIO, BIO-A, PKI-AUTH and OCC-AUTH. The VIS authentication  
777 mechanism cannot be verified electronically and provides “LITTLE to NO” confidence in the  
778 identity of the cardholder. It should not be used when another mechanism is practical.

### 779 4.1 Interoperability

780 In this publication, the term interoperability means the ability of a PACS to use any PIV Card  
781 issued by any agency to authenticate the cardholder by performing one or more PIV  
782 authentication mechanisms. The data objects and keys placed on a PIV Card during issuance use  
783 specific cryptographic algorithms selected from the acceptable algorithms in [\[SP800-78\]](#),  
784 *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. A PACS application  
785 can interrogate the card to learn which algorithms are used. To attain full interoperability, a  
786 relying PACS application will need to support all acceptable algorithms, key lengths, and key  
787 material that could be presented, either by a PIV Card or by the PIV infrastructure.

788 The interoperability goal of a PIV-enabled PACS can be stated:

- 789 1. Any PIV Card can provide proof of identity to any electronic PACS (access is granted  
790 only if the identity is so authorized).
- 791 2. After a successful authentication, the authentication mechanism provides the  
792 cardholder’s authenticated identity (see [Section 5.4](#)) to the relying party.

793 To achieve interoperability, the PACS should at least observe the following conditions:

- 794 + If the PKI-CAK authentication mechanism is performed by a PACS application, the  
795 PACS should support all of the asymmetric algorithms permitted for the asymmetric  
796 CAK, as specified in Table 3-1 of [\[SP800-78\]](#), i.e., RSA 2048 and ECDSA P-256,  
797 and the PACS should accept all valid Card Authentication certificates.

- 798 + If the PKI-AUTH authentication mechanism is performed by a PACS, the accepted  
799 algorithms will be the same as PKI-CAK, but the PACS will accept only PIV  
800 Authentication certificates and require PIN entry.
- 801 + If authentication using off-card biometric comparison is performed (BIO or BIO-A),  
802 the PACS should support all of the signature algorithms and key sizes permitted by  
803 Table 3-2 of [\[SP800-78\]](#).
- 804 + PINs required for PIV authentication mechanisms are strings of six to eight decimal  
805 digits. For PKI-AUTH, BIO, and BIO-A authentication mechanisms, a PIN entry  
806 device must acquire the PIN from the cardholder and present it to the PIV Card for  
807 activation.
- 808 + The PACS supports at least one PIV authentication mechanism that is supported by  
809 all PIV Cards. For example, a PACS may use the PKI-AUTH authentication  
810 mechanism to authenticate all cardholders. Alternatively, the PACS may use the BIO  
811 authentication mechanism to authenticate most cardholders, but use the PKI-AUTH  
812 authentication mechanism to authenticate those cardholders from whom fingerprints  
813 could not be collected.

814 The PIMM presented in [Section 7.6](#) can be used to measure progress towards the interoperability  
815 goal. When PIV implementation is complete, all installed PACS readers are required to be from  
816 the approved products list of the [\[FIPS 201 EP\]](#), and each will be capable of one or more PIV  
817 authentication mechanism, such that each PACS reader will be capable of authenticating any PIV  
818 cardholder using a PIV authentication mechanism, including those with PIV Cards that do not  
819 implement any of the optional card capabilities.

820 The ability of a PIV Card and cardholder to authenticate at a reader does not mean they will be  
821 granted access—it means only that the cardholder has been identified, with the assurance level of  
822 the authentication mechanism employed, by the reader. A cardholder must authenticate and be  
823 authorized to be granted access. Authorization policies and mechanisms are outside the scope of  
824 [\[FIPS201\]](#).

825 **Recommendation 4.1:** To obtain the full benefit of PIV interoperability, PIV  
826 project managers should ensure that relying systems have the capability to use all  
827 cryptographic algorithms that apply to the authentication mechanism(s) performed.  
828 Departments and agencies are required to procure and deploy [\[HSPD-12\]](#) products  
829 from the [\[FIPS 201 EP\]](#) Approved Products List where applicable,<sup>5</sup> and can use the  
830 PIMM presented in [Section 7](#) to measure progress toward the goal of  
831 interoperability.

---

<sup>5</sup> The Evaluation Program directly supports the acquisition process for implementing HSPD-12. OMB Memorandum [\[M-06-18\]](#) directs that agencies must acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications in order to ensure government-wide interoperability.



## 832 4.2 Qualities of the Complete Implementation

833 The PIV System implementation will be complete when the following qualities have been  
834 achieved.

- 835 1. PIV authentication mechanisms are used wherever they are applicable, in accordance  
836 with [\[HSPD-12\]](#) and [\[FIPS201\]](#).
- 837 2. Electronic authentication (as opposed to VIS authentication) is the common practice.
- 838 3. Electronic validation of the PIV Card is done at or near the time of authentication.<sup>6</sup>
- 839 4. All PIV Card access control decisions are made by comparing the selected PIV  
840 identifier to access control list (ACL) entries. See [Section 5.4](#) and [Appendix C](#) for  
841 details.
- 842 5. PIV authentication mechanisms are applied based on the impact assessed for the area.
- 843 6. Cryptographic and biometric authentications are applied widely in moderate- and  
844 high-impact [\[FIPS199\]](#) areas.
- 845 7. Agencies exhibit reciprocal trust in the process assurance of PCIs.
- 846 8. Both new and upgraded PACS applications accept PIV Cards as proof of identity for  
847 user registration/provisioning, user authentication, or both.
- 848 9. Authentication transactions have been optimized; especially at access points that only  
849 require one-factor authentication and that have high throughput requirements.

850 [\[HSPD-12\]](#) declares its goals are to “...enhance security, increase Government efficiency, reduce  
851 identity fraud, and protect personal privacy,” and states specific criteria to be met by the  
852 implementation:

853 “Secure and reliable forms of identification” for purposes of this directive means  
854 identification that (a) is issued based on sound criteria for verifying an individual employee's  
855 identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist  
856 exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by  
857 providers whose reliability has been established by an official accreditation process. The  
858 Standard will include graduated criteria, from least secure to most secure, to ensure  
859 flexibility in selecting the appropriate level of security for each application.

860 The Federal Information Security Modernization Act [\[FISMA\]](#) mandates the standardization of  
861 security management practices for information systems. The foundational concept of [\[FISMA\]](#)  
862 security management is impact assessment and impact-based planning (“impact” being a  
863 generalization of “exposure” to monetary and non-monetary damage). [\[FIPS201\]](#) follows this  
864 methodology by implementing authentication mechanisms at four E-Authentication confidence

---

<sup>6</sup> In some cases, validating PIV Cards at the time of authentication is not practical. In these instances, it is possible to maintain a local cache of validated PIV Cards, provided that the cache is updated regularly.

865 levels (LITTLE or NO, SOME, HIGH, and VERY HIGH). A gap remains, however, between the  
 866 concepts of impact and confidence levels. This document suggests a method to close this gap  
 867 through the use of risk-based planning and the establishment of “Controlled, Limited, Exclusion”  
 868 boundaries for appropriately protecting facility assets or resources.

869 Interoperability of PIV Cards and PIV authentication mechanisms is not a guaranteed  
 870 consequence of the technical standard. Government-wide interoperability also requires federal  
 871 agencies to exhibit reciprocal trust in the processes of PCIs and the service quality of the PIV  
 872 Card validation and revocation infrastructure. Reciprocal trust is enabled by the requirements for  
 873 the PIV issuance process stated in [\[FIPS201\]](#), and supported by the accreditation process  
 874 methodology described in [\[SP800-79\]](#), *Guidelines for the Authorization of Personal Identity*  
 875 *Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*. Trust is built when  
 876 the technical standard is thorough, unambiguous, and grounded in practical requirements; when  
 877 the conformance and audit processes are documented and uniformly practiced; and when positive  
 878 PIV System audit results are available to the community of relying parties.

879 **Recommendation 4.2:** Once all appropriate authentication mechanisms are  
 880 satisfied, access control decisions are made by comparing the selected PIV  
 881 identifier (see [Section 5.4](#)) against the ACL entries.

882 **Recommendation 4.3:** As agencies develop risk-based implementation plans, they  
 883 will create and evolve plans for PIV Card issuance and application integration.  
 884 They might consider which of the nine qualities are most relevant to agency goals  
 885 and priorities, and derive further project objectives, metrics, and milestones from  
 886 those qualities. They should also consider the relation of [\[HSPD-12\]](#) to [\[FISMA\]](#)  
 887 requirements, and examine the potential for cost tradeoffs where PIV can replace  
 888 more expensive authentication methods.

### 889 4.3 Benefits of the Complete Implementation

890 The complete PIV System will be an identity infrastructure that is attractive to federal agencies,  
 891 application owners, and contractors because of these benefits:

- 892 + Enhanced trust. PIV Cards will be issued in accordance with standardized, audited  
 893 processes, which will exceed the best practice level for low- and moderate-impact  
 894 applications today, and equal best practice reached for high-impact applications.
- 895 + Resistance to misuse and cloning. Electronic validation of the PIV Card, using digital  
 896 signatures, makes it tamper-resistant. Cryptographic challenge/response protocols  
 897 make the PIV Card counterfeit-resistant. Biometric authentication makes the PIV  
 898 Card non-transferable.
- 899 + Status and revocation. PIV Card Issuer process assurance will extend beyond the  
 900 issuance action to PIV Card validation and revocation services. These services are  
 901 required elements of the PIV infrastructure, and will be implemented, monitored, and  
 902 audited with the same care as the PIV issuance process.
- 903 + Standard identity infrastructure. Application developers will assume, as a default,  
 904 that registration and authentication will use a PIV Card identity, reducing

905 development cost, registration time, and the application learning curve for new  
906 subjects.

907 + Integrated system. PACS will be fully integrated with other PIV system components  
908 that perform provisioning, enrollment, and finalization.

909 + Fewer passwords. A single PIV Card provides a small set of authentication methods  
910 that are applicable to many applications and in many contexts. This means  
911 significantly fewer passwords and account enrollments.

912 Each of these points both enhances security and creates efficiency of operation. Reducing  
913 passwords and password helpdesk calls, reusing identity enrollment across multiple applications,  
914 collapsing redundant status and revocation processes (separate processes for revocation on  
915 termination across multiple applications), and replacing authentication credentials that are easily  
916 shared or transferred will reduce operating costs borne by federal agencies. Availability of a  
917 skilled workforce familiar with the standardized PIV identity infrastructure, implementation of  
918 PIV issuance with a standardized identity verification methodology, the existence of high-  
919 availability online services for PIV Card status and validation, and pre-enrollment in a graduated,  
920 multi-factor authentication scheme all enhance security current practice in many applications.  
921 The replacement of password (single-factor) authentication with PIV Card (up to three-factor)  
922 authentication is a fundamental advance in authentication assurance.

923 Biometric enrollment is mandatory for the PIV Card. Every government employee and  
924 contractor who can provide at least one fingerprint image of acceptable quality will be pre-  
925 enrolled for biometric authentication.<sup>7</sup> Iris images may also be collected from a PIV applicant. In  
926 the complete PIV System, the marginal cost for biometric enrollment to the application owner,  
927 relative to other authentication mechanisms, is near zero, enabling more applications to gain the  
928 benefits of biometric authentication.

929 **Recommendation 4.4:** Operational metrics should be designed to measure actual  
930 benefits over the operational lifetime of the PIV System. They may be derived by  
931 formulating each of the expected benefits above as a service quality metric, e.g., for  
932 “integrated system,” service quality could be defined as the percentage of PACS  
933 registrations that are performed automatically by provisioning from the PIV  
934 issuance system.

#### 935 4.4 Infrastructure Requirements

936 The qualities and benefits of the complete PIV System can only be achieved if its  
937 implementation is supported by general advances in infrastructure used by PACS. The following  
938 areas have significant influence on the rate at which the complete PIV System integration can be  
939 achieved by PACS, and should therefore be supported by PACS upgrades and new PACS  
940 procurements:

---

<sup>7</sup> Section 6.2.1 of [\[FIPS201\]](#) states “When biometric authentication cannot be performed, PKI-AUTH is the recommended alternate authentication mechanism.” Also, see Sections 3.2, 3.3 and 3.4 of [\[SP800-76\]](#).

- 941 1. Fast, two-way communication between readers and controllers or panels.
- 942 2. Fast network communication between readers, controllers, or panels and PIV status
- 943 and validation services.

944 Point (1) allows readers to access cached validation status during access control transactions.  
945 Point (2) allows controllers or panels to cache the validation status. Points (1) and (2) combined  
946 could allow readers direct access to PIV status and validation services, if needed.

947 **Recommendation 4.5:** Maximum benefit will be obtained from the PIV System when it  
948 is adequately supported by infrastructure. Infrastructure upgrades may be justified,  
949 especially to improve communication between PACS system elements (e.g., support two-  
950 way communication).

## 951 **5. PIV Authentication Mechanisms**

952 This section provides a discussion of the PIV authentication mechanisms and their application in  
953 PACS environments. PIV authentication mechanisms offer a range of security measures (of  
954 different throughputs) that can be applied in a PACS environment. This section first describes a  
955 measurement scale for authentication assurance relevant to PACS. Then it discusses security  
956 offerings of each PIV authentication mechanism and their combinatory effects on identity  
957 authentication. Finally, this section provides recommendations on the use of PIV authentication  
958 mechanisms in a PACS environment.

### 959 **5.1 Authentication Factors**

960 One of the functions of the PACS application is to verify the identity of the cardholder  
961 presenting a PIV Card. The PACS application may perform one or more authentication  
962 mechanisms using the PIV Card to establish confidence in the identity of the cardholder. The  
963 authentication of an identity is based on the verification of one, two, or three of these factors: a)  
964 “something you have,” for example, possession of the PIV Card; b) “something you know,” for  
965 example, knowledge of the PIN; and c) “something you are,” for example, presentation of live  
966 fingerprints or irises by a cardholder.

967 The PIV authentication mechanisms operate in several different ways as defined in [\[FIPS201\]](#),  
968 [\[SP800-73\]](#), and [\[SP800-76\]](#). For example, the CHUID data object may be read from the PIV  
969 Card and its signature verified (CHUID authentication mechanism). A private key on the PIV  
970 Card may be used to sign a challenge (PKI-CAK and PKI-AUTH authentication mechanisms). A  
971 valid biometric from the card may be compared against a live scan (BIO, BIO-A, and OCC-  
972 AUTH authentication mechanisms).

973 PIV authentication mechanisms may be performed by different entities, referred to here as  
974 verifiers. For example, a PACS application verifies the signature on a data object, the signing of  
975 a challenge using a private key, or the comparison of biometric templates. The verifier can also  
976 be the PIV Card itself. For example, the PIV Card verifies the PIN or the fingerprint (in the case  
977 of OCC). The PACS should only trust the PIN verification by the PIV Card if it has verified that  
978 the card is a valid PIV Card.

979 The confidence in the cardholder’s identity increases with the number of factors used to  
980 authenticate the PIV Card. [Table 5-1](#) and [Table 5-2](#) provide lists of PIV authentication  
981 mechanisms and their authentication factors when used on the contact and contactless interfaces,  
982 respectively. Note that there are a few authentication mechanisms that are recognized as unique  
983 combinations in these tables. This is due to the fact that neither BIO(-A) nor PKI-CAK nor  
984 SYM-CAK individually provide the “something you know” authentication factor, but when  
985 BIO(-A) is used together with either PKI-CAK or SYM-CAK, PIN verification provides this  
986 factor since the card has been verified to be a valid PIV Card. Many different combinations of  
987 the PIV authentication mechanisms are possible and an exhaustive list of combinations is  
988 provided in [Appendix D](#).

989 Note that an authentication mechanism is not considered to provide any factors of authentication  
990 if the authentication is not successful. For example, in the case of the PKI-AUTH and PKI-CAK

991 authentication mechanisms, if the PACS application is unable to validate the authentication  
 992 certificate from the presented card or does not receive a response to its challenge that can be  
 993 verified using the public key in the certificate, then the PACS application cannot count the  
 994 authentication attempt towards meeting the requirements for granting access to an area.<sup>8</sup>

995 As noted in [Section 4.1](#), in order to achieve interoperability, each access point in a PACS needs  
 996 to support at least one PIV authentication mechanism that is supported by all PIV Cards. In  
 997 [Table 5-1](#) and [Table 5-2](#), the authentication mechanisms represented in **bold** are the  
 998 authentication mechanisms that can be implemented using only features that are mandatory for  
 999 PIV Cards issued under FIPS 201-2. Of these authentication mechanisms, however, only PKI-  
 1000 AUTH (when used in conjunction with the PIV Card PIN) and CHUID + VIS are currently  
 1001 supported by all PIV Cards. PKI-CAK will be supported by all valid PIV Cards after August  
 1002 2019, once all PIV Cards (issued under FIPS 201-1) without Card Authentication certificates  
 1003 have expired.

1004 While the CHUID + VIS authentication mechanism does provide interoperability its use is  
 1005 deprecated, since it provides “LITTLE or NO” confidence in the identity of the cardholder.  
 1006 However, CHUID + VIS may be used until September 2019 as part of a strategy to migrate to a  
 1007 stronger authentication mechanism, such as PKI-CAK, as described in [Section 5.3.1](#).

1008 While the Cardholder Fingerprints data object needed for the BIO and BIO-A authentication  
 1009 mechanisms is mandatory, it may not be possible to collect usable fingerprints from some  
 1010 cardholders. So, PACS that use BIO(-A) to authenticate cardholders should be prepared to use an  
 1011 alternative authentication mechanism with PIV Cards that have no minutiae in the Cardholder  
 1012 Fingerprints data object (see Section 4.4.3 of [\[SP800-76\]](#)). PKI-AUTH is the recommended  
 1013 alternate authentication mechanism.

<b>PIV Authentication Mechanism</b>	<b>Have</b>	<b>Know</b>	<b>Are</b>	<b>Authentication Factors (HKA Vector)</b>
<b>CHUID + VIS</b>	x			1
<b>BIO</b>			x	1
<b>SYM-CAK</b>	x			1
<b>PKI-CAK</b>	x			1
<b>BIO-A</b>	x		x	2
<b>PKI-AUTH</b>	x	x <sup>**</sup>	x <sup>***</sup>	2
<b>OCC-AUTH</b>	x		x	2

<sup>8</sup> If the authentication mechanism fails for a reason that indicates that the presented card is not valid, then the failed authentication attempt should raise an alarm.

<sup>\*\*</sup> If the PIN is used to satisfy the security condition for use, then the PKI-AUTH authentication mechanism provides the following 2 factors of authentication: (i) something you have (i.e., the card) and (ii) something you know (i.e., the PIN).

<sup>\*\*\*</sup> If OCC is used to satisfy the security condition for use, then the PKI-AUTH authentication mechanism provides the following 2 factors of authentication: (i) something you have (i.e., the card) and (ii) something you are (i.e., on-card biometric match). Note that OCC is an optional PIV Card feature. As result, PKI-AUTH does not support interagency interoperability when OCC is used to satisfy the security condition of use. Use of the PIV Card PIN, on the other hand, enables the PKI-AUTH authentication mechanism to achieve interagency interoperability.

