

Retired Draft

Warning Notice

The attached draft document has been RETIRED. NIST has discontinued additional development of this document, which is provided here in its entirety for historical purposes.

Retired Date September 23, 2021

Original Release Date March 7, 2014

Retired Document

Status Initial Public Draft (IPD)

Series/Number NIST Interagency or Internal Report 7981

Title Mobile, PIV, and Authentication

Publication Date March 2014

Additional Information <https://csrc.nist.gov/publications/detail/nistir/7981/archive/2014-03-07>
<https://csrc.nist.gov/projects/piv>

Draft NISTIR 7981

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

Mobile, PIV, and Authentication

Hildegard Ferraiolo
Andrew Regenscheid
William Burr
David Cooper
Salvatore Francomacaro

Mobile, PIV, and Authentication

Hildegard Ferraiolo
Andrew Regenscheid
David Cooper
Salvatore Francomacaro
*Computer Security Division
Information Technology Laboratory, NIST*

William Burr
Dakota Consulting, Inc.

March 2014



U.S. Department of Commerce
Penny Pritzker, Secretary

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

25
26
27
28
29
30
31 |
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68

69
70

71
72

National Institute of Standards and Technology Interagency Report 7981
14 pages (March 2014)

73

74

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

75

76

77

78

79

80

81

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

82

83

84

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at <http://csrc.nist.gov/publications>.

85

86

87

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

88

89

90

91

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: piv_comments@nist.gov

92

Reports on Computer Systems Technology

93 The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology
94 (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's
95 measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of
96 concept implementations, and technical analyses to advance the development and productive use of
97 information technology. ITL's responsibilities include the development of management, administrative,
98 technical, and physical standards and guidelines for the cost-effective security and privacy of other than
99 national security-related information in Federal information systems.

100

101

102

103

104

Abstract

105

106 The purpose of this document is to analyze various current and near-term options for remote electronic
107 authentication from mobile devices that leverage both the investment in the PIV infrastructure and the
108 unique security capabilities of mobile devices, such as smart phones and tablets.

109

110

111

112

113

Keywords

114

115 electronic authentication; Derived PIV Credential; PIV Card; microSD; USB; UICC; mobile device;
116 smart phone; tablet

Table of Contents

117			
118			
119	1.	INTRODUCTION	5
120	2.	BACKGROUND	5
121	2.1	MOBILE DEVICES AND TECHNOLOGIES.....	5
122	2.2	PERSONAL IDENTITY VERIFICATION (PIV) INFRASTRUCTURE	6
123	3.	ELECTRONIC AUTHENTICATION APPROACH.....	6
124	3.1	Using PIV Cards.....	7
125	3.2	Using Derived PIV Credentials	8
126	3.2.1	Current Technology Supported Approaches	8
127	3.2.2	Possible Near-Term Approaches.....	9
128	4.	ANALYSIS AND RECOMMENDATIONS.....	10
129		APPENDIX A— ACRONYMS.....	13
130		APPENDIX B— REFERENCES	13
131			

132 **1. Introduction**

133 In the past decade, mobile devices have already significantly changed business capabilities,
134 allowing employees access to information resources wherever and whenever they need it. These
135 devices are both an opportunity and a challenge. Their unique capabilities – including their
136 always-on, always-connected nature – can facilitate more efficient and effective government, but
137 also create new challenges to ensure the confidentiality, integrity and availability of information
138 accessed by these devices.

139 This document focuses on the challenge of electronic authentication from mobile devices, defined
140 as the process of establishing confidence in user identities electronically presented to an
141 information system from a mobile device. The Federal government’s current approach to
142 electronic authentication in traditional computing devices requires the use of Personal Identity
143 Verification (PIV) Cards, which are “credit card size” smart cards using credentials based in
144 public key cryptography. Users must insert these cards into readers built into, or attached to, the
145 computers they use to access government information. While this approach to electronic
146 authentication works reasonably well with desktop and laptop computers, the same approach for
147 mobile devices, lacking the space for integrated smart card readers, would require bulky add-on
148 readers.

149 The purpose of this document is to analyze various current and near-term options for electronic
150 authentication that leverage both the investment in the PIV infrastructure and the unique security
151 capabilities of mobile devices, such as smart phones and tablets. While any of the options
152 discussed in this paper could support government security and interoperability requirements, we
153 believe current trends in the mobile device ecosystem argue for a flexible electronic
154 authentication policy that allows for close integration between the credential and the mobile
155 device.

156 **2. Background**

157 **2.1 Mobile Devices and Technologies**

158 In recent years, a new class of commercial computer products, “mobile devices,” has dramatically
159 disrupted the IT industry while providing many opportunities for better information services and
160 business processes. Mobile devices, such as smart phones and tablets, are powerful, Internet-
161 connected computers, small and light enough to be carried nearly anywhere.

162 Mobile devices, in the form of mobile phones and Personal Digital Assistants (PDAs), have been
163 available in some form for over twenty years, but advances in technologies and services over the
164 past six years have greatly increased their capabilities and use in the public and private sector.
165 The development of powerful, energy-efficient processors and small, reliable touch screens, along
166 with the now-ubiquitous availability of WiFi and 3G/4G mobile broadband networks, have
167 spurred constant innovation in this space.