SYM-CAK + BIO(-A)	x	x	x	3
<b>PKI-CAK + BIO(-A)</b>	x	x	x	3

1014

**Table 5-1 - PIV Authentication Mechanisms on the Contact Interface**

1015 [Table 5-2](#) provides a list of PIV Authentication mechanisms that are appropriate for use over the  
 1016 contactless interface. Note that there are some authentication mechanisms listed in [Table 5-1](#) for  
 1017 use over the contact interface that are not listed in [Table 5-2](#). The authentication mechanisms that  
 1018 are not listed in [Table 5-2](#) are authentication mechanisms that would require the use of secure  
 1019 messaging when performed over the contactless interface, but that do not require the use of  
 1020 secure messaging when performed over the contact interface. Since support for secure messaging  
 1021 is optional, these authentication mechanisms do not support interagency interoperability when  
 1022 performed over the contactless interface, but (with the exception of SYM-CAK + BIO(-A)) do  
 1023 support interagency interoperability when performed over the contact interface, and so use of the  
 1024 contact interface is preferable for these authentication mechanisms.

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors (HKA Vector)
<b>CHUID + VIS</b>	x			1
SYM-CAK	x			1
<b>PKI-CAK</b>	x			1
OCC-AUTH	x		x	2

1025

**Table 5-2 - PIV Authentication Mechanisms on the Contactless Interface**

1026 Each of the PIV authentication mechanisms is described further in the following sections.

1027 **5.1.1 Authentication using PIV Visual Credentials (VIS)**

1028 Visual authentication entails inspection of the topographical features on the front and back of the  
 1029 PIV Card. The human guard checks to see that the PIV Card looks genuine, compares the  
 1030 cardholder’s facial features with the picture on the card, checks the expiration date printed on the  
 1031 card, verifies the correctness of other data elements printed on the card, and visually verifies the  
 1032 security feature(s) on the card. The effectiveness of this mechanism depends on the training,  
 1033 skill, and diligence of the guard (to match the face in spite of changes in physical appearance –  
 1034 beard, mustache, hair coloring, eye glasses, etc.) – counterfeit IDs can pass visual inspections  
 1035 easily. Digital scanners, printers, and image editing software have made counterfeiting easier.  
 1036 Moreover, the visual verification of security features does not scale well across agencies since  
 1037 each agency may implement different security features. For these reasons, [FIPS201](#) has  
 1038 downgraded this authentication mechanism to indicate that it provides “LITTLE or NO”  
 1039 confidence in the identity of the cardholder.

1040 **5.1.2 Authentication using the Cardholder Unique Identifier (CHUID)**

1041 The CHUID, as defined in [FIPS201](#) and [TIG SEPACS](#), is one of the mandatory data objects  
 1042 on PIV Cards. The CHUID contains two data elements, the FASC-N and the Card UUID, that  
 1043 uniquely identify the PIV Card. The CHUID also uniquely identifies an individual since each  
 1044 PIV Card is issued to an individual. The CHUID data object is signed by the issuer so alterations  
 1045 or modifications to a CHUID can be detected. An expired CHUID, failure of signature



1046 verification or path validation results in a failed authentication attempt that does not admit a  
1047 cardholder for access.

1048 The CHUID is a free read object on the PIV Card; and thus it can be read or cloned easily.  
1049 Because of the risk of cloning, the CHUID authentication mechanism provides “LITTLE or NO”  
1050 confidence in the identity of the cardholder. For this reason, the CHUID authentication  
1051 mechanism has been deprecated in [\[FIPS201\]](#) and is expected to be removed in a future revision  
1052 of the standard.

1053 **Recommendation 5.1:** Agencies currently implementing the CHUID  
1054 authentication mechanism are highly encouraged to transition to another PIV  
1055 authentication mechanism as soon as possible (see [Section 5.3.1](#) for a suggested  
1056 migration strategy).

### 1057 **5.1.3 Authentication with the Card Authentication Certificate (PKI-CAK)**

1058 The asymmetric Card Authentication key, as defined in [\[FIPS201\]](#), is one of two mandatory  
1059 asymmetric authentication keys present on the PIV Card. As the name implies, the purpose of the  
1060 PKI-CAK authentication mechanism is to authenticate the card and therefore its possessor.  
1061 Unlike the CHUID authentication mechanism, the PKI-CAK authentication mechanism is highly  
1062 resistant to cloning, since cloning would require obtaining a copy of the private key. PKI-CAK  
1063 also provides protection against use of a revoked card as authentication fails and cardholder  
1064 access is denied when certificate validation indicates that the certificate has been revoked.  
1065 Similarly, failed signature verification or path validation results in a failed authentication attempt  
1066 that does not admit a cardholder for access.

1067 The PKI-CAK authentication mechanism is unique among the PIV authentication mechanisms  
1068 since it is the only PIV authentication mechanism that provides at least SOME confidence in the  
1069 identity of the cardholder that can be performed over the contactless interface using only card  
1070 features that are mandatory under [\[FIPS201\]](#).

1071 **Recommendation 5.2:** NIST recommends that agencies transition to use of the  
1072 PKI-CAK authentication mechanism at access points that only require single-factor  
1073 authentication. (See [Section 5.3.1](#) for a suggested transition strategy.)

### 1074 **5.1.4 Authentication with the Symmetric Card Authentication Key (SYM-CAK)**

1075 The SYM-CAK authentication mechanism is similar to the PKI-CAK authentication mechanism,  
1076 except that it uses the optional symmetric Card Authentication key to authenticate the card and it  
1077 does not provide protection against use of a revoked card. Due to its optionality and its use of a  
1078 single symmetric key that needs to be shared, stored and protected with reader components,  
1079 SYM-CAK is not suitable as an interoperable authentication mechanism as mandated by [\[HSPD-](#)  
1080 [12\]](#), and therefore is only suitable for use in authenticating PIV Cards issued by the same agency  
1081 that operates the PACS.

### 1082 **5.1.5 Unattended Authentication Using Off-Card Biometric Comparison (BIO)**

1083 PACS may perform off-card biometric authentication using the fingerprint information or the



1084 optional iris images stored on the PIV Card.<sup>9</sup> The biometric on the PIV Card is signed by the  
1085 issuer, so the authenticity of the biometric can be checked by the PACS. Verification of the  
1086 signature on the biometric data object, and matching of the reference biometric template with the  
1087 sample biometric template, is performed by the PACS application. The verification of signature  
1088 and matching of biometric results in one-factor authentication. This authentication mechanism  
1089 does not include authentication of the PIV Card.

1090 Potentially, a biometric template could be placed on a fake card – so neither the “something you  
1091 have” nor “something you know” factors are validated. As a result, this document rates the BIO  
1092 authentication mechanism as a one-factor (“something you are”) authentication mechanism. BIO  
1093 combined with a cryptographic challenge/response authenticates the PIV Card and thus achieves  
1094 three-factor authentication (see Section [5.1.9](#)).

1095 **Recommendation 5.3:** Biometric readers, especially those used at access points to  
1096 Limited and Exclusion areas, should have a proven capability to accept live fingers  
1097 and reject artificial fingers. Biometric readers, especially unattended readers in an  
1098 Unrestricted area, should be physically hardened to protect against direct electrical  
1099 compromise.

#### 1100 **5.1.6 Attended Authentication Using Off-Card Biometric Comparison (BIO-A)**

1101 The BIO-A authentication mechanism is the same as BIO authentication but an attendant  
1102 supervises the use of the PIV Card and the submission of the PIN and the sample biometric by  
1103 the cardholder. Some fingerprint biometric readers have been shown to accept fake or synthetic  
1104 fingerprints; others may allow access to internal wiring with relative ease. The presence of an  
1105 attendant during BIO-A authentication serves to mitigate these risks. Moreover, the presence of  
1106 an attendant also provides increased assurance, relative to BIO, that a fake card is not being used,  
1107 which accounts for an additional authentication factor of “something you have.” Since the PIN is  
1108 verified by the PIV Card and the card itself is not verified by PACS, the “something you know”  
1109 authentication factor is not validated. In summary, the BIO-A authentication mechanism benefits  
1110 from a presence of visual, but not from a strong challenge/response authentication, with the PIV  
1111 Card. Therefore, BIO-A is considered a two-factor authentication mechanism.

#### 1112 **5.1.7 Authentication with the PIV Authentication Certificate (PKI-AUTH)**

1113 The PIV Authentication key, as defined in [\[FIPS201\]](#), is a mandatory asymmetric key present on  
1114 the PIV Card. A PACS that performs public key cryptography-based authentication with the PIV  
1115 Authentication key uses the PKI-AUTH authentication mechanism. Use of PKI-AUTH provides  
1116 two-factor authentication, since the cardholder must present the card (something you have) and  
1117 either enter a PIN (something you know) or submit a fingerprint (something you are) to unlock  
1118 the card in order to successfully authenticate.

---

<sup>9</sup> As noted in Section 4.2.3.1 of [\[FIPS201\]](#), neither the fingerprint templates nor the iris images are guaranteed to be present on a PIV Card, since it may not be possible to collect fingerprints from some cardholders and iris images collection is optional. When biometric authentication cannot be performed, PKI-AUTH is the recommended alternate authentication mechanism. Agency security policy may require additional authentication mechanisms in consideration of impact-based security management.

1119 Similar to the PKI-CAK authentication mechanism, the PKI-AUTH authentication mechanism  
1120 involves validation of the PIV Authentication certificate. The validation protects against use of a  
1121 revoked card as authentication fails and cardholder access is denied when certificate validation  
1122 indicates that the certificate has been revoked. Similarly, failed signature verification or path  
1123 validation results in a failed authentication attempt that does not admit a cardholder for access.

#### 1124 **5.1.8 Authentication Using On-Card Biometric Comparison (OCC-AUTH)**

1125 The PIV Card may optionally implement on-card biometric comparison (OCC). With OCC,  
1126 biometric comparison data is stored on the card and cannot be read, but may be used by the card  
1127 to authenticate the cardholder.

1128 The OCC-AUTH authentication mechanism is implemented by performing OCC over secure  
1129 messaging. The PACS authenticates the PIV Card as part of the process of establishing secure  
1130 messaging, and the response from the PIV Card indicating that OCC was successful can be  
1131 verified since the response includes a message authentication code. Therefore, OCC-AUTH  
1132 provides two-factor authentication – something you have (i.e., the card via establishment of the  
1133 secure messaging protocol with the PACS application) and something you are (i.e., a fingerprint  
1134 via OCC). The OCC-AUTH authentication mechanism is highly resistant to cloning. However, it  
1135 does not protect against use of a revoked card. Additionally, not all PIV Cards support OCC-  
1136 AUTH, as both secure messaging and OCC are optionally card capabilities.

#### 1137 **5.1.9 (PKI-CAK | SYM-CAK) + BIO(-A) Authentication**

1138 Three-factor authentication may also be achieved by combining BIO(-A) with either PKI-CAK  
1139 or SYM-CAK. In this case, the PKI-CAK or SYM-CAK authentication mechanism is used to  
1140 authenticate the PIV Card and therefore the entry of the PIN to access the biometric fingerprint  
1141 template can now be trusted.

1142 As with the PKI-CAK authentication mechanism when performed alone, the PKI-CAK + BIO(-  
1143 A) authentication mechanism is highly resistant to cloning. The mechanism also protects against  
1144 the use of a revoked card as the authentication fails and the cardholder is denied access when  
1145 certificate validation indicates that the PIV Card has been revoked. SYM-CAK + BIO(-A) is also  
1146 highly resistant to cloning but does not protect against the use of a revoked card. Unlike PKI-  
1147 CAK, SYM-CAK relies on an optional PIV Card feature, so the SYM-CAK + BIO(-A)  
1148 authentication mechanism does not support interagency interoperability.

#### 1149 **5.2 Multi-Factor Authentication**

1150 Possession of a valid PIV Card as evidenced by visual inspection of the card, reading a signed  
1151 object from the card, or performing challenge/response authentication with the card, provides  
1152 one-factor authentication. For this reason, the VIS, CHUID, SYM-CAK and PKI-CAK  
1153 authentication mechanisms provide one-factor authentication. VIS provides weak one-factor  
1154 authentication since the card verification is subjective. CHUID also provides weak one-factor  
1155 authentication since it can be cloned. The BIO authentication mechanism provides one-factor  
1156 authentication since the reference biometric template is compared against the sample biometric  
1157 template without verifying the authenticity of the card itself. The PKI-AUTH authentication  
1158 mechanism provides two-factor authentication since it requires possession of the PIV Card and

1159 knowledge of the PIN or a fingerprint that matches the OCC data. OCC-AUTH achieves two-  
1160 factor authentication as the authenticity of the card is verified through secure messaging and thus  
1161 the on-card biometric match can be trusted. The BIO-A authentication mechanism provides two-  
1162 factor authentication since the reference biometric template is compared with the sample  
1163 biometric template in the presence of an attendant. For BIO(-A), knowledge of the PIN can only  
1164 be considered as a factor of authentication by combining this mechanism with either the PKI-  
1165 CAK or SYM-CAK authentication mechanism. This is because once the PIV Card is  
1166 authenticated the verification of the PIN can be trusted. The next section describes the use of  
1167 multi-factor authentication in the PACS environment.

### 1168 **5.3 Selection of PIV Authentication Mechanisms**

1169 A risk-based approach should be used when selecting appropriate PIV authentication  
1170 mechanisms for physical access to Federal Government buildings and facilities. Determining risk  
1171 to the facility is beyond the scope of this document; however, an agency may use a Facility  
1172 Security Level (FSL) Determination<sup>10</sup> to derive the FSL for its facilities. There is no simple one-  
1173 to-one mapping between the FSL and the authentication mechanism(s) that should be employed.  
1174 An FSL I campus facility may have a need for nested perimeters due to localized high-value  
1175 assets. An FSL III facility may not have any high-value assets but may be larger in population.  
1176 An FSL V facility may need the highest level of authentication assurance at all access points  
1177 except the public entrance to a visitor center.

1178 For these reasons, it is recommended that authentication mechanisms be selected on the basis of  
1179 protective areas established around assets or resources. This document adopts the concept of  
1180 “Controlled, Limited, Exclusion” areas as defined in [\[PHYSEC\]](#). Procedurally, proof of  
1181 affiliation is often sufficient to gain access to a Controlled area (e.g., an agency’s badge to that  
1182 agency’s headquarters’ outer perimeter). Access to Limited areas is often based on functional  
1183 subgroups or roles (e.g., a division badge to that division’s building or wing). The individual  
1184 membership in the group or privilege of the role is established by authentication of the identity of  
1185 the cardholder. Access to Exclusion areas may be gained by individual authorization only.  
1186 Federal Government facilities can be identified and categorized in these areas and correspond  
1187 generally to LOW (for Controlled), MODERATE (for Limited), and HIGH (for Exclusion)  
1188 impact assets or resources [\[FIPS199\]](#). This document recommends that [Table 5-3](#) be used to  
1189 determine the minimum number of authentication factors needed to satisfy security requirements  
1190 of the area.<sup>11</sup>

1191

1192

---

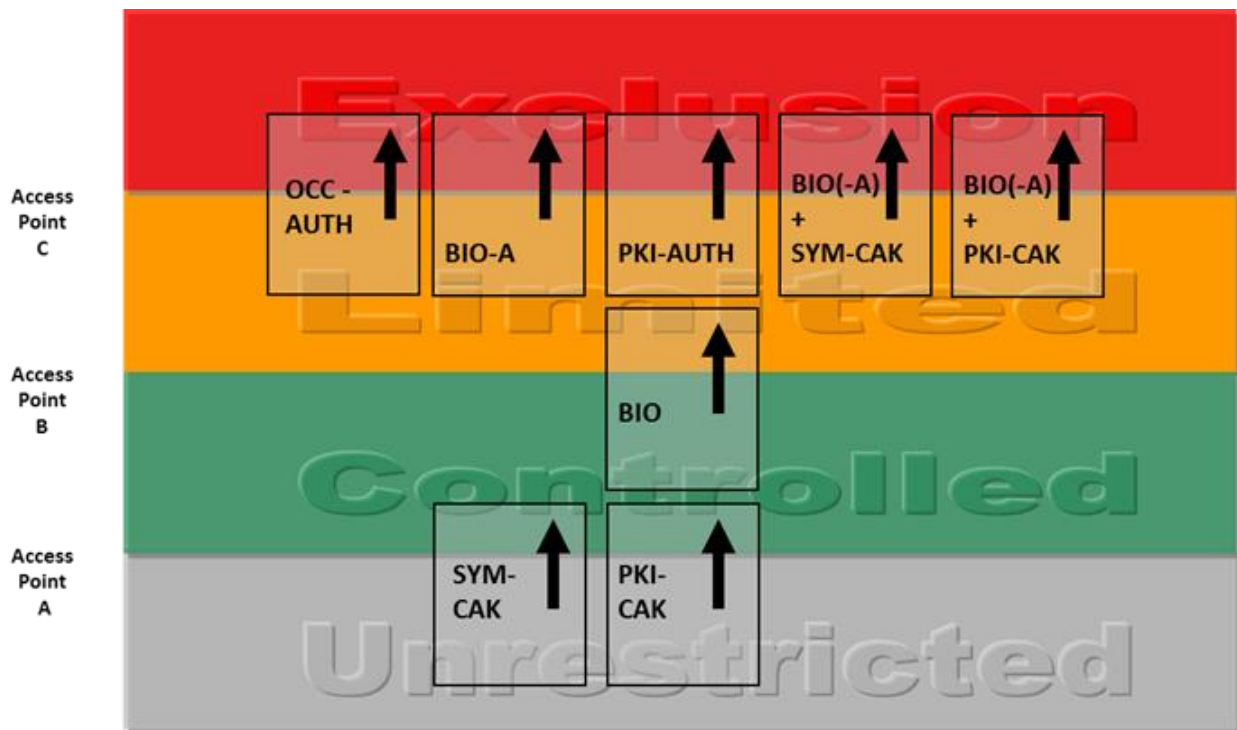
<sup>10</sup> FSL determination is the criteria and process used in determining the security level of a Federal facility, as described in “The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard” [\[ISC-RMPI\]](#).

<sup>11</sup> As noted in [Section 5.1](#), the security requirements of an area may only be satisfied by authentication mechanisms that are performed successfully (e.g., all signatures can be verified and all certificates are currently valid (not expired or revoked)).

Security Areas	Number of Authentication Factors Required
Controlled	1
Limited	2
Exclusion	3

1193 **Table 5-3 - Authentication Factors for Security Areas**

1194 [Figure 5-1](#) illustrates the innermost perimeter at which each PIV authentication mechanism may  
 1195 be used based on the authentication assurance level of the mechanism. [Table 5-3](#) and [Figure 5-1](#)  
 1196 both express constraints on the authentication mechanism that may be selected. The combined  
 1197 effect of [Table 5-3](#) and [Figure 5-1](#) determines exactly what mechanisms may be used. An  
 1198 exhaustive list of possible uses of PIV authentication mechanisms within protected areas is  
 1199 provided in [Appendix D](#).



1200  
 1201 **Figure 5-1: Innermost Use of PIV Authentication Mechanisms**

1202 The figure should be interpreted with the following notes:

1203 Note 1. “BIO(-A) + PKI-CAK” means a combined authentication mechanism performing PKI-  
 1204 CAK and BIO or PKI-CAK and BIO-A at the same access point, both using the contact  
 1205 interface of the PIV Card. The term “combine” means that more than one independent  
 1206 authentication mechanism must successfully authenticate the presenting person, at the  
 1207 same access point, before access is permitted.

1208 Note 2. Authentication mechanisms shown at a perimeter in [Figure 5-1](#) may also be used alone  
1209 at a perimeter farther out, subject to the requirements in [Table 5-3](#), but not the reverse. If  
1210 authentication mechanisms are combined in ways not shown in [Figure 5-1](#), at least one  
1211 of the combined mechanisms must be allowed by [Figure 5-1](#) at the security perimeter of  
1212 use.

1213 Note 3. In a particular facility, a single perimeter may separate areas with a difference of more  
1214 than one impact level. A single perimeter may allow access from Unrestricted to  
1215 Limited, Unrestricted to Exclusion, or Controlled to Exclusion areas, and in these cases,  
1216 the PIV authentication mechanisms should be combined to achieve necessary  
1217 authentication factors to enter the innermost area.

1218 Note 4. Within a Controlled or Limited area, an access point to an adjacent area at the same  
1219 impact level may employ any of the authentication mechanisms shown in [Figure 5-1](#).

1220 Note 5. Within an Exclusion area, an access point to an adjacent area at the same impact level  
1221 should use two or three-factor authentication.

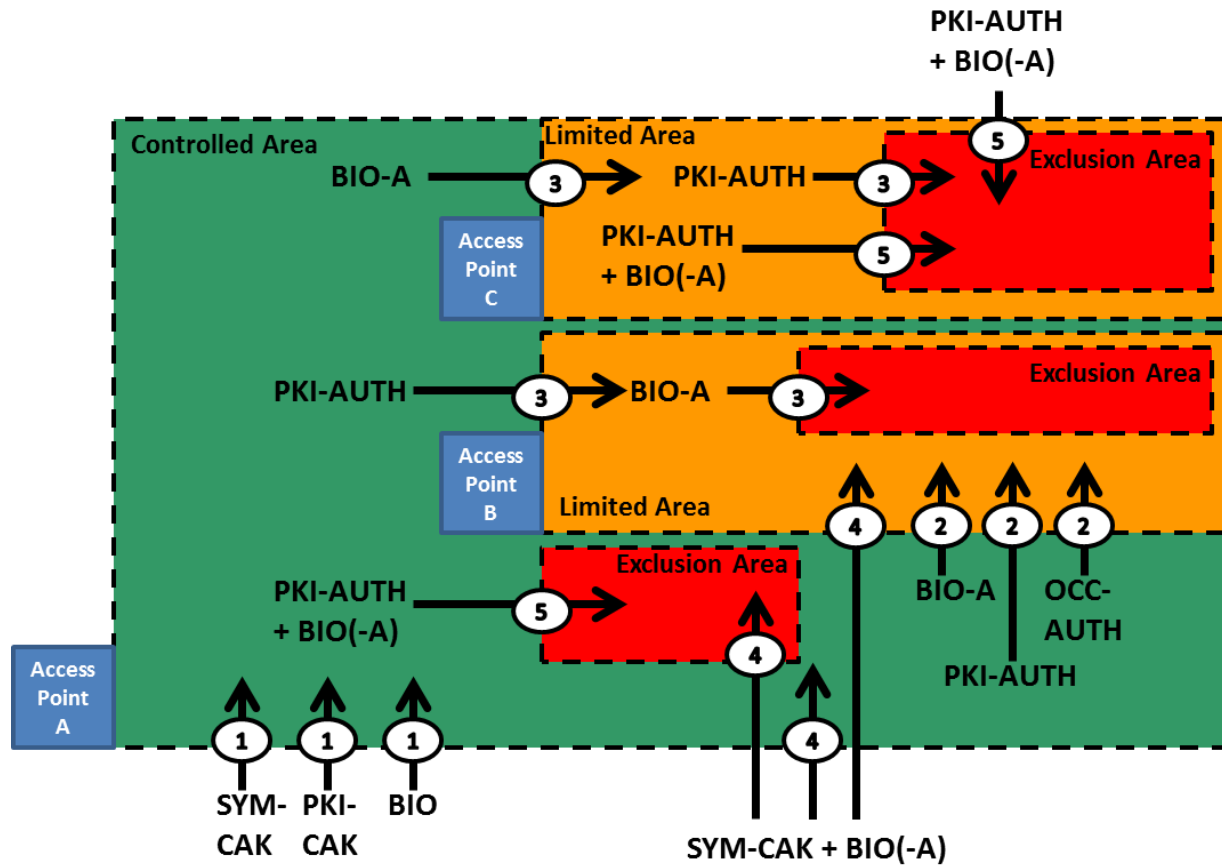
1222 Note 6. In most cases, [Figure 5-1](#) and these notes allow flexibility in the selection of specific  
1223 authentication mechanisms. A decision should be made based on the local security  
1224 policy and operational considerations.

1225 Notes (3) and (5) ensure that two-factor authentication is always employed to enter Limited  
1226 areas, and three-factor authentication is employed to enter Exclusion areas. It also ensures that  
1227 credential validation is done in either case.

1228 Notes (4) and (5) add some flexibility in the case of discretionary access control among areas at  
1229 the same impact level.

1230 The previous version of this document included the combined VIS + CHUID authentication  
1231 mechanism as an option to transitioning from Unrestricted to Controlled areas. VIS + CHUID,  
1232 however, is not included in this version of the document since both VIS and CHUID provide  
1233 “LITTLE or NO” confidence in the identity of the cardholder. Agencies currently implementing  
1234 the CHUID + VIS authentication mechanism need to transition to another PIV authentication  
1235 mechanism as soon as possible. [Section 5.3.1](#) provides a migration strategy that ends the use of  
1236 the CHUID authentication mechanism by September 2019. If a PACS continues to use the  
1237 CHUID authentication mechanism after September 2019, then the official that signs the  
1238 Authorization to Operate needs to indicate acceptance of the risks (see Sections [2.7](#) and [2.8](#)).

1239 PIV authentication mechanisms can be mapped to perimeter crossings in many ways, provided  
1240 that the requirements of this section are met. [Figure 5-2](#) below provides some examples of  
1241 mapping PIV authentication mechanisms to the perimeter crossings within a facility.



1242

1243

Figure 5-2: Examples of Mapping PIV Authentication Mechanisms

1244 [Figure 5-2](#) illustrates five different examples. Other sequences of authentication mechanisms are  
 1245 possible. Refer to [Appendix D](#) for a complete list of possible combinations of PIV authentication  
 1246 mechanisms that could be used in federal agency facility environments. Each example below is  
 1247 labeled with a number and is described as follows:

1248

1249

1. The PKI-CAK, SYM-CAK and BIO authentication mechanisms provide one-factor authentication and can be used to cross from Unrestricted to Controlled areas.

1250

1251

1252

2. The BIO-A, PKI-AUTH and OCC-AUTH authentication mechanisms provide two-factor authentication and can be used to cross into Limited areas. The example shows these authentication mechanisms to cross from Controlled to Limited areas.

1253

1254

1255

1256

1257

1258

1259

1260

3. Authentication in context can be leveraged if the “Controlled, Limited, Exclusion” areas are nested. This example shows that if the BIO(-A) authentication mechanism is used to access the Limited area, then the PKI-AUTH authentication mechanism may be used to control access to the Exclusion area without requiring the cardholder to repeat the BIO(-A) authentication mechanism. Conversely, if the PKI-AUTH authentication mechanism was used to access the Limited area, then BIO-A authentication may be used to control access to the Exclusion area. Authentication in context can be leveraged only when the PACS can store and recall recent access control decisions. This in turn would



1261 require a cardholder to authenticate at the outer perimeter prior to the inner perimeter.  
 1262 The risk of piggybacking, in which a person follows a cardholder through a door without  
 1263 authenticating, may thus be mitigated by authentication in context.

1264 4. This example shows that an authentication at one level may be used at lower levels. This  
 1265 example shows the SYM-CAK + BIO(-A) authentication mechanism may be used to  
 1266 cross from Unrestricted to Controlled, Unrestricted to Limited, or Unrestricted to  
 1267 Exclusion.

1268 5. This example shows that authentication in context is not always possible and a single  
 1269 perimeter may separate areas with a difference of more than one impact level.<sup>12</sup> The  
 1270 example shows that combined PKI-AUTH + BIO(-A) authentication mechanism may be  
 1271 used to cross from Unrestricted to Exclusion, Controlled to Exclusion, or Limited to  
 1272 Exclusion. Note that the three-factor authentication rule is observed in all possible  
 1273 crossings.

1274 [Figure 5-2](#) shows some legitimate examples of mapping PIV authentication mechanisms to the  
 1275 perimeter crossings. There are also authentication mechanisms that do not meet the requirements  
 1276 of [Table 5-3](#). For example, the PKI-CAK or SYM-CAK authentication mechanism should not be  
 1277 used to access Limited or Exclusion areas. Limited and Exclusion areas require either two or  
 1278 three-factor authentication, while the PKI-CAK and SYM-CAK mechanisms only provide one-  
 1279 factor authentication. Also, sometimes combining authentication mechanisms does not add up to  
 1280 the required authentication factors. For example, PKI-CAK + PKI-AUTH is not a valid  
 1281 authentication mechanism to access Exclusion areas. Note that PKI-CAK + PKI-AUTH only  
 1282 provides two factors (“something you have” and “something you know”) of authentication.

1283 **Recommendation 5.4:** Authentication assurance will be increased if a PACS uses  
 1284 relevant information from previous access control decisions (“context”) when  
 1285 making a new access control decision. For example, if a cardholder attempts to pass  
 1286 from a Controlled to a Limited area, the PACS could require that the cardholder  
 1287 was recently allowed access to the Controlled area. Historically, rigorous  
 1288 implementation of this concept required person-traps and exit tracking, but partial  
 1289 implementations have significant value, and could be strengthened by new  
 1290 technology and systems integration.

### 1291 5.3.1 Migrating Away from the Legacy CHUID Authentication Mechanism

1292 The CHUID authentication mechanism was included in the initial FIPS 201 to enable electronic  
 1293 authentication with legacy systems, but was deprecated in FIPS 201-2, and is expected to be  
 1294 removed in the next revision, because of its security concerns, as described in [Section 2.7](#) and  
 1295 [Section 2.8](#). In addition, both the CHUID and VIS authentication mechanisms were downgraded  
 1296 in FIPS 201-2 to indicate that they provide LITTLE or NO assurance in the identity of the

---

<sup>12</sup> Although a single perimeter could separate areas with a difference of more than one impact level, this practice may be judged high risk and be prohibited by local security policy.

1297 cardholder. For these reasons, use of the CHUID authentication mechanism, even in combination  
1298 with VIS, is no longer recommended. Departments and agencies are strongly encouraged to  
1299 transition to other authentication mechanisms as soon as possible.

1300 It is understood, however, that an immediate transition away from use of the CHUID  
1301 authentication mechanism will not be feasible in many cases. While [Section 5.1](#) describes several  
1302 authentication mechanisms, PKI-CAK is the only authentication mechanism providing at least  
1303 SOME assurance in the identity of the cardholder that has the potential to provide fast  
1304 authentication and that can be implemented using only card features that are mandatory under  
1305 FIPS 201-2. However, at the moment, not all PIV Cards support the PKI-CAK authentication  
1306 mechanism since the Card Authentication certificate was optional prior to FIPS 201-2. Rather  
1307 than using CHUID + VIS to authenticate all cardholders until all valid PIV Cards have Card  
1308 Authentication certificates, a gradual transition to alternative authentication mechanisms is  
1309 recommended. Two strategies for transitioning away from use of the CHUID + VIS  
1310 authentication mechanism are described below, one for use with PIV Cards that have been  
1311 preregistered with the PACS before they are used at an access point and one for use with PIV  
1312 Cards that have not been preregistered. Preregistration is recommended, when possible, since it  
1313 allows for some aspects of the authentication to be performed in advance (see [Sections 5.5](#) and  
1314 [5.6](#), and [Appendix A](#)), thus reducing transaction times when PIV Cards are presented at access  
1315 points.

1316 If a PIV Card is registered with the PACS before it is used at an access point, then the  
1317 authentication mechanism to use with the card at entry points to Controlled areas may be  
1318 determined at the time of registration. If the PIV Card was issued by the agency that controls the  
1319 PACS and the card has a symmetric Card Authentication key, then the SYM-CAK authentication  
1320 mechanism may be used.<sup>13</sup> Alternatively, if a Card Authentication certificate is present on the  
1321 card, then the PKI-CAK authentication mechanism should be used. In the absence of a Card  
1322 Authentication certificate, the card should be validated during the registration process using the  
1323 PKI-AUTH authentication mechanism in order to ensure that it is a valid PIV Card, and not a  
1324 card produced via visual counterfeiting and electronic cloning, as described in [Sections 2.3](#) and  
1325 [2.8](#). If the card is determined to be valid, then the CHUID + VIS authentication mechanism may  
1326 be used.

1327 If a PIV Card that has not been preregistered with the PACS is presented at an entry point to a  
1328 Controlled area and the PACS allows use of cards that have not been preregistered, then the  
1329 system should first try to read the Card Authentication certificate from the card, and use the PKI-  
1330 CAK authentication mechanism if the certificate is present. In the absence of the Card  
1331 Authentication certificate, the card should be authenticated using the CHUID + VIS  
1332 authentication mechanism.

1333 FIPS 201-2 requires all PIV Cards issued after September 2014 to include a Card Authentication

---

<sup>13</sup> Since the SYM-CAK authentication mechanism does not provide protection against use of a revoked card, agencies using this authentication mechanism would need to have processes in place to deauthorize use of PIV Cards in the PACS when cards are revoked.



1334 certificate. So, using the transition strategies described above, use of the CHUID + VIS  
 1335 authentication mechanism should gradually decrease until it is entirely eliminated by September  
 1336 2019 once all valid PIV Cards have completed their five-year lifecycle and have been replaced  
 1337 with cards containing the Card Authentication certificate.

#### 1338 **5.4 PIV Identifiers**

1339 Once the cardholder is authenticated, the next step is making an access control decision. Access  
 1340 control decisions can be made by comparing PIV identifiers against access control list (ACL)  
 1341 entries. Examples of PIV identifiers used in access control decisions include the FASC-N (entire  
 1342 or part of), the Card Universally Unique Identifier (UUID), and the optional Cardholder UUID.

1343 When deciding on the identifier to be used for access control decisions, agencies should consider  
 1344 the advantages and disadvantages of each type. Some of these decisions include the need to be  
 1345 able to grant access to holders of PIV Cards issued by another agency, and whether the agency  
 1346 will grant access to holders of PIV-Interoperable Cards (PIV-I Cards<sup>14</sup>).

1347 [Table 5-4](#) illustrates the pros and cons of using each identifier:

PIV Identifier	Pros	Cons
FASC-N	<ul style="list-style-type: none"> <li>Available on all PIV Cards</li> <li>Access control permissions can be based on one or more fields within the FASC-N</li> </ul>	<ul style="list-style-type: none"> <li>ACL entries may need to change every time a PIV Card is re-issued. (See <a href="#">Appendix C</a>)</li> <li>Not available on PIV-I Cards</li> </ul>
Card UUID	<ul style="list-style-type: none"> <li>Available on all PIV-I Cards</li> <li>Available on all PIV Card issued under FIPS 201-2</li> </ul>	<ul style="list-style-type: none"> <li>ACL entries have to be updated every time a PIV or PIV-I Card is re-issued</li> <li>May not be available on PIV Cards issued under FIPS 201-1</li> </ul>
Cardholder UUID	<ul style="list-style-type: none"> <li>ACL entries do not have to be updated every time a cardholder is issued a new card</li> </ul>	<ul style="list-style-type: none"> <li>Not available all cards since it is optional</li> <li>Only appears in the CHUID data object</li> </ul>

1348

**Table 5-4 - PIV Identifiers**

1349 The FASC-N is a required data element on the PIV Card, which enables agencies to use it as an  
 1350 identifier for access control decisions. An advantage of the FASC-N over the Card UUID and the  
 1351 Cardholder UUID is that ACLs can be based on one or more fields within the FASC-N (see  
 1352 [Appendix C](#)). The FASC-Ns on PIV-I Cards, however, cannot be used in access control  
 1353 decisions, since they are not assigned in a manner than ensure uniqueness.

---

<sup>14</sup> PIV-I Cards are defined in [PIV-I NFI] and further clarified in [PIV-I FAQ] and [PIV-I CP]. The intent of [PIV-I NFI] is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and their applications, and that may be trusted for particular purposes at the discretion of the relying Federal departments and agencies.

1354 The Card UUID is a required data element for PIV-I Cards that enables departments and  
1355 agencies to identify a PIV-I cardholder. The Card UUID is also a required data element for PIV  
1356 Cards issued under FIPS 201-2. So, after August 2019, once all PIV Cards issued under FIPS  
1357 201-1 have expired, PACS will be able to use the Card UUID in ACLs with all PIV and PIV-I  
1358 Cards.

1359 The Cardholder UUID is an optional data element introduced in FIPS 201-2. Unlike the FASC-N  
1360 and Card UUID, the Cardholder UUID is a persistent identifier for the cardholder that does not  
1361 change when the cardholder receives a replacement card. So, for cards that have a Cardholder  
1362 UUID, use of the Cardholder UUID can avoid the need to update ACL entries every time a  
1363 cardholder is issued a new card. However, since the Cardholder UUID only appears in the  
1364 CHUID data object, use of this identifier to make access control decisions would tend to increase  
1365 transaction times, as there would be a requirement to authenticate the cardholder (e.g., using  
1366 PKI-CAK), then read and validate the CHUID data object, and then compare an identifier in the  
1367 CHUID data object to an identifier in the data object used during the authentication in order to  
1368 ensure that both data objects were issued to the same card (e.g., comparing the Card UUID in the  
1369 CHUID to the Card UUID in the Card Authentication certificate). An alternative would be store  
1370 both the Cardholder UUID and either the FASC-N or Card UUID in the ACL, grant access if the  
1371 card's FASC-N or Card UUID is present on the ACL, and only check the Cardholder UUID if  
1372 the presented FASC-N or Card UUID is not on the ACL. If the Cardholder UUID is found on the  
1373 ACL, then the corresponding FASC-N or Card UUID should be updated in the ACL for use in  
1374 future transactions.

## 1375 **5.5 PACS Registration**

1376 Before a PACS may grant access to a cardholder, the cardholder must be authorized for access in  
1377 the PACS. Authorization may be granted to a group of individuals, such as all PIV cardholders,  
1378 or all PIV cardholders sponsored by a specific agency (see [Appendix C](#)). If authorization is  
1379 granted to specific individuals, information about the cardholder (see [Section 5.4](#)) must be added  
1380 to the PACS server's authorization database.

1381 If online credential validation is performed by the PACS at the time of each authentication (see  
1382 [Section 5.6](#)), the PACS might not need to store any information about the cardholder other than  
1383 the authorizations and transaction audit log. If a caching status proxy is employed, information  
1384 about the cardholder, including the cardholder's certificate, must be added to the server's  
1385 database. Where one-factor authentication is sufficient, the Card Authentication or PIV  
1386 Authentication certificate may be used. Where at least two-factor authentication is required, the  
1387 PIV Authentication certificate should be used.

1388 When the individual is enrolled using a caching status proxy, the enrollment station obtains the  
1389 PIV Authentication or Card Authentication certificate from the PIV Card, validates the  
1390 certificate (including checking the certificate's revocation status), and sends a challenge to the  
1391 card to verify that it holds the private key corresponding to the certificate. The authentication  
1392 certificate is then added to the server's database, along with any other information about the  
1393 individual that the server maintains (e.g., the individual's authorizations).

1394 Since certificate revocation is used as a mechanism to indicate that a PIV Card should no longer  
1395 be considered valid, the caching status proxy should periodically revalidate all of the certificates

1396 in its database and deactivate the access privileges of any individual whose certificate has  
1397 expired or has been revoked. Revalidation should be performed by the caching status proxy at  
1398 least once per day. Once the decision has been made to revoke a PIV Card, agencies may employ  
1399 local deauthorization methods to supplement certificate revocation and achieve a more rapid  
1400 local effect.

1401 **Recommendation 5.5:** The CHUID may be collected at registration, but it should  
1402 not be retained. A stored CHUID presents a risk, because it can be copied and used  
1403 to gain access at access points that have not yet migrated away from use of the  
1404 CHUID authentication mechanism. Data elements (e.g., the FASC-N and Global  
1405 Unique Identifier (GUID)) may be extracted from the CHUID and retained, as may  
1406 a hash of the CHUID. *NIST strongly recommends against the storage of complete*  
1407 *CHUIDs in relying systems.*

1408 **Recommendation 5.6:** PKI-AUTH and PKI-CAK authentication mechanisms  
1409 should be implemented by a PACS reader capable of full certificate path validation,  
1410 either online or using a caching status proxy. Agencies should consider using online  
1411 status checks when the most up to date PIV Card status is necessary or if access is  
1412 being granted to Exclusion areas. If a caching status proxy is used, the certificates  
1413 should be captured when the PIV Card is registered to the PACS.

## 1414 5.6 Credential Validation and Path Validation

1415 *Credential validation* is the process of determining if a presented identity credential is valid, i.e.,  
1416 was legitimately issued and has not expired or been revoked.

1417 [\[FIPS201\]](#) requires that any credential used in an authentication mechanism be checked to ensure  
1418 that it was legitimately issued. However, not all credentials on the PIV Card include an  
1419 expiration date. So, when performing the BIO, BIO-A, OCC-AUTH or SYM-CAK  
1420 authentication mechanism, an additional credential needs to be checked in order to verify that the  
1421 PIV Card has not expired or been revoked. This additional credential may be the CHUID, the  
1422 PIV Authentication certificate, or the Card Authentication certificate.

1423 The preferred option is to validate one of the authentication certificates. Section 5.5 of [\[FIPS201\]](#)  
1424 states “*The presence of a valid, unexpired, and unrevoked authentication certificate on a card is*  
1425 *proof that the card was issued and is not revoked.*” The footnote in Section 6.2.2.1 of [\[FIPS201\]](#)  
1426 further says, “*The PIV Authentication certificate or Card Authentication certificate may be*  
1427 *leveraged to verify that the card is not expired.*” These statements imply that the validity of the  
1428 PIV Card can be determined by performing path validation (see below) on the PIV  
1429 Authentication certificate or Card Authentication certificate.

1430 Particularly in the case of the authentication certificates, online credential validation is extremely  
1431 valuable to relying parties because it retrieves the most up-to-date credential status, that block  
1432 access of fraudulent PIV Cards that have been lost or stolen. However, online, on-demand  
1433 credential validation may not always be practical. Some reasons include: (i) a noticeable delay in  
1434 response time and (ii) absence of network connectivity to the certification authority. In these  
1435 circumstances, it may be possible for PIV Cards of interest to be registered with a caching status  
1436 proxy. The caching status proxy polls the status of all registered cards periodically, and caches

1437 the status responses from their issuer(s). Relying parties will see quick query-response service  
1438 from the caching status proxy. The cache status should be updated at least once every 24 hours.

1439 **Recommendation 5.7:** Online credential validation should be implemented for all  
1440 of the PIV authentication mechanisms whenever most up-to-date status is  
1441 necessary.

1442 **Recommendation 5.8:** Caching techniques should be used to implement credential  
1443 validation to get improved performance or when online, on-demand credential  
1444 validation is not possible. It is also recommended that the cached data be protected  
1445 against tampering.

1446 **Recommendation 5.9:** Credential status checks that indicate that the certificate has  
1447 been revoked should always prevent a cardholder from access.

1448 Data objects read from the PIV Card by a reader must not be fully trusted as authentic (i.e.,  
1449 produced by a PCI) and unmodified until their digital signatures are verified. Most data objects  
1450 in a PIV Card Application have embedded digital signatures (i.e., all certificates, the CHUID,  
1451 fingerprint templates, facial image, iris images, and security object). The authenticity of data  
1452 objects that do not have embedded digital signatures (e.g., Printed Information Buffer) can be  
1453 verified since hashes of these data objects are included in the Security Object.

1454 *Path validation (or trust path validation)* is the process of verifying the binding between the  
1455 subject identifier and subject public key in a certificate, based on the public key of a trust anchor,  
1456 through the validation of a chain of certificates that begins with a certificate issued by the trust  
1457 anchor and ends with the target certificate. The public key of a trust anchor is implicitly trusted  
1458 by the relying party (generally, this means it was installed into the relying system by means of a  
1459 trusted process, such as a direct device-to-device copy). Full trust in a PIV authentication  
1460 mechanism requires that path validation succeed for each PIV data object used by the  
1461 mechanism.<sup>15</sup>

1462 [\[FIPS201\]](#) requires that path validation be performed for all PIV authentication mechanisms,  
1463 since these authentication mechanisms can be fully trusted only if path validation is performed.  
1464 In the absence of path validation, an impostor could forge a fingerprint template and a CHUID  
1465 object, for example, with signatures from a phony certification authority. BIO authentication  
1466 would succeed with this counterfeit PIV Card, and the forgery would not be detected.

1467 **Recommendation 5.10:** Credential validation must be performed on all signed  
1468 data objects required by the authentication mechanism in use. Path validation of a  
1469 certificate should employ either online or cached status checks depending on the  
1470 authentication use case, the PACS environment and the performance requirements.  
1471 Because path validation is a part of credential validation, both services can be

---

<sup>15</sup> If a data object is not used in the authentication mechanism being performed, path validation need not be performed on the data object's digital signature for the authentication result to be fully trusted.

1472           economically implemented by a single PACS service component.

1473   **5.7 Lost PIV Card or Suspicion of Fraudulent Use**

1474   If a lost PIV Card is found by a person other than the cardholder, or if a pattern of PIV Card  
1475   activity raises suspicions of fraudulent use, the security office of the issuing agency, or of the  
1476   cardholder's duty station, should be notified. The security office (issuing and local duty station)  
1477   will determine if further investigation is warranted and if the PCI should be asked to revoke the  
1478   PIV Card.

1479

## 1480 **6. PACS Use Cases**

1481 [\[HSPD-12\]](#) requires that PIV credentials include graduated criteria, from least secure to most  
 1482 secure, for authentication to ensure flexibility in selecting the appropriate level of security for  
 1483 each application. PIV credentials, as defined in [\[FIPS201\]](#), offer a range of security, which is  
 1484 discussed in [Section 5](#). This section provides recommendations for the appropriate use of  
 1485 graduated security in PIV credentials for the PACS.

1486 PIV credentials can be used at federally-owned buildings or leased spaces, single or multi-tenant  
 1487 occupancy, commercial spaces shared with non-government tenants, and government-owned  
 1488 contractor-operated facilities. This includes existing and new construction or major  
 1489 modernizations, standalone facilities, and federal campuses. Thus, PIV credentials apply to  
 1490 facilities requiring varying levels of security with differing security requirements.

1491 To begin, the agency must know the security requirements for its facility. Since this is beyond  
 1492 the scope of this document, it is assumed that the agency has completed its facility security risk  
 1493 assessment. It is also assumed that the agency is using the FSL determination [\[ISC-RMP\]](#) to  
 1494 derive the security requirement for its facility. The FSL takes into account size and population,  
 1495 as well as several other factors that capture the value of the facility to the government and to  
 1496 potential adversaries. Other factors, including mission criticality, symbolism, and threat to tenant  
 1497 agency, are also considered. For the purposes of protecting assets and placement of proper  
 1498 security measures, size and population may not be as important as the mission criticality,  
 1499 symbolism, and threat to the tenant agency. Although there is no simple one-to-one mapping  
 1500 between FSL and the authentication mechanism(s), the FSL indicates the general risk to the  
 1501 facility. Based on the FSL, an agency should identify and categorize PACS perimeters as  
 1502 protecting Controlled, Limited, or Exclusion areas. Appropriate security measures can then be  
 1503 implemented based on the areas identified for the facility in consultation with the real property  
 1504 authority and legal authority. This section provides example use cases of PIV authentication  
 1505 mechanisms in the following facility environments:

- 1506 + Single-Tenant Facility—A facility that only includes a federal tenant, or multiple  
 1507 components of the same department or agency that fall under one “umbrella” for  
 1508 security purposes.
- 1509 + Multi-Tenant Facility—A facility that includes tenants from multiple federal  
 1510 departments and agencies, but no non-federal tenants.
- 1511 + Mixed-Multi-Tenant Facility—A facility that includes tenants from multiple federal  
 1512 departments and agencies as well as one or more non-federal tenants.
- 1513 + Single-Tenant Campus—Federal facilities with two or more buildings surrounded  
 1514 (and thus defined) by a perimeter.
- 1515 + Multi-Tenant Campus—Two or more federal facilities located contiguous to one  
 1516 another and typically sharing some aspects of the environment, such as parking,  
 1517 courtyards, private vehicle access roads or gates, entrances to connected facilities, etc.  
 1518 May also be referred to as a “Federal center” or “Complex.”

## 1519 6.1 Single-Tenant Facility

1520 In single-tenant facilities, a single tenant defines its own security requirements and controls its  
 1521 own security measures. Implementation of security measures is uniform. The facility may be an  
 1522 owned or a leased space. If the space is leased, the tenant usually can impose security  
 1523 requirements based on its needs. This type of facility may range from FSL I to FSL V. Therefore,  
 1524 it may have LOW, MODERATE, or HIGH value assets to protect. Facilities evaluated at FSL I  
 1525 or II may not implement PACS and may continue without PACS. Facilities evaluated at FSL III  
 1526 or above should implement PACS. These facilities may have general access areas where  
 1527 individual identification and authentication is not possible, or necessary. In this case, the agency  
 1528 should establish at least one perimeter beyond which individual authentication is required and  
 1529 conducted with PACS. [Figure 6-1](#) is an example of a single-tenant facility. The figure shows a  
 1530 building with multiple floors occupied by one tenant. The one security perimeter is the lobby  
 1531 where the cardholder authentication takes place. This one-perimeter facility should be designated  
 1532 as a Controlled, Limited, or Exclusion area and the appropriate authentication mechanisms  
 1533 should be selected from [Figure 5-1](#).

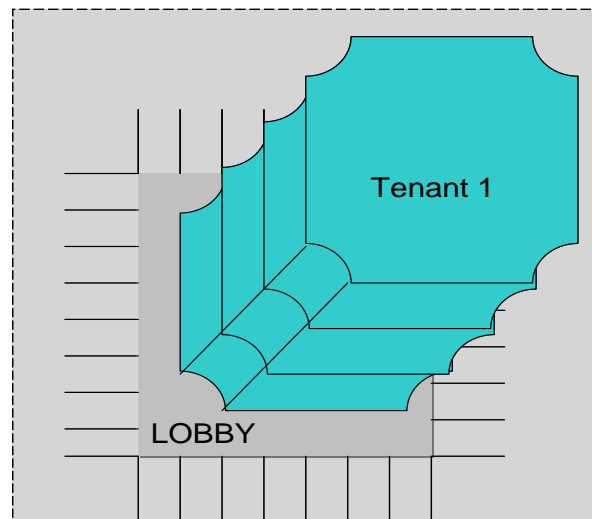


Figure 6-1: Single-Tenant Facility

## 1543 6.2 Multi-Tenant Facility

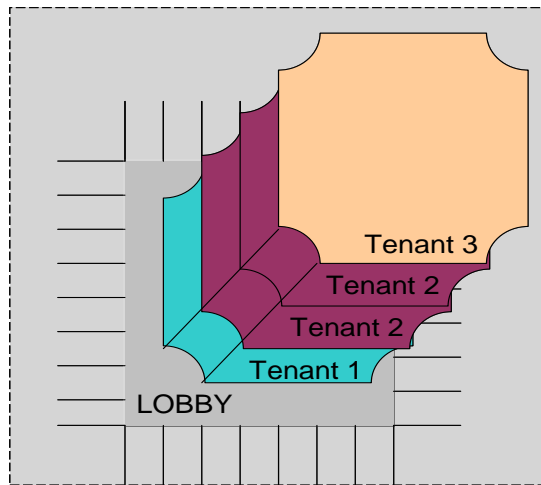
1544 The challenge with a multi-tenant facility is to meet the security policies and requirements of the  
 1545 individual tenants in the facility. Some tenants may need higher security than others. The  
 1546 security policies may not be uniform and cannot be imposed upon others. In this situation, a  
 1547 collective (also known as the Building Security Committee) determination has to be made by the  
 1548 designated officials (representatives for each federal tenant), the owning or leasing department or  
 1549 agency, and the security organization responsible for the facility to identify appropriate areas  
 1550 within the facility. In the end, the decision may be to implement the highest necessary security  
 1551 for the entire facility or to apply the lowest security to the facility while affording individual  
 1552 agencies additional security at their interior perimeters.

1553 If the highest security is implemented for the entire facility, there is one security perimeter and  
 1554 the security posture is no different from a single-tenant facility. Otherwise, the multi-tenant



1555 facility may be viewed as an outer and inner perimeter where different security can be  
 1556 implemented. The outer perimeter is the most common security measure that all the tenants  
 1557 agreed to and the inner perimeter is an agency-specific security measure. For example, the  
 1558 facility may designate Controlled area at the outer perimeter but one of the tenant agencies may  
 1559 require Exclusion area protection. Access to the building may be generally satisfied with a  
 1560 Controlled area authentication mechanism, but the individual agency should implement an  
 1561 Exclusion area authentication mechanism for access to its floor(s). In this example, the building  
 1562 is the outer perimeter while access to an individual floor is the inner perimeter.

1563 Since there are multiple tenants in the facility, it is strongly recommended that each individual  
 1564 tenant designate its own “Controlled, Limited, Exclusion” areas and employ appropriate  
 1565 [\[FIPS201\]](#) authentication mechanisms as in [Figure 5-1](#). Since by definition the multi-tenant  
 1566 facility hosts Federal Government employees and contractors, the outer perimeter can be PIV-  
 1567 enabled and individual agencies may piggyback on the authentication performed at the outer  
 1568 perimeter. [Figure 6-2](#) is an example of a multi-tenant facility. The building lobby is the outer  
 1569 perimeter implementing PIV-enabled PACS, while the individual tenants implement additional  
 1570 security perimeters for stronger cardholder authentication.



1571  
 1572  
 1573  
 1574  
 1575  
 1576  
 1577  
 1578 **Figure 6-2: Multi-Tenant Facility**

### 1579 **6.3 Mixed-Multi-Tenant Facility**

1580 The mixed-multi-tenant facility use case is an example of a facility with a mix of PIV  
 1581 cardholders and non-PIV cardholders. Therefore, some tenants in this facility may not possess  
 1582 PIV Cards for authentication. It may be difficult if not impossible to develop one acceptable  
 1583 security policy for all the tenants. The federal tenants in this facility should ensure they have  
 1584 leverage to implement necessary PIV authentication mechanisms for access to their space. The  
 1585 tenant agencies should designate their own “Controlled, Limited, Exclusion” areas and then  
 1586 evaluate if the facility’s PACS will accommodate their security needs. Each Federal Government  
 1587 tenant should ensure an appropriate PIV authentication mechanism from [Table 5-1](#) or [Table 5-2](#)  
 1588 is implemented for its designated areas. If the facility’s PACS cannot accommodate agencies’  
 1589 security needs, the tenant agencies should establish their own PACS. This may be considered an  
 1590 inner perimeter to the facility. In this case, the outer perimeter (i.e., access to the building) does  
 1591 not provide any authentication context. The individual agency should manage its own PACS

1592 server and user access. In many cases, the tenant agency will not have the authority to implement  
1593 security measures independently; however, relationships in place should be used to negotiate  
1594 security measures.

1595 In the event that it is not possible to establish individual PACS and the facility is evaluated at  
1596 FSL III or above, the tenant should consider the risk involved with inadequate security and make  
1597 future plans to improve security posture in accordance with the PIMM model in [Section 7](#).

## 1598 **6.4 Single-Tenant Campus**

1599 As opposed to a single-tenant facility, a campus is a collection of buildings, labs, and parking  
1600 spaces that are geographically co-located within a large perimeter. The large perimeter is  
1601 typically a fenced compound with a gate through which federal employees, contractors, and  
1602 visitors gain access. This type of a facility may be assessed at FSL III or above simply due to its  
1603 population and size. All the areas within the campus may not have the same security  
1604 requirements. Some spaces may be generally accessible to campus visitors, while some may be  
1605 specialized spaces such as a high-security lab or a chemical storage area that require a higher  
1606 level of security protection. In this scenario, one security measure for all spaces might be  
1607 overbearing and hamper business processes. The campus environment can be further  
1608 characterized as one big perimeter (outer perimeter) and multiple smaller (inner) perimeters.  
1609 There are interdependencies between these perimeters that are further elaborated through the  
1610 “Controlled, Limited, Exclusion” areas.

1611 In the campus environment, a cumulative effect of authentication is achieved as an individual  
1612 traverses boundaries from Unrestricted to Controlled to Limited to Exclusion areas. In other  
1613 words, authentication performed to gain access to a Controlled area should not be repeated to  
1614 gain access to a Limited area. Instead, a complementary evidence of identity should be used to  
1615 achieve multi-factor authentication of the individual who requests access to the Limited area.  
1616 The same logic applies to the Exclusion area.

1617 Spaces within a campus may have varying degrees of security. The campus may be subdivided  
1618 into “Controlled, Limited, Exclusion” areas. Moreover, a campus may have one or more areas  
1619 that are subdivided. A single Controlled or Limited area may be divided into sub-areas for  
1620 purposes of discretionary or Need-To-Know access control. As a matter of local policy, the use  
1621 of single-factor authentication may be sufficient to access sub-areas within the same Controlled  
1622 or Limited area.

1623 The following sections discuss the use of PIV authentication mechanisms in a campus  
1624 environment with multiple perimeters. This document does not address non-PIV authentication  
1625 mechanisms.

### 1626 **6.4.1 FSL I or II Campus Facility**

1627 [Figure 6-3](#) depicts a security posture of an FSL I or II campus facility. It includes one or more  
1628 Controlled areas that are available to authorized personnel. Since an FSL I or II campus facility  
1629 can be considered a low-risk area, a PACS may or may not be maintained to preclude  
1630 unauthorized entries. When PACS is maintained, SOME confidence in the identity of the  
1631 cardholder should be achieved. Implementation of PIV authentication mechanisms for  
1632 Controlled areas would be an appropriate countermeasure for security at this facility. PKI-CAK,

1633 SYM-CAK, and BIO are the three recommended authentication mechanisms in this  
 1634 environment. Note that these authentication mechanisms validate “something you have” or  
 1635 “something you are” (one-factor authentication).

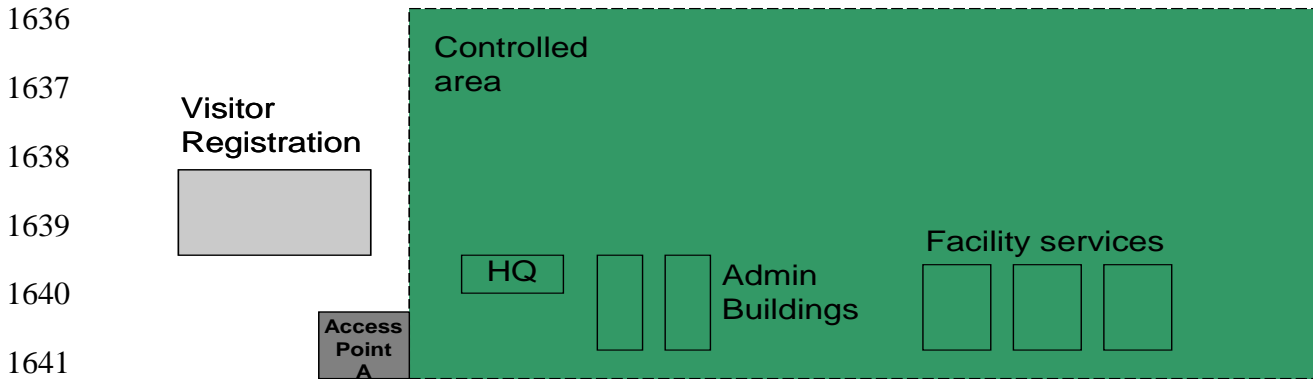


Figure 6-3: FSL I or II Campus Facility

1642

1643 **6.4.2 FSL III Campus Facility**

1644 [Figure 6-4](#) depicts a security posture of an FSL III campus facility. It includes one or more  
 1645 Controlled areas as well as Limited areas that are restricted to specific groups of individuals.  
 1646 Since an FSL III campus facility can be considered a moderate-risk facility, a PACS should  
 1647 provide additional security to the more valuable assets. HIGH confidence in the identity of the  
 1648 cardholder should be achieved for access to the Limited area. Note that the entire facility does  
 1649 not need the highest level of security. Access to the Limited area should be complemented with  
 1650 the authentication already completed at the Controlled area. Implementation of BIO(-A), PKI-  
 1651 AUTH or OCC-AUTH authentication mechanisms would be an appropriate countermeasure for  
 1652 the Limited area.<sup>16</sup> Note that these authentication mechanisms validate “something you are” or  
 1653 “something you know” (another factor in authentication).

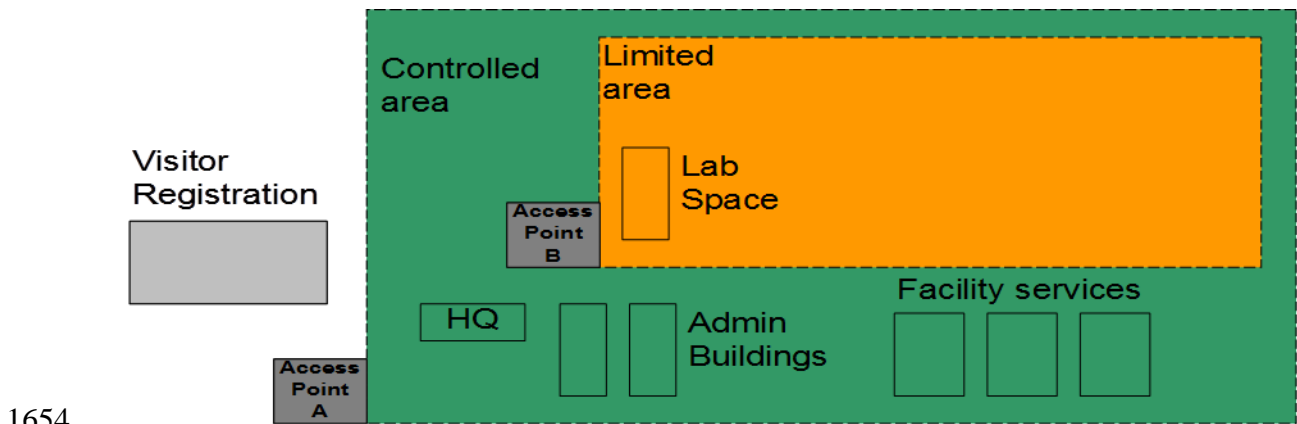
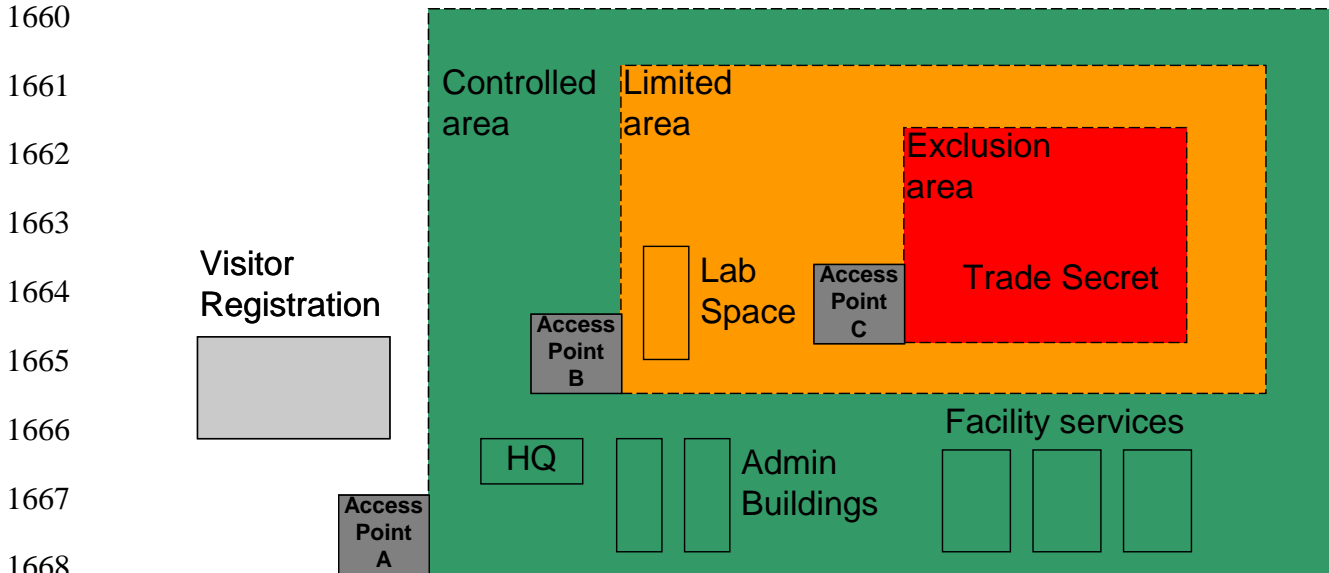


Figure 6-4: FSL III Campus Facility

<sup>16</sup> Use of the BIO authentication mechanism for access to the Limited area would require the ability to use authentication in context where it is known that the cardholder needed to perform the PKI-CAK, SYM-CAK, BIO-A, PKI-AUTH, or OCC-AUTH authentication mechanism in order to access the Controlled area.

### 1656 6.4.3 FSL IV or V Campus Facility

1657 [Figure 6-5](#) depicts a security posture of an FSL IV or V campus facility. It includes one or more  
 1658 Controlled areas, Limited areas, and Exclusion areas that are restricted to specific groups of  
 1659 individuals.



1669 **Figure 6-5: FSL IV or V Campus Facility**

1670 Although there is not a simple one-to-one mapping between FSLs and PACS authentication  
 1671 assurance levels at access control points, generally higher-risk areas will need stronger identity  
 1672 assurance. Since an FSL IV or V facility is considered a high-risk area, a PACS should achieve  
 1673 VERY HIGH confidence in the identity of the cardholder for access to the Exclusion areas. Note  
 1674 that the entire facility does not need the highest level of confidence in the identity of the  
 1675 cardholder. For access to the Exclusion areas, three-factor authentication should be achieved.  
 1676 This can be accomplished in multiple ways, as shown in [Figure 5-2](#).

### 1677 6.5 Multi-Tenant Campus

1678 The multi-tenant campus environment is similar to the single-tenant campus except that  
 1679 individual tenants will have their own security policies and the enforcement may be different. A  
 1680 tenant may benefit from the authentication mechanism(s) implemented at the outer perimeter;  
 1681 however, agencies may implement their own PACS within their space. In this case, if an agency  
 1682 were to benefit from other agencies' PACS, its PACS should have communication links with  
 1683 other PACS on the campus.

1684 Once again, each individual tenant within a campus should designate its own Controlled, Limited  
 1685 and Exclusion areas and identify appropriate PIV authentication mechanism(s) required for  
 1686 access to its space (see [Figure 5-1](#)). The tenants can then determine if they can simply use the  
 1687 campus PACS application, if they should add security by implementing an additional PIV  
 1688 authentication mechanism, or if they should implement a stand-alone PACS. Each individual  
 1689 tenant should ensure that appropriate PIV authentication mechanism(s) from [Figure 5-1](#) are  
 1690 implemented for its designated areas.

## 1691 **6.6 Role-Based Access Control**

1692 Authorization of identities enrolled in a PACS is viewed as separate from cardholder  
 1693 authentication. PACS may grant access only to cardholders who were enrolled and authorized in  
 1694 the PACS server prior to presenting their credentials for authentication, or they may make on-  
 1695 the-fly<sup>17</sup> access control decisions by evaluating the information on presented PIV Cards against a  
 1696 set of access control rules. Because PIV Cards contain only a few mandatory subject attributes  
 1697 (just the Agency Code, Employee Affiliation, and Investigation Status Indicator) that may be  
 1698 used for role-based access control, role or group permissions will usually be derived from off-  
 1699 card information.

1700 **Recommendation 6.1:** Because having on-card role and permission information  
 1701 would raise difficult challenges concerning update and revocation, PACS  
 1702 permissions should generally be stored in a PACS facilities-based component, such  
 1703 as a panel or controller database.

## 1704 **6.7 Temporary Badges**

1705 [\[HSPD-12\]](#) mandated a common identification and verification standard for federal employees  
 1706 and contractors for physical access to federally controlled facilities and logical access to  
 1707 federally controlled information systems. OMB Memorandum M-05-24 [\[M-05-24\]](#) clarifies the  
 1708 eligibility requirements for a PIV Card. Temporary employees and contractors are those  
 1709 individuals employed 6 month or less. These individuals are not required to receive a PIV Card  
 1710 and agencies are permitted to issue non-PIV Cards to these individuals. In addition, PIV  
 1711 cardholders who have forgotten their cards may be issued a non-PIV Card on a temporary basis.  
 1712 Temporary badges will thus be necessary (although in smaller numbers than before) for the  
 1713 indefinite future.

1714 An agency or facility should consider the relationship of temporary badges to PIV Cards and  
 1715 their PACS system(s) when selecting temporary badge products. Factors to consider during the  
 1716 procurement process include:

- 1717 + The [\[M-05-24\]](#) requirement that temporary badges be visually and electronically  
 1718 distinguishable from PIV Cards.
- 1719 + Capabilities and costs of enrollment stations, which will likely be local to the facility  
 1720 for best turnaround time.
- 1721 + The interoperability of temporary badges with PIV readers and authentication  
 1722 mechanisms (especially PKI-CAK for physical access).
- 1723 + The assignment of unique identifiers (FASC-N or UUID) to temporary badges, to  
 1724 foster interoperability with PIV readers.
- 1725 + The suitability of contactless-only temporary badges for physical access.

---

<sup>17</sup> Although making on-the-fly access control decisions is acceptable, it should be noted that this could introduce considerable delay in the end-user authorization process; and is therefore not recommended.

1726 + The performance, cost, and security tradeoffs between disposable and reusable  
1727 temporary badges.

1728 Many approaches to temporary badges are possible. However, a smart-card based solution that  
1729 leverages current infrastructure and interoperates with federal PIV Card readers and their  
1730 applications is recommended.

### 1731 **6.8 Disaster Response and Recovery Incidents**

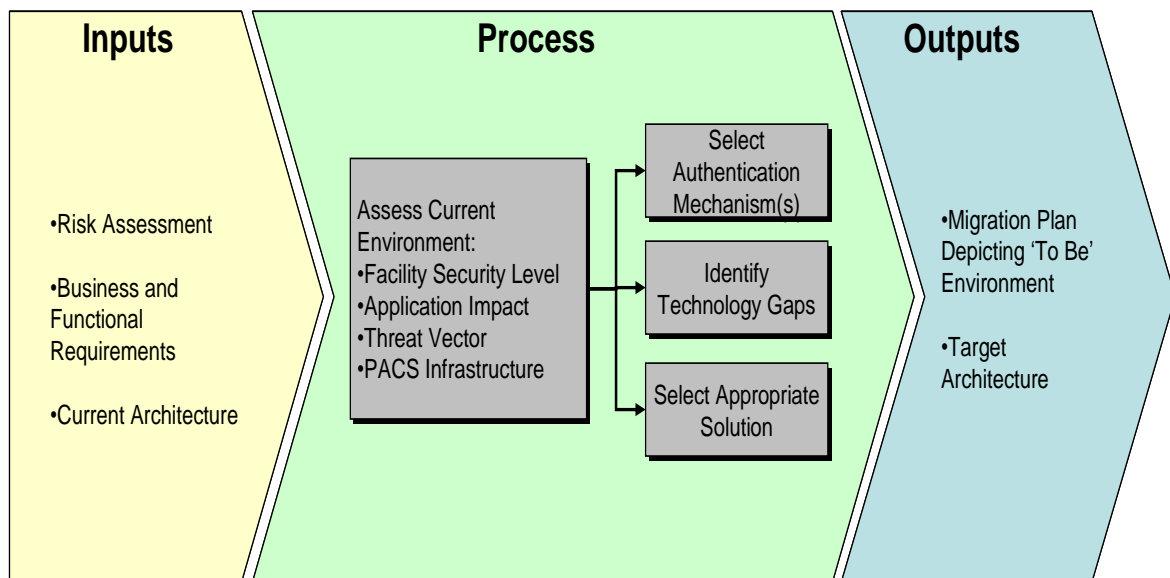
1732 In addition to the use of a PIV credential for cardholder authentication during routine everyday  
1733 use, the PIV credentials may also be used for access to federal facilities and federally controlled  
1734 areas internal to disaster response and recovery incident scenes. Federal agencies should consider  
1735 access for personnel from agencies with responsibilities under the National Response  
1736 Framework, National Incident Management System, National Infrastructure Protection Plan, and  
1737 the National Continuity Policy Implementation Plan when identifying and categorizing PACS  
1738 perimeters as protecting Controlled, Limited, and Exclusion areas. Subsequently, agencies  
1739 should apply appropriate (in accordance with [Table 5-3](#)) PIV authentication mechanisms to the  
1740 areas to ensure that incident management personnel, emergency response providers, and other  
1741 personnel (including temporary personnel) and resources likely needed to respond to a natural  
1742 disaster, act of terrorism, or other manmade disaster can be electronically authenticated in order  
1743 to attain movement internal to federally controlled facilities and areas within the incident scene.

## 1744 7. Migration Strategy

1745 Earlier sections provide the tools agencies will need to prepare a migration plan for PIV-enabling  
 1746 their PACS environment. This section discusses how these tools may be used to aid agencies  
 1747 with developing a migration plan.

### 1748 7.1 Project Planning

1749 Planning for a migration to PIV-enabled PACS should be viewed as an opportunity to modernize  
 1750 a legacy PACS. Given the threat environment, as described in [Section 2](#), migrating to PIV-  
 1751 enabled PACS enhances security, fosters trust among agencies, and creates cost efficiencies.  
 1752 This section provides a strategy for developing migration plans, as shown in [Figure 7-1](#).



1762 **Figure 7-1: Migration Strategy**

1763 Planning should be risk-based. Not all access points will require the same level of authentication  
 1764 assurance. Therefore, it is important to start with the risk assessment, which distills into PACS  
 1765 requirements. A migration plan can then be developed to help the agency transition to the desired  
 1766 PIV-enabled PACS environment.

### 1767 7.2 Risk Assessment

1768 Risk assessments provide a method of prioritizing the criticality of assets (or the impact of the  
 1769 loss of assets), threats, and countermeasure strategies. A structured process allows for the  
 1770 documentation of risks by subject matter experts based on their judgments and assumptions. The  
 1771 final product is a broad set of priorities, both physical and cyber, that contribute to the protection  
 1772 of the critical systems or functions.

1773 The input to this assessment is the understanding of risks in the current environment.  
 1774 Specifically, knowledge of existing vulnerabilities and the impact of attacks should be attained.  
 1775 [Section 2](#) provides attack vectors that must be well understood and acted upon. The goal should



1776 be to embed the countermeasures against the identified threats in migration to PIV-enabled  
1777 PACS. [\[HSPD-12\]](#) requires the standard to provide graduated levels of security in PIV  
1778 credentials. Note that the combination of one or more authentication mechanisms must be  
1779 employed to mitigate the counterfeiting, skimming, sniffing, social engineering, and cloning  
1780 threats.

### 1781 **7.3 Business and Functional Requirements**

1782 Each agency has a unique operational environment. Agencies vary in size, organizational  
1783 structure, and geographic topography. Moreover, their PACS requirements are driven by their  
1784 mission and by risk and vulnerability assessment. These factors resulted in pre-HSPD-12 PACS  
1785 environments that were site-specific and hardly interoperable with other agency  
1786 implementations. [\[HSPD-12\]](#) added two requirements to these implementations, namely  
1787 enhanced security and government-wide use of common identification. In other words, an  
1788 identity credential issued by agency A must be usable by agency B. Note that [\[HSPD-12\]](#) leaves  
1789 the authorization decision to individual agencies. [Section 4](#) provides characteristics of a PIV-  
1790 enabled PACS system that substantiates the goals of [\[HSPD-12\]](#). Agencies are encouraged to use  
1791 these characteristics to determine business and functional requirements applicable to their  
1792 environment.

### 1793 **7.4 Develop Migration Plan**

1794 Developing a migration plan requires a vision for PIV-enabled PACS operations. Specifically, a  
1795 new business process needs to be charted by those with legacy PACS to address the use of PIV  
1796 credentials. This business process will be dependent on the flexibility available in changing the  
1797 current environment. Some agencies may be renting spaces where access control is managed by  
1798 someone else. In the end, however, an agency should have a plan to use the PIV Card.

1799 The OMB Circular Number A-11, Part 7, Section 300: *Planning, Budgeting, Acquisitions, and*  
1800 *Management of Capital Assets* establishes policy for the planning, budgeting, acquisition, and  
1801 management of federal capital assets, and provides introduction on budget justification and  
1802 reporting requirements for major IT investments for federal agencies. OMB Circular A-11 spells  
1803 out the requirements for supporting several legislative directives including, but not limited to, the  
1804 Clinger-Cohen Act of 1996, which requires agencies to use a disciplined capital planning and  
1805 investment control process to acquire, use, maintain and dispose of information technology. In  
1806 particular, the Clinger-Cohen Act specifically instructs the head of each executive agency to  
1807 establish effective and efficient capital planning processes for selecting, managing, and  
1808 evaluating the results of all of its major investments in information systems.

1809 In migration planning, agencies should first determine the level of identity assurance required to  
1810 gain access to their resources. Guidelines on determining the level of identity assurance and  
1811 selecting a corresponding authentication mechanism are provided in [Section 5](#) of this document.  
1812 Once authentication mechanisms are selected, agencies will need to identify technology gaps in  
1813 the existing system. The gaps may be in the existing readers, control panels, or PACS servers.  
1814 [Section 6](#) discusses prominent scenarios and provides recommendations on filling technology  
1815 gaps.

1816 It is recommended that agencies plan to ultimately reach the highest level of authentication

1817 assurance that displays all the qualities identified in [Section 4.2](#). For this, guidance is provided in  
1818 the following section to enable agencies to progress in stages.

## 1819 **7.5 Migration Strategy & Tactics**

1820 Continuity of operations planning is essential to the success of a migration from legacy PACS to  
1821 PIV-enabled PACS. Planning lays the strategic framework that makes tactical, moment-to-  
1822 moment change management possible without catastrophic disruptions. This section suggests  
1823 sample strategies that can help the tactics succeed.

- 1824 1. Encourage the project staff to train themselves. In parallel with project planning,  
1825 create opportunities for the project staff to learn by doing on a small scale.
- 1826 2. Budget the project carefully. The total cost of ownership of a complete PIV-enabled  
1827 PACS system may be less than that of an upgraded system.
- 1828 3. In order for any PIV implementation to be successful, cross-departmental  
1829 collaboration is imperative. The needs of operational units left out of the process may  
1830 not be fully understood.
- 1831 4. Look for project synergies. For example, PACS modernization may contribute to  
1832 facility monitoring, and emergency access policies for First Responders may trigger  
1833 reevaluation of PACS role models and authentication methods.
- 1834 5. Develop a relationship with a senior partner. A “senior partner” should be farther  
1835 along in implementation, or have deeper expertise, than your organization.
- 1836 6. Consider acquiring access system components that are software and hardware  
1837 upgradeable to meet anticipated future requirements. For example, an agency may not  
1838 see the need for contact interfaces at this time; however, it should look to purchase  
1839 products that either have a dual-interface (contact and contactless capability) or plug-  
1840 in for contact card readers. The agency may have a choice to add contact readers  
1841 without replacing the reader infrastructure.
- 1842 7. Use the extra bandwidth to support remote monitoring and diagnosis, off-loading of  
1843 service elements, credential validation, cryptographic key management, and so on.
- 1844 8. Initially, buy multifunction readers that read both legacy and PIV Cards and can  
1845 perform all PIV electronic use cases—they can be used anywhere. Care should be  
1846 taken to avoid identifier collisions between two technologies. The agency should  
1847 design to the highest authentication assurance level that it thinks it may require in the  
1848 future.
- 1849 9. Keep performance in mind. Deploy systems integrators that are certified<sup>18</sup> and aim to  
1850 improve transaction performance.

---

<sup>18</sup> More information about GSA-certified HSPD-12 service providers can be found at <http://www.idmanagement.gov/qualified-hspd-12-service-providers>.

- 1851 10. As experience and the number of deployed readers grow, select more restricted and  
1852 cost-effective readers implementing just the required authentication mechanisms.
- 1853 11. Avoid long-term, side-by-side operation of legacy and PIV technologies.

## 1854 **7.6 PIV Implementation Maturity Model (PIMM)**

1855 In a document focused on the integration of PIV authentication mechanisms with PACS systems,  
1856 it is impossible to provide detailed recommendations on project planning for PACS  
1857 modifications or upgrades. The planning space is simply too large, due to the variations in local  
1858 requirements, the asset inventory and impact assessment, project size, the installed base of  
1859 electronic PACS systems, requirements for integration with other facilities' infrastructure  
1860 subsystems, etc.

1861 Instead, we recommend in this section a PIMM that can be used to measure the progress of a  
1862 facility or an agency towards a complete PIV implementation. The PIMM should be applied only  
1863 to facilities that have established a requirement for an electronic PACS.

1864 The PIMM is organized around the assumption of three enclosing perimeters: the Controlled  
1865 area, the Limited area, and the Exclusion area, shown in [Figure 5-1](#). In a general sense,  
1866 Controlled, Limited and Exclusion areas may be considered as the security perimeters consistent  
1867 with protection of low, moderate, and high impact assets, respectively. The following PIMM  
1868 maturity levels begin by achieving some capability and experience with PIV-based PACS:

- 1869 1. Maturity Level 1—Ad Hoc PIV Verification. A site has the ability to authenticate PIV  
1870 Cards by performing required authentication mechanisms on an ad hoc, on-demand  
1871 basis. For example, card and cardholder authentication is achieved with a handheld  
1872 device or a specific personal computer, for special or occasional uses.
- 1873 2. Maturity Level 2—Systematic PIV Verification to Controlled Area. At the outer  
1874 perimeter of the site (Controlled area), PIV Cards are accepted as proof of identity,  
1875 possibly in addition to currently deployed non-PIV PACS cards. A visitor registration  
1876 procedure exists to accept PIV Cards and if necessary convert PIV authentication to a  
1877 currently deployed non-PIV PACS card.
- 1878 3. Maturity Level 3—Access to Exclusion Areas by PIV or Exception Only. Access to  
1879 Exclusion areas (the most sensitive areas) is permitted by PIV authentication or  
1880 “exception” only. Here, exceptions are the exceptions to PIV issuance (e.g., less than  
1881 six months association). However, all access to exclusion areas is also subject to  
1882 authorization, and authorization would typically only be granted to PIV cardholders.  
1883 The exception case might be applied to exclusion areas for very important person  
1884 (VIP) visitors, for example. At Level 3, currently deployed non-PIV PACS cards are  
1885 not acceptable for authentication to Exclusion areas.
- 1886 4. Maturity Level 4—Access to Exclusion and Limited Areas by PIV or Exception Only.  
1887 Access to Limited areas (generally, those permitting clearance level- or role-based  
1888 authorization) is permitted by PIV authentication or exception only. At Level 4,  
1889 currently deployed non-PIV PACS cards are not acceptable for authentication to

1890 Exclusion or Limited areas. BIO, BIO-A, OCC-AUTH and PKI-AUTH are acceptable  
1891 authentication mechanisms in Limited Areas for authorized PIV cardholders.

1892 5. Maturity Level 5—Access to Exclusion, Limited, or Controlled Areas by PIV or  
1893 Exception Only. Access to Controlled areas (showing evidence of organizational  
1894 affiliation, or registration for a visitor, with or without escort) is permitted by PIV  
1895 authentication or exception only. At Level 5, currently deployed non-PIV PACS cards  
1896 are not acceptable for authentication to any areas. That is, only the PIV Card is an  
1897 acceptable credential for federal employees and contractors.

1898 The first two recommended maturity levels achieve some capability and experience with PIV  
1899 authentication mechanisms. This capability may exist in parallel with deployed PACS, and after  
1900 Level 2, the facility has achieved a capability to accept PIV Cards from visitors for access to  
1901 Controlled areas. The next three maturity levels displace deployed PACS to Exclusion, Limited,  
1902 and Controlled areas, beginning with the highest-impact areas (with, presumably, the smallest  
1903 number of access control points and authorized subjects) and moving to the Controlled area (with  
1904 the largest number of access control points and authorized subjects). At Level 5, the entire  
1905 facility has been converted to PIV authentication mechanisms at all access points, and/or all  
1906 subjects, where it is required and appropriate.<sup>19</sup>

1907 Maturity levels are progressive: for example, achieving Level 2 requires satisfying all of the  
1908 requirements of Level 1 in addition to the requirements of Level 2. Maturity levels can be  
1909 applied to individual facilities, or by extension to multiple facilities within a bureau or agency.  
1910 When applied to multiple facilities, a maturity level is achieved when each of the facilities in the  
1911 group has achieved the maturity level individually.

## 1912 **7.7 PIV-in-PACS Best Practices**

1913 [\[HSPD-12\]](#) mandates the establishment of government-wide identity credentials and the use of  
1914 these credentials in gaining physical access to federally controlled facilities. This implies that a  
1915 PACS application installed at these facilities should interoperate with the credential standardized  
1916 by [\[FIPS201\]](#), the PIV Card, issued by any government agency. The PIV Card interface and data  
1917 model requirements are fully specified through [\[FIPS201\]](#) and companion documents. For the  
1918 PACS application (or PIV-enabled PACS application), the following best practices are  
1919 recommended.

- 1920 + PACS application providers to employ products that are approved through the [\[FIPS](#)  
1921 [201 EP\]](#) for relevant product categories.
- 1922 + For each access transaction, once the applicable authentication mechanisms are  
1923 satisfied, all PACS access decisions are based on the utilization of an acceptable PIV  
1924 identifier (see [Section 5.4](#)).

---

<sup>19</sup> Note that some use of methods other than [\[FIPS201\]](#) authentication mechanisms will continue because not everyone is eligible or required to have a PIV Card.

- 1925 + The PACS application that uses PKI-AUTH or PKI-CAK authentication mechanisms  
1926 should support all of the asymmetric algorithms specified in Table 3-1 of [\[SP800-78\]](#).
- 1927 + Each facility should be mapped to the “Controlled, Limited, Exclusion” model and an  
1928 assignment of PIV authentication mechanisms to all access control points in  
1929 accordance with [Section 5.1](#).
- 1930 + Signature verification and path validation is performed on all signed data objects for  
1931 the PIV authentication mechanisms used. Failure of signature verification or path  
1932 validation results in a failed authentication attempt that does not admit a cardholder  
1933 for access.
- 1934 + Credential validation is implemented for all authentication mechanisms and failure of  
1935 the validation results in a failed authentication attempt that does not admit a  
1936 cardholder for access. Caching of validation results (with periodic recheck) is  
1937 preferred in certain circumstances (see [Section 5.6](#)).
- 1938 + The CHUID authentication mechanism should be implemented only when combined  
1939 with the VIS authentication mechanism, and only as part of a strategy to migrate to a  
1940 stronger authentication mechanism, such as PKI-CAK (see [Section 2.9](#) and [Section](#)  
1941 [5.3.1](#)).
- 1942 + Newly purchased systems must support other authentication mechanisms besides the  
1943 CHUID mechanism (e.g., PKI-CAK).
- 1944 + All PACS applications should operate at PIMM Level 5.
- 1945

## 1946 **Appendix A—Improving Authentication Transaction Times**

1947 The deprecation of the CHUID authentication mechanism marks the end for authentication based  
 1948 on reading a static identifier. With the deprecation of the CHUID authentication, however, PACS  
 1949 systems lose a mechanism that is by nature fast. The PKI-CAK authentication mechanism,  
 1950 which, as described in [Section 5.3.1](#), is the most logical replacement for the CHUID  
 1951 authentication mechanism, is computationally expensive. To approach transaction times closer to  
 1952 the CHUID authentication mechanism, optimizations are needed within the PIV Cards as well as  
 1953 with the readers and associated infrastructure. Transaction times for other authentication  
 1954 mechanisms are also important, and many of the recommendations in this section apply to other  
 1955 PIV authentication mechanisms as well.

1956 The steps of the PKI-CAK authentication mechanism can be described as follows:

- 1957 • The reader obtains information from the PIV Card that allows it to determine an identifier  
 1958 for the card and to determine the card's Card Authentication certificate.
- 1959 • The reader sends a challenge string to the PIV Card and requests an asymmetric operation  
 1960 in response.
- 1961 • The card responds to the previously issued challenge by signing it using the Card  
 1962 Authentication private key.
- 1963 • The relying system (reader or controller) uses the public key from the Card  
 1964 Authentication certificate to verify the response from the card.
- 1965 • The relying system verifies that the Card Authentication certificate is valid.
- 1966 • The relying system uses the identifier from the card to make an access control decision.

1967 Each of the steps above presents an opportunity for optimization.

1968 As a starting point, PCIs should consider performance when purchasing card stock, as the card is  
 1969 involved in four of the six steps above. When the PKI-CAK authentication mechanism is  
 1970 performed the PIV Card needs to perform a power-up self-test, perform a private key signature  
 1971 operation using the Card Authentication private key, and transmit data to the reader, so the  
 1972 performance of all of these steps is relevant to the overall performance of the card. [\[SP800-78\]](#)  
 1973 allows the Card Authentication key to be either a 2048-bit RSA key or an elliptic curve  
 1974 cryptography (ECC) P-256 key, and many cards support both cryptographic algorithms. When a  
 1975 card supports both algorithms, the performance of both algorithms should be considered.

1976 **Recommendation A.1:** Since ECC private key operations are generally faster than  
 1977 RSA private key operations, PCIs should consider issuing PIV Cards with ECC  
 1978 Card Authentication keys rather than RSA.

1979 The performance of the PIV Card is partially dependent upon the reader. The PKI-CAK  
 1980 authentication mechanism is usually performed over the contactless interface, with the PIV Card



1981 being powered by the reader's magnetic field, and cards will operate more slowly when they are  
 1982 underpowered. Improper installation of the reader may lead to the card being underpowered, and  
 1983 it may also create interference that makes communication between the card and the reader  
 1984 unreliable, which would also lead to increased transaction times.

1985 **Recommendation A.2:** Make use of Qualified HSPD-12 Service Providers<sup>20</sup> to  
 1986 ensure that PACS components are properly installed and that readers are properly  
 1987 tested and tuned to provide optimal performance.

1988 In order to maximize performance, the PIV Card needs to be held correctly within the reader's  
 1989 magnetic field. So, departments and agencies should provide information to their cardholders on  
 1990 the proper way to present their cards to the readers. Placing an image on the reader depicting the  
 1991 proper orientation of the card may also be helpful.

1992 Preregistration of PIV Cards can help to speed up many of the steps in the PKI-CAK  
 1993 authentication mechanism. If the card's Card Authentication certificate was obtained during the  
 1994 preregistration process then it doesn't need to be read from the card at the time of  
 1995 authentication.<sup>21</sup> Instead, the reader can obtain an identifier from the card (e.g., by reading the  
 1996 initial portion of the CHUID and extracting the FASC-N, GUID, or Cardholder UUID) and can  
 1997 then use the identifier to look up the certificate in the local cache. In addition, status information  
 1998 for the Card Authentication certificate may be obtained from a caching status proxy rather than  
 1999 performing certificate validation at the time of authentication.<sup>22</sup>

2000 In many PACS systems, data is transferred from the reader to the controller using the Wiegand  
 2001 protocol, which is very slow and only allows for one-way communication. Replacing the cabling  
 2002 between the reader and the controller to support fast two-way communication will provide  
 2003 several benefits: it will speed up the transfer of the card's identifier from the reader to the  
 2004 controller; it will enable the caching of the Card Authentication certificate at the controller; and  
 2005 it will allow the reader to offload more of the processing to the controller. Given that card  
 2006 readers tend to have very little processing power, it may be more efficient, if fast two-way  
 2007 communication is available, for the reader to send the results of the challenge to the controller  
 2008 rather than performing the signature verification itself.

2009 **Recommendation A.3:** Consider the benefits of upgrading the communications  
 2010 infrastructure between readers and controllers and then using the improved  
 2011 communication to move processing steps to the component that can perform the step  
 2012 most efficiently.

---

<sup>20</sup> Information about Qualified HSPD-12 Service Providers can be found at <http://www.idmanagement.gov/qualified-hspd-12-service-providers>.

<sup>21</sup> The PACS should be prepared to handle cases in which the Card Authentication certificate on the card was replaced (due to re-key) after the card was preregistered.

<sup>22</sup> Agencies should consider using online status checks when the most up to date PIV Card status is necessary.



## 2013 Appendix B—Recommendations

### 2014 Section 1.2

2015 **Recommendation 1.1:** This document recommends a risk-based approach for  
 2016 selecting appropriate PIV authentication mechanisms to manage physical access to  
 2017 Federal Government facilities and assets. Agencies should seek recommendations  
 2018 on PACS architectures, authorization, and facility protection from other sources.

### 2019 Section 2.9

2020 **Recommendation 2.1:** [\[Section 2\]](#) emphasizes the technical risks associated with  
 2021 the legacy CHUID authentication mechanism. If the CHUID authentication  
 2022 mechanism is used without restriction, operational risk increases as the value of  
 2023 targets and the availability of cloning and counterfeiting tools increase. [\[FIPS201\]](#)  
 2024 deprecates the use of the CHUID authentication mechanism since it provides  
 2025 ‘LITTLE or NO’ confidence in the identity of the cardholder, and so relying  
 2026 systems should phase out use of this authentication mechanism as soon as possible.  
 2027 NIST recommends transitioning away from the CHUID authentication mechanism  
 2028 using the strategy described in [Section 5.3.1](#).

### 2029 Section 4.1

2030 **Recommendation 4.1:** To obtain the full benefit of PIV interoperability, PIV  
 2031 project managers should ensure that relying systems have the capability to use all  
 2032 cryptographic algorithms that apply to the authentication mechanism(s) performed.  
 2033 Departments and agencies are required to procure and deploy [\[HSPD-12\]](#) products  
 2034 from the [\[FIPS 201 EP\]](#) Approved Products List where applicable,<sup>23</sup> and can use  
 2035 the PIMM presented in [Section 7](#) to measure progress toward the goal of  
 2036 interoperability.

### 2037 Section 4.2

2038 **Recommendation 4.2:** Once all appropriate authentication mechanisms are  
 2039 satisfied, access control decisions are made by comparing the selected PIV  
 2040 identifier (see [Section 5.4](#)) against the ACL entries.

2041 **Recommendation 4.3:** As agencies develop risk-based implementation plans, they  
 2042 will create and evolve plans for PIV Card issuance and application integration.  
 2043 They might consider which of the nine qualities are most relevant to agency goals  
 2044 and priorities, and derive further project objectives, metrics, and milestones from

---

<sup>23</sup> The Evaluation Program directly supports the acquisition process for implementing HSPD-12. OMB Memorandum [\[M-06-18\]](#) directs that agencies must acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications in order to ensure government-wide interoperability.

2045 those qualities. They should also consider the relation of [\[HSPD-12\]](#) to [\[FISMA\]](#)  
2046 requirements, and examine the potential for cost tradeoffs where PIV can replace  
2047 more expensive authentication methods.

#### 2048 Section 4.3

2049 **Recommendation 4.4:** Operational metrics should be designed to measure actual  
2050 benefits over the operational lifetime of the PIV System. They may be derived by  
2051 formulating each of the expected benefits above as a service quality metric, e.g., for  
2052 “integrated system,” service quality could be defined as the percentage of PACS  
2053 registrations that are performed automatically by provisioning from the PIV  
2054 issuance system.

#### 2055 Section 4.4

2056 **Recommendation 4.5:** Maximum benefit will be obtained from the PIV System  
2057 when it is adequately supported by infrastructure. Infrastructure upgrades may be  
2058 justified, especially to improve communication between PACS system elements  
2059 (e.g., support two-way communication).

#### 2060 Section 5.1.2

2061 **Recommendation 5.1:** Agencies currently implementing the CHUID  
2062 authentication mechanism are highly encouraged to transition to another PIV  
2063 authentication mechanism as soon as possible (see [Section 5.3.1](#) for a suggested  
2064 migration strategy).

#### 2065 Section 5.1.3

2066 **Recommendation 5.2:** NIST recommends that agencies transition to use of the  
2067 PKI-CAK authentication mechanism at access points that only require single-factor  
2068 authentication. (See [Section 5.3.1](#) for a suggested transition strategy).

#### 2069 Section 5.1.5

2070 **Recommendation 5.3:** Biometric readers, especially those used at access points to  
2071 Limited and Exclusion areas, should have a proven capability to accept live fingers  
2072 and reject artificial fingers. Biometric readers, especially unattended readers in an  
2073 Unrestricted area, should be physically hardened to protect against direct electrical  
2074 compromise.

#### 2075 Section 5.3

2076 **Recommendation 5.4:** Authentication assurance will be increased if a PACS uses  
2077 relevant information from previous access control decisions (“context”) when  
2078 making a new access control decision. For example, if a cardholder attempts to pass  
2079 from a Controlled to a Limited area, the PACS could require that the cardholder  
2080 was recently allowed access to the Controlled area. Historically, rigorous

2081 implementation of this concept required person-traps and exit tracking, but partial  
2082 implementations have significant value, and could be strengthened by new  
2083 technology and systems integration.

#### 2084 Section 5.5

2085 **Recommendation 5.5:** The CHUID may be collected at registration, but it should  
2086 not be retained. A stored CHUID presents a risk, because it can be copied and used  
2087 to gain access at access points that have not yet migrated away from use of the  
2088 CHUID authentication mechanism. Data elements (e.g., the FASC-N and Global  
2089 Unique Identifier (GUID)) may be extracted from the CHUID and retained, as may  
2090 a hash of the CHUID. *NIST strongly recommends against the storage of complete*  
2091 *CHUIDs in relying systems.*

2092 **Recommendation 5.6:** PKI-AUTH and PKI-CAK authentication mechanisms  
2093 should be implemented by a PACS reader capable of full certificate path validation,  
2094 either online or using a caching status proxy. Agencies should consider using  
2095 online status checks when the most up to date PIV Card status is necessary or if  
2096 access is being granted to Exclusion areas. If a caching status proxy is used, the  
2097 certificates should be captured when the PIV Card is registered to the PACS.

#### 2098 Section 5.6

2099 **Recommendation 5.7:** Online credential validation should be implemented for all  
2100 of the PIV authentication mechanisms whenever most up-to-date status is  
2101 necessary.

2102 **Recommendation 5.8:** Caching techniques should be used to implement  
2103 credential validation to get improved performance or when online, on-demand  
2104 credential validation is not possible. It is also recommended that the cached data be  
2105 protected against tampering.

2106 **Recommendation 5.9:** Credential status checks that indicate that the certificate  
2107 has been revoked should always prevent a cardholder from access.

2108 **Recommendation 5.10:** Credential validation must be performed on all signed  
2109 data objects required by the authentication mechanism in use. Path validation of a  
2110 certificate should employ either online or cached status checks depending on the  
2111 authentication use case, the PACS environment and the performance requirements.  
2112 Because path validation is a part of credential validation, both services can be  
2113 economically implemented by a single PACS service component.

#### 2114 Section 6.6

2115 **Recommendation 6.1:** Because having on-card role and permission information  
2116 would raise difficult challenges concerning update and revocation, PACS  
2117 permissions should generally be stored in a PACS facilities-based component, such  
2118 as a panel or controller database.

2119 Appendix A

2120 **Recommendation A.1:** Since ECC private key operations are generally faster than  
2121 RSA private key operations, PCIs should consider issuing PIV Cards with ECC  
2122 Card Authentication keys rather than RSA.

2123 **Recommendation A.2:** Make use of Qualified HSPD-12 Service Providers<sup>24</sup> to  
2124 ensure that PACS components are properly installed and that readers are property  
2125 tested and tuned to provide optimal performance.

2126 **Recommendation A.3:** Consider the benefits of upgrading the communications  
2127 infrastructure between readers and controllers and then using the improved  
2128 communication to move processing steps to the component that can perform the step  
2129 most efficiently.

2130

---

<sup>24</sup> Information about Qualified HSPD-12 Service Providers can be found at <http://www.idmanagement.gov/qualified-hspd-12-service-providers>.

## 2131 **Appendix C—FASC-N Uniqueness**

2132 Access control decisions can be made by comparing PIV identifiers (see [Section 5.4](#)) against the  
 2133 ACL entries. While any of the PIV identifiers may be used in making access control decisions,  
 2134 within the limitations described in [Section 5.4](#), this appendix discusses the use of the FASC-N, or  
 2135 portions of the FASC-N, for making access control decisions.

2136 Three components of the FASC-N, the Agency Code, System Code, and Credential Number,  
 2137 constitute the FASC-N Identifier. An individual's FASC-N Identifier is unique among all  
 2138 cardholders when the complete three-element subset of the FASC-N is used for comparison.  
 2139 There will be no collisions since all the cardholders have been assigned unique numbers. An  
 2140 ACL pattern may match the entire FASC-N, just the Agency Code, or the Agency Code and  
 2141 System Code (e.g., all PIV Cards issued to one agency, or to one site in one agency) without  
 2142 introducing dangerous collisions or ambiguities across agencies. The values of additional FASC-  
 2143 N fields may be included in the identifiers that are compared against the ACL entries.

2144 This restricts the access control comparison to one of three cases when using the FASC-N:

- 2145 1. the Agency Code alone (i.e., all PIV Cards with the same Agency Code are accepted);
- 2146 2. the Agency Code and System Code only (i.e., all PIV Card with the same Agency  
 2147 Code and System Code are accepted); or
- 2148 3. the Agency Code, System Code, and Credential Number (i.e., a uniquely identified  
 2149 PIV Card).

2150 Any of these cases may also include comparison of additional FASC-N values such as the  
 2151 Credential Series, Individual Credential Issue, Organizational Identifier, or Person Identifier.<sup>25</sup>

2152 The FASC-N data fields are defined as fixed length values of Binary Coded Decimal digits. The  
 2153 complete subset of three data fields is 14 decimal digits in length, as stored on the PIV Card.  
 2154 Other representations of the FASC-N Identifier, for example a binary representation, may be  
 2155 used off card, provided that they are isomorphic with respect to pattern matching. The following  
 2156 examples demonstrate the possible uses of FASC-N in a PIV-enabled PACS application.

### 2157 **C.1 Full FASC-N Comparison**

2158 The following table shows a successful match against an ACL pattern consisting of a full FASC-  
 2159 N comparison. These examples show an organization-specific access control policy that includes  
 2160 the comparison of all FASC-N fields.

---

<sup>25</sup> [\[SP800-73\]](#) allows issuers to populate the FASC-N's Credential Series, Individual Credential Issue, Organizational Identifier, and Person Identifier fields with all zeros, so these fields may not always provide useful information for comparison.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8377	8377
Credential Number	123456	123456
Credential Series	1	1
Individual Credential Issue	1	1
Person Identifier	1234567890	1234567890
Organizational Category	1	1
Organizational Identifier	0010	0010
Person/Organization Association Category	1	1

2161

2162

2163

The following table shows an unsuccessful match against an ACL pattern consisting of full FASC-N comparison.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8377	8377
Credential Number	123456	234567
Credential Series	1	1
Individual Credential Issue	1	1
Person Identifier	1234567890	1234567890
Organizational Category	1	1
Organizational Identifier	0010	0010
Person/Organization Association Category	1	1

2164

2165 **C.2 FASC-N Identifier Comparison**

2166 The following table shows a successful match against an ACL pattern consisting of one specific  
2167 FASC-N Identifier.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8377	8377
Credential Number	123456	123456

2168 The following table shows an unsuccessful match against an ACL pattern consisting of one  
2169 specific FASC-N Identifier.  
2170

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8367	8377
Credential Number	123456	123456

2171

2172 **C.3 Partial FASC-N Comparison**

2173 The following table shows a successful match against an ACL pattern consisting of an Agency  
2174 Code and the System Code. The “x” symbols represent “don’t care” decimal digits.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	3728
System Code	8391	8391
Credential Number	654321	xxxxxxx

2175 The following table shows an unsuccessful match against an ACL pattern consisting of an  
2176 Agency Code and the System Code.  
2177

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3628	3728



System Code	8377	8377
Credential Number	123456	xxxxxx

2178  
2179  
2180

The following table shows a disallowed pattern that is not an initial string of the FASC-N Identifier.

FIELD NAME	PIV Card FASC-N	ACL FASC-N Pattern
Agency Code	3728	37xx
System Code	8377	83xx
Credential Number	123456	xxxxxx

2181

2182 **C.4 Isomorphic FASC-N Comparison**

2183 The following table shows a successful match against an ACL pattern, with the FASC-N  
2184 Identifier and the upper and lower bounds of the ACL pattern represented in hexadecimal. The  
2185 match succeeds because the presented FASC-N Identifier is in the closed interval [LB, UB]. This  
2186 example is the same as the MATCH example of [C.2](#), with a shift in representation from decimal  
2187 to hexadecimal.

FIELD VALUE	PIV Card FASC-N	ACL Pattern LB	ACL Pattern UB
Hexadecimal Value	21E9E156BBB1	21E9DBE03300	21E9E1D613FF

2188  
2189  
2190  
2191  
2192  
2193

The following table shows an unsuccessful match against an ACL pattern, with the FASC-N Identifier and the upper and lower bounds of the ACL pattern represented in hexadecimal. The match fails because the presented FASC-N Identifier is not in the closed interval [LB, UB]. This example is the same as the NO MATCH example of [C.2](#), with a shift in representation from decimal to hexadecimal.

FIELD VALUE	PIV Card FASC-N	ACL Pattern LB	ACL Pattern UB
Hexadecimal Value	21010BD3F280	21E9DBE03300	21E9E1D613FF

2194

## 2195 Appendix D—Possible PIV Authentication Mechanisms in PACS

2196 [Section 5.3](#) provides recommendations for selecting the authentication mechanisms to use at  
 2197 access points. For access to Controlled areas, it considers any PIV authentication mechanism that  
 2198 provides at least SOME confidence in the identity of the cardholder to be acceptable (see Table  
 2199 6-2 in [\[FIPS201\]](#)). For access to Limited areas, it recommends use of a PIV authentication  
 2200 mechanism that provides either HIGH or VERY HIGH confidence in the identity of the  
 2201 cardholder (see Table 6-2 in [\[FIPS201\]](#)). It also recommends that the single-factor BIO  
 2202 authentication mechanism only be used to grant access to a Limited area if the PACS can ensure  
 2203 that the cardholder needed to authenticate at another access point with a different authentication  
 2204 mechanism in order to get to the Limited access point (authentication in context). For access to  
 2205 Exclusion areas, it recommends use of a PIV authentication mechanism that provides for at least  
 2206 two-factor authentication at the access point (see [Table 5-1](#)), and that the PACS ensure that all  
 2207 three factors are authenticated prior to granting access to Exclusion area (possibly through  
 2208 authentication in context).

2209 This appendix provides a complete list of possible PIV authentication mechanism combinations  
 2210 that are available for application to federal facilities. The following acronyms are used in this  
 2211 appendix, where each acronym represents the set of PIV authentication mechanisms that provide  
 2212 the specified factor(s) of authentication.

Acronym	PIV Authentication Mechanisms
H (One factor – something you have)	PKI-CAK, SYM-CAK
A (One factor – something you are)	BIO
HK (Two factors – something you have, something you know)	PKI-AUTH
HA (Two factors – something you have, something you are)	BIO-A, OCC-AUTH, PKI-AUTH <sup>26</sup>
HKA (Three factors – something you have, something you know, something you are)	PKI-CAK+BIO(-A), SYM-CAK+BIO(-A)

2213 Note that the table above only lists individual PIV authentication mechanisms that correspond to  
 2214 each acronym, except for the combinations as identified in [Section 5.1](#). However, other PIV  
 2215 authentication mechanism combinations that provide the same set of authentication factors can  
 2216 be derived. For combined authentication mechanisms it is assumed that the combination is  
 2217 completed using the same interface. For example, in the case of SYM-CAK+BIO, both SYM-  
 2218 CAK and BIO would need to be performed over the contact interface, since BIO is performed  
 2219 over the contact interface as per [Table 5-1](#).

2220 When an access point separates a protective area from an Unrestricted area or when  
 2221 authentication in context cannot be used, [Section 5.3](#) recommends that one of the following be  
 2222 used:

---

<sup>26</sup> When used with OCC.

- 2223 • For access to a Controlled area – any authentication mechanism listed above (H, A, HK,  
2224 HA, or HKA)
- 2225 • For access to a Limited area – any two- or three-factor authentication mechanism listed  
2226 above (HK, HA, or HKA)
- 2227 • For access to an Exclusion area – any three-factor authentication mechanism listed above  
2228 (HKA)

2229 The tables below show all possible PIV authentication mechanism combinations that may be  
2230 used when authentication in context can be utilized. The first table shows all possible options for  
2231 accessing a Limited area when the Limited area can only be accessed from within a Controlled  
2232 area. It shows that if only “something you are” was authenticated to access the Controlled area  
2233 (row 2), then the options for granting access to the Limited area are the same as if authentication  
2234 in context were not available, however, if “something you have” is authenticated to access the  
2235 Controlled area (row 1), then there is the additional option of only authenticating “something you  
2236 are” (BIO) before granting access to the Limited area.

	Access Point A (Controlled)	Access Point B (Limited)
1	H, HK, HA, or HKA	A, HK, HA, or HKA
2	A	HK, HA, or HKA

2237 The second table shows all possible combinations when a facility has Controlled, Limited, and  
2238 Exclusion areas, Limited areas can only be accessed from within Controlled areas, and Exclusion  
2239 areas can only be accessed from within Limited areas.

	Access Point A (Controlled)	Access Point B (Limited)	Access Point C (Exclusion)
1	H	A or HA	HK or HKA
2	H	HK	HA or HKA
3	H	HKA	HK, HA, or HKA
4	A	HK or HKA	HK, HA, or HKA
5	A	HA	HK or HKA
6	HK	A, HA, or HKA	HK, HA, or HKA
7	HK	HK	HA or HKA
8	HA	A or HA	HK or HKA
9	HA	HK or HKA	HK, HA, or HKA
10	HKA	A, HK, HA, or HKA	HK, HA, or HKA

2240 The “Access Point C” column shows the authentication mechanisms that can be used to access  
2241 an Exclusion area given the authentication mechanisms used to access the surrounding  
2242 Controlled and Limited areas (the “Access Point A” and “Access Point B” columns). For  
2243 example, rows 4 and 5 show (as did row 2 in the first table) that if only “something you are” was  
2244 authenticated to access the Controlled area, then two- or three-factor authentication is required at  
2245 the Limited access point (HK, HA, or HKA). Row 4 shows that if HK or HKA is used at the

2246 Limited access point after A (i.e., BIO) is used at the Controlled access point, then any two- or  
 2247 three-factor authentication mechanism may be used at an Exclusion access point, whereas row 5  
 2248 shows that if HA is used at the Limited access point after A (i.e., BIO) is used at the Controlled  
 2249 access point, then “something you know” needs to be authenticated at the Exclusion access point  
 2250 (HK or HKA).

2251 The third and fourth tables show all combinations in cases in which authentication in context can  
 2252 be used, but there are access points that separate areas that differ by more than one impact level.  
 2253 The third table shows the combinations for cases in which Exclusion areas can be accessed from  
 2254 within Controlled areas, and the fourth table shows combinations for cases in which Limited  
 2255 areas can be accessed from Unrestricted areas and Exclusion areas can be accessed from within  
 2256 those Limited areas.

	Access Point A (Controlled)	Access Point B (Exclusion)
1	H	HKA
2	A or HA	HK or HKA
3	HK	HA or HKA
4	HKA	HK, HA, or HKA

2257

	Access Point A (Limited)	Access Point B (Exclusion)
1	HK	HA or HKA
2	HA	HK or HKA
3	HKA	HK, HA, or HKA

2258

2259

**Appendix E—References**

- [FIPS199] Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information System*, February 2004. <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf> [accessed 1/20/15].
- [FIPS201] Federal Information Processing Standard 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013. <http://dx.doi.org/10.6028/NIST.FIPS.201-2>.
- [FIPS 201 EP] *FIPS 201 Evaluation Program*. <http://www.idmanagement.gov/ficam-testing-program> [accessed 2/4/15].
- [FISMA] *Federal Information Security Modernization Act of 2014*, Pub. L. 113-283, 128 Stat 3073. <https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf> [accessed 5/18/15].
- [HSPD-12] Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004. <http://www.dhs.gov/homeland-security-presidential-directive-12> [accessed 11/5/2015]
- [ISC-RMP] *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, 1st edition, August 2013. [http://www.dhs.gov/sites/default/files/publications/ISC\\_Risk-Management-Process\\_Aug\\_2013.pdf](http://www.dhs.gov/sites/default/files/publications/ISC_Risk-Management-Process_Aug_2013.pdf) [accessed 12/16/2015].
- [ISO/IEC7816] (Parts 3:2006, 4: 2013, 5:2004, 6:2004, 8:2004, and 9:2004), *Information technology — Identification cards — Integrated circuit(s) cards with contacts*.
- [ISO/IEC14443] (Parts 1:2008, 2:2010, 3:2011, and 4:2008) *Identification cards - Contactless integrated circuit(s) cards – Proximity cards*
- [M-04-04] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003. <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf> [accessed 1/20/15].
- [M-05-24] OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005. <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf> [accessed 1/20/15].

- [M-06-18] OMB Memorandum M-06-18, *Acquisition of Products and Services for Implementation of HSPD-12*, June 2006.  
<https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-18.pdf> [accessed 12/03/15].
- [SKIMMER] OMB Memorandum M-08-01, *HSPD-12 Implementation Status*, October 2007.  
<http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-01.pdf> [accessed 1/20/15].
- [MINEXII] NIST Interagency Report 7477, Revision II, *MINEX II: Performance of Fingerprint Match-on-Card Algorithms, Phase IV Report*, March 15, 2011.  
[http://www.nist.gov/customcf/get\\_pdf.cfm?pub\\_id=908096](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=908096) [accessed 1/20/15].
- [PIV-I CP] Federal Public Key Infrastructure Policy Authority (FPKIPA), *Personal Identity Verification Interoperable (PIV-I) Certification Process*, Version 1.1, January 20, 2015,  
[http://www.idmanagement.gov/sites/default/files/documents/PIVI\\_Certification\\_Process\\_V1.1\\_0.pdf](http://www.idmanagement.gov/sites/default/files/documents/PIVI_Certification_Process_V1.1_0.pdf) [accessed 12/03/15].
- [PIV-I FAQ] Federal Identity, Credentialing, and Access Management (FICAM), *Personal Identity Verification Interoperable (PIV-I), Frequently Asked Questions (FAQ)*, Version 1.0, June 28 2010.  
[http://www.idmanagement.gov/sites/default/files/documents/PIV-I\\_FAQ.pdf](http://www.idmanagement.gov/sites/default/files/documents/PIV-I_FAQ.pdf) [accessed 11/30/15].
- [PIV-I NFI] Federal CIO Council, *Personal Identity Verification Interoperability For Non-Federal Issuers*, Version 1.1, July 2010.  
<http://www.idmanagement.gov/documents/personal-identity-verification-piv-interoperability-non-federal-issuers> [accessed 8/15/15].
- [PHYSEC] Field Manual 3-19.30, *Physical Security*. Headquarters, Department of the Army, United States of America, January 8, 2001.
- [RFC5280] Request for Comments (RFC) 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Internet Engineering Task Force (IETF), May 2008.  
<http://www.ietf.org/rfc/rfc5280.txt> [accessed 12/03/15].
- [SECTION508] *Section 508 of the Rehabilitation Act of 1973, as amended*, 29 U.S.C. §794(d), <http://www.section508.gov> [accessed 1/20/15].
- [SKIMMER] I. Kirschenbaum and A. Wool, “How to Build a Low-Cost, Extended-Range RFID Skimmer,” *Proceedings of the 15th USENIX Security Symposium (Security '06)*, Vancouver, British Columbia, Canada, July 31 – August 4, 2006, USENIX Association: Berkeley, California, 2006, pp. 43-57.

- [https://www.usenix.org/legacy/event/sec06/tech/full\\_papers/kirschenbaum/kirschenbaum.pdf](https://www.usenix.org/legacy/event/sec06/tech/full_papers/kirschenbaum/kirschenbaum.pdf) [accessed 12/03/15].
- [SP800-63] NIST Special Publication 800-63-2, *Electronic Authentication Guideline*, August 2013, <http://dx.doi.org/10.6028/NIST.SP.800-63-2>.
- [SP800-73] NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, May 2015. <http://dx.doi.org/10.6028/NIST.SP.800-73-4>.
- [SP800-76] NIST Special Publication 800-76-2, *Biometric Specifications for Personal Identity Verification*, July 2013. <http://dx.doi.org/10.6028/NIST.SP.800-76-2>.
- [SP800-78] NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, May 2015. <http://dx.doi.org/10.6028/NIST.SP.800-78-4>.
- [SP800-79] NIST Special Publication 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, July 2015. <http://dx.doi.org/10.6028/NIST.SP.800-79-2>.
- [SP800-87] NIST Special Publication 800-87 Revision 1, *Codes for the Identification of Federal and Federally-Assisted Organizations*, April 2008. [http://csrc.nist.gov/publications/nistpubs/800-87-Rev1/SP800-87\\_Rev1-April2008Final.pdf](http://csrc.nist.gov/publications/nistpubs/800-87-Rev1/SP800-87_Rev1-April2008Final.pdf).
- [TIG SCEPACS] *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.3*, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, December 20, 2005. <https://www.idmanagement.gov/sites/default/files/documents/PACS.pdf> [accessed 11/6/2015].



## 2261 **Appendix F—Terminology**

2262 The following terms are used in this document.

Access Control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
Access Control List	A list of (identifier, permissions) pairs associated with a resource or an asset. As an expression of security policy, a person may perform an operation on a resource or asset if and only if the person's identifier is present in the access control list (explicitly or implicitly), and the permissions in the (identifier, permissions) pair include the permission to perform the requested operation.
Asymmetric Keys:	Two related keys, a public key and a private key, that are used to perform complementary operations, such as authentication, encryption and decryption, signature generation and signature verification.
Assurance Level (or E-Authentication Assurance Level)	A measure of trust or confidence in an authentication mechanism defined in <a href="#">[M-04-04]</a> and NIST Special Publication (SP) 800-63 <a href="#">[SP 800-63]</a> , in terms of four levels: <ul style="list-style-type: none"> <li>• Level 1: LITTLE OR NO confidence</li> <li>• Level 2: SOME confidence</li> <li>• Level 3: HIGH confidence</li> <li>• Level 4: VERY HIGH confidence</li> </ul>
Authentication	The process of establishing confidence of authenticity; in this case, in the validity of a person's identity. In this publication, authentication often means the performance of a PIV authentication mechanism.
Authentication in Context	Authentication in context is a concept in which PACS may benefit from previous authentication within nested areas in a facility. The PACS may use information from previous access control decisions ("context") when making a new access control decision.
Authorization	In this publication, a process that associates permission to access a resource or asset with a person and the person's identifier(s).
Authenticator	A memory, possession, or quality of a person that can serve as proof of identity, when presented to a verifier of the appropriate kind. For example, passwords, cryptographic keys, and biometrics

	are authenticators.
BIO or BIO-A	A <a href="#">[FIPS201]</a> authentication mechanism that is implemented by using a fingerprint or iris images data object sent from the PIV Card to the PACS and which is matched to the cardholder’s live scan. Note that the shorthand “BIO(-A)” is used throughout the document to represent both BIO and BIO-A authentication mechanisms.
Building Security Committee	A committee consisting of representatives of Federal tenants in a facility, and possibly the building owner or management. The committee is responsible for building-specific security issues and approval of security policies and practices.
Card UUID	The Card UUID is a UUID that is unique for each card, and is a required data element on all <a href="#">[SP800-73]</a> compliant PIV Cards.
Cardholder	An individual possessing an issued PIV Card.
Cardholder Unique Identifier (CHUID)	A <a href="#">[FIPS201]</a> authentication mechanism that is implemented by transmission of the CHUID data object from the PIV Card to PACS, or the PIV Card data object of the same name.
Cardholder UUID	The Cardholder UUID is a UUID that is a persistent identifier for the cardholder. This UUID is an optional data element on <a href="#">[SP800-73]</a> compliant PIV Cards.
Certificate	A data object containing a subject identifier, a public key, and other information that is digitally signed by a certification authority. Certificates convey trust in the relationship of the subject identifier to the public key.
Certificate Revocation List	A list of revoked public key certificates created and digitally signed by a certification authority. See <a href="#">[RFC5280]</a>
Certification Authority	A trusted entity that issues and revokes public key certificates.
Cloning	In this publication, a process to create a verbatim copy of a PIV Card, or a partial copy sufficient to perform one or more authentication mechanisms as if it were the original card.
Contact Reader	A smart card reader that communicates with the integrated circuit chip in a smart card using electrical signals on wires touching the smart card’s contact pad. The PIV contact interface is standardized by International Organization of Standards / International Electrotechnical Commission (ISO/IEC) 7816-3 <a href="#">[ISO/IEC7816]</a> .

Contactless Reader	A smart card reader that communicates with the integrated circuit chip in a smart card using radio frequency (RF) signaling. The PIV contactless interface is standardized by <a href="#">[ISO/IEC 14443]</a> .
Controller (or Control Panel, or Panel)	A device located within the secure area that communicates with multiple PIV Card readers and door actuators, and with the Head End System. The PIV Card readers provide cardholder information to the controller, which it uses to make access control decisions and release door-locking mechanisms. The controller communicates with the Head End System to receive changes in access permissions, report unauthorized access attempts and send audit records and other log information. Most modern controllers can continue to operate properly during periods of time in which communication with the Head End is disrupted and can journal transactions so that they can be reported to the Head End when communication is restored.
Counterfeiting	In this publication, the creation of a fake ID card that can perform one or more authentication mechanisms, without copying a legitimate card (see Cloning).
Credential	In this publication, a collection of information about a person, attested to by an issuing authority. A credential is a data object (e.g., a certificate) that can be used to authenticate the cardholder. One or more data object credentials may be stored on the same physical memory device (e.g., a PIV Card).
Credential Validation	The process of determining if a credential is <i>valid</i> , i.e., it was legitimately issued, its activation date has been reached, it has not expired, it has not been tampered with, and it has not been revoked, suspended, or revoked by the issuing authority.
Digital Signature	A data object produced by a digital signature method, such as Rivest, Shamir, Aldeman (RSA) or the Elliptic Curve Digital Signature Algorithm (ECDSA), that when verified provides strong evidence of the origin and integrity of the signed data object.
Federal Agency Smart Credential Number (FASC-N)	As required by <a href="#">[FIPS201]</a> , the FASC-N is one of the primary identifiers on the PIV Card for physical access control. The FASC-N is a fixed length (25 byte) data object, specified in <a href="#">[TIG SCEPACS]</a> , and included in several data objects on a PIV Card.
FASC-N Identifier	The FASC-N shall be in accordance with <a href="#">[TIG SCEPACS]</a> . A subset of FASC-N, a FASC-N Identifier, is a unique identifier as described in <a href="#">[TIG SCEPACS]</a> . Section 2.1, 10 <sup>th</sup> paragraph of <a href="#">[TIG SCEPACS]</a> states “For full interoperability of a PACS it must at a minimum be able to distinguish fourteen digits (i.e., a combination

of an Agency Code, System Code, and Credential Number) when matching FASC-N based credentials to enrolled card holders.” Also, Section 6.6, 3<sup>rd</sup> paragraph of [\[TIG SCEPACS\]](#) states, “The combination of an Agency Code, System Code, and Credential Number is a fully qualified number that is uniquely assigned to a single individual.” The Agency Code is assigned to each Department or Agency by Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations* [\[SP800-87\]](#). The subordinate System Code and Credential Number value assignment is subject to Department or Agency policy, provided that the FASC-N Identifier (i.e., the concatenated Agency Code, System Code, and Credential Number) is unique for each card.

Head End System (or Access Control Server)	A system including application software, database, a Head End server, and one or more networked personal computers. The Head End server is typically used to enroll an individual's name, create a unique ID number, and assign access privileges and an expiration date. The server is also used to maintain this information and refresh the controller(s) with the latest changes.
Identifier (or Unique Identifier)	In this publication, a data object, assigned by an authority, that unambiguously identifies a person within a defined community. For example, a driver license number identifies a licensed driver within a state. The authority registers people and guarantees assignment of each identifier to a unique person.
Identity Credential	A credential that contains one or more identifiers for its subject, a person. In this publication, an identity credential is designed to verify the identity of its subject through authentication mechanisms, via an electronically mechanism (see PKI-CAK, PKI-AUTH, BIO, BIO-A, etc.) or a manual mechanism (see VIS).
Infrastructure	Distributed substructure of a large-scale organization that facilitates related functions or operations, e.g., telecommunications infrastructure. With regard to PACS, components include conduit, cabling, power supplies, battery backup, electrified door hardware, door position switches, and remote exit devices, as well as connectivity with other life safety systems that will ensure egress in the event of an emergency.
Interoperability	In this publication, the quality of allowing any government facility or information system to verify a cardholder’s identity using the credentials on the PIV Card, regardless of the PIV Card Issuer (PCI).
Issuance (or Credential	The process by which an issuing authority obtains and verifies information about a person, assigns one or more unique identifiers

Issuance)	to the person, prepares information to be placed in or on a credential, produces a physical or data object credential, and delivers the finished credential to its subject. In the case of PIV Cards, issuance is performed only by accredited PCIs.
Issuer	The organization that is issuing the PIV Card to an applicant.
Multi-Factor Authentication	Authentication based on more than one factor. In some contexts, each factor is a different authenticator. In other contexts, each factor is one of “something you know, something you have, something you are” (i.e., memorized fact, token, or biometric) and thus the number of factors is 1, 2, or 3.
OCC-AUTH	A two-factor authentication mechanism that uses secure messaging and on-card comparison of cardholder fingerprint(s).
Online Certificate Status Protocol (OCSP)	An online protocol used to determine the status of a public key certificate. See <a href="#">[RFC2560]</a>
PACS Registration	The process of authenticating, validating, and verifying information about the PIV cardholder prior to entering the information into a PACS server. The information added during registration is then utilized to perform authentication and authorization of an individual at an access point.
Path Validation (or Trust Path Validation)	The process of verifying the binding between the subject identifier and subject public key in a certificate, based on the public key of a trust anchor, through the validation of a chain of certificates that begins with a certificate issued by the trust anchor and ends with the target certificate. Successful path validation provides strong evidence that the information in the target certificate is trustworthy.
Personal Identification Number (PIN)	A short numeric password (6 to 8 digits) used as an authenticator by the PIV Card to authenticate the cardholder.
Personal Identity Verification (PIV) Card	A physical artifact (e.g., identity card, “smart” card) issued to an individual that contains a PIV Card Application which stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
PIV Implementation Maturity Model (PIMM)	A model that can be used to measure the progress of a facility or an agency towards accepting PIV Cards.

PIV System	A system comprised of components and processes that support a common (smart card-based) platform for identity authentication across Federal departments and agencies for access to multiple types of physical access environments.
Physical Access Control System (PACS)	An electronic system that controls the ability of people to enter a protected area, by means of authentication and authorization at access control points.
PKI	A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification.
PKI-AUTH	A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the PIV Authentication certificate and key.
PKI-CAK	A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the Card Authentication certificate and key.
Private Key	A cryptographic key used with a public key cryptographic algorithm, which is uniquely associated with an entity, and not made public; it is used to generate a digital signature; this key is mathematically linked with a corresponding public key.
Public Key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public; it is used to verify a digital signature; this key is mathematically linked with a corresponding private key.
Reader	A device that interfaces with a PIV Card and a controller to execute or support execution of one or more PIV authentication mechanisms.
Relying Party	In this publication, an entity, such as a PACS, that depends upon the trust model of the PIV System to correctly produce the results of authentication, i.e., the identity of the cardholder.
Revocation	The process by which an issuing authority renders an issued credential useless. For example, a certification authority may revoke certificates it issues. Typically, a certificate is revoked if its corresponding private key is known to be, or suspected to be, compromised.
Secret Key	A key used by a symmetric key algorithm to encrypt, decrypt, sign, or verify information. In a symmetric key infrastructure (SKI), the sender and receiver of encrypted information must

share the same secret key.

Secure Messaging	A protocol by which a PIV Card Application is authenticated to the relying system. Secure Messaging is used to provide confidentiality and integrity protection for the card commands that are sent to the card as for the responses from the PIV Card.
Skimming	Surreptitiously obtaining data from a contactless smart card, using a hidden reader that powers, commands, and reads from the card within the maximum read distance (reported as about 25 cm with <a href="#">[ISO/IEC 14443]</a> smart cards like the PIV Card). <a href="#">[SKIMMER]</a>
Sniffing	Surreptitiously obtaining data from a contactless smart card, using a hidden reader that receives RF signals from a legitimate reader and smart card when they perform a transaction. Sniffing is a form of electronic eavesdropping. Sniffing is possible at greater distances than skimming.
Social Engineering	A process or technique, similar to a confidence game, used to obtain information from a person without raising suspicion.
SYM-CAK	The SYM-CAK is an authentication mechanism based on the optional symmetric card authentication key. As the name implies, the purpose of the SYM-CAK authentication mechanism is to authenticate the card and thereby the cardholder.
Symmetric Key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.
Trust Anchor	A named entity producing digital signatures, and a corresponding certificate that a relying party has decided to trust, i.e., if a digital signature is verified using the public key within the certificate, the signature is trusted to have been made by the entity named in the certificate.
Validation	In this publication, the process of determining that an identity credential was legitimately issued and is still valid, i.e., has not expired or been revoked.
Verification	The process of determining if an assertion is true, particularly the process of determining if a data object possesses a digital signature produced by the purported signer.
VIS	A <a href="#">[FIPS201]</a> authentication mechanism in which the visual identity verification of a PIV Card is done by a human guard.
Virtual Contact	An interface established over the contactless interface after the



**Interface** presentation of the pairing code to the PIV Card using secure messaging. All non-card-management operations that are allowed over contact interface may be carried out over the VCI.

**Wiegand** With regard to deployed PACS, a one-way communication protocol consisting of a formatted bit string used from the access reader to the controller. It can be used with any media, including proximity, bar code, magnetic stripe, and smart cards.

2263

## 2264 **Appendix G—Abbreviations and Acronyms**

2265	<b>ACL</b>	Access Control List
2266	<b>BIO</b>	Authentication Using Off-Card Biometric Comparison
2267	<b>BIO-A</b>	Attended Authentication Using Off-Card Biometric Comparison
2268	<b>BIO(-A)</b>	A short-hand to represent both BIO and BIO-A authentication mechanism
2269	<b>CHUID</b>	Cardholder Unique Identifier
2270	<b>CRL</b>	Certificate Revocation List
2271	<b>DUNS</b>	Data Universal Numbering System
2272	<b>ECC</b>	Elliptic Curve Cryptography
2273	<b>ECDSA</b>	Elliptic Curve Digital Signature Algorithm
2274	<b>FASC-N</b>	Federal Agency Smart Credential Number
2275	<b>FIPS</b>	Federal Information Processing Standards
2276	<b>FISMA</b>	Federal Information Security Modernization Act
2277	<b>FSL</b>	Facility Security Level
2278	<b>GSA</b>	General Services Administration
2279	<b>GUID</b>	Global Unique Identification Number
2280	<b>HSPD</b>	Homeland Security Presidential Directive
2281	<b>ID</b>	Identification
2282	<b>IEC</b>	International Electrotechnical Commission
2283	<b>ISC</b>	Interagency Security Committee
2284	<b>ISO</b>	International Organization for Standardization
2285	<b>IT</b>	Information Technology
2286	<b>ITL</b>	Information Technology Laboratory
2287	<b>LB</b>	Lower Bound
2288	<b>NIST</b>	National Institute of Standards and Technology
2289	<b>OCC</b>	On-Card Biometric Comparison
2290	<b>OCC-AUTH</b>	Authentication Using On-Card Biometric Comparison
2291	<b>OCSP</b>	Online Certificate Status Protocol
2292	<b>OMB</b>	Office of Management and Budget
2293	<b>PACS</b>	Physical Access Control System
2294	<b>PCI</b>	PIV Card Issuer
2295	<b>PIMM</b>	PIV Implementation Maturity Model
2296	<b>PIN</b>	Personal Identification Number
2297	<b>PIV</b>	Personal Identity Verification
2298	<b>PKI-AUTH</b>	Authentication with the PIV Authentication Certificate Credential
2299	<b>PKI-CAK</b>	Authentication with the Card Authentication Certificate Credential
2300	<b>POST</b>	Power-up self-test
2301	<b>RF</b>	Radio Frequency
2302	<b>RSA</b>	Rivest, Shamir, Aldeman
2303	<b>SP</b>	Special Publication

- 2304 **SYM-CAK** Authentication with the Symmetric Card Authentication Key
- 2305 **UB** Upper Bound
- 2306 **UUID** Universally Unique Identifier
- 2307 **VCI** Virtual Contact Interface
- 2308 **VIS** Authentication using PIV Visual Credentials
- 2309