168 Along with the significant capabilities of mobile devices, market pressure is driving the
169 manufacturing of smaller, lighter devices with adequate battery life, at low cost. These
170 constraints drive mobile device manufacturers to limit external ports and distinct computer chips,
171 and focus on integrating features into the System on Chip (SoC) that is the core component of
172 every mobile device.

173 The unique set of security features and constraints of mobile devices, combined with the different
174 way in which we use and secure mobile devices relative to traditional desktop and laptop
175 computers necessitates the identification and standardization of alternative electronic

176 authentication mechanisms that leverage the same identity management infrastructure that has
177 already been deployed.

178 **2.2 Personal Identity Verification (PIV) Infrastructure**

179 The deployment of PIV Cards and their supporting infrastructure was initiated by Homeland
180 Security Presidential Directive-12 (HSPD-12), which mandated a common identification standard
181 to enhance security, promote interoperability and increase Government efficiency. HSDP-12 was
182 intended to address wide variations in the quality and security of authentication mechanisms used
183 across federal agencies. It directed the federal government to establish and adopt an interoperable
184 standard providing graduated levels of security to provide agencies with the flexibility to deploy
185 appropriate mechanisms based on their environment and the sensitivity of their data. To meet the
186 goals outlined in HSPD-12, the PIV Card was designed to be interoperable across the federal
187 government – both for physical access to government facilities and logical access to Federal
188 information systems. The PIV Card contains several identity credentials supported by a public
189 key infrastructure (PKI) to provide strong identity assurance in an interoperable manner. To
190 provide a high level of trust in the credentials across the Federal enterprise, the PIV standard
191 established common processes for identity proofing and credential issuance.

192 Today, federal agencies have issued PIV Cards to the vast majority of federal employees and
193 contractors and the emphasis has shifted from PIV Card issuance to its use for logical and
194 physical access. Applications such as MyPay, Employee Express, and the OMB Max Portal are
195 just a few examples where the PIV Card is used for government network access.

196 **3. Electronic Authentication Approach**

197 With a worldwide market for mobile device sales of approximately 1 billion devices annually, the
198 public sector has limited market pressure to impact security capabilities and features. Instead,
199 features and capabilities are largely determined by consumers purchasing mobile devices for
200 personal use. Despite this challenge, government security needs are generally similar to business
201 needs and consumer applications, including mobile payments and digital rights management.
202 This presents an excellent opportunity for the federal government to continue to work with
203 industry to identify the security practices, standards and guidelines that can support both public
204 and private sector needs.

205 The mobile ecosystem is highly competitive, with different mobile device manufacturers,
206 platforms, and wireless carriers rapidly implementing and deploying new capabilities, often with
207 different focuses. Allowing for varied implementations and the level of innovation we have come
208 to expect from the mobile ecosystem argues for a flexible approach to electronic authentication
209 from mobile devices to ensure departments and agencies can take advantage of these capabilities.

210 This section will describe and analyze a number of proposed approaches that leverage the existing
211 PIV infrastructure to authenticate users. Some options are supported by currently available
212 technologies, and others require the development or commercialization of technologies that are
213 not currently available. However, even options supported by current technologies may not be
214 immediately deployable, as additional standardization, testing, or software development may be
215 needed to make these options compatible with government systems as intended by HSPD-12.

216 These proposals provide a range of options, some perhaps only transitional, facilitating different
217 operational scenarios for mobile devices, from high security government-owned mobile devices,
218 to dual-use bring-your-own-device (BYOD) scenarios.

219 3.1 Using PIV Cards

220 One general approach to electronic authentication from mobile devices is to find ways to use the
221 PIV Card itself with the mobile device. Unlike some laptops, mobile devices are generally too
222 small to integrate smart card readers into the device itself, requiring alternative approaches for
223 communicating between the PIV Card and the mobile device.

224 Currently, using PIV Cards with mobile devices would require the use of third-party smart card
225 readers separate from, but attached to, the mobile device itself. Any time the user attempts to
226 access an IT resource, he or she would need to insert the PIV Card into the separate reader and
227 enter his or her PIN. While this approach is rather cumbersome for users, it has the advantage
228 that agencies would not need to issue and manage another set of PKI credentials for users.

229 3.1.1 Current Technology Supported Approaches

230 *USB/Bluetooth Card Readers*

231 **Description:** PIV Cards could be used with existing and new mobile devices with the use
232 of add-on smart card readers. These readers would interface with the mobile device over
233 a wired (e.g., USB, Apple's Lightning) or wireless (Bluetooth) interface. Applications
234 (e.g., browsers, e-mail clients) would need to interface with the smart card reader.

235 **Availability:** High – Third-party card readers using Bluetooth, USB, or other proprietary
236 connectors are available for most mobile device platforms. Application support for using
237 PIV Cards through these readers is more limited, which could complicate use.

238 **Benefits:** This approach allows the use of existing credentials on PIV Cards, removing
239 the need to provision and manage new credentials to users and devices.

240 **Considerations:** This is a cumbersome approach, requiring users to carry their PIV
241 Cards and card readers with them whenever they need to use their devices. This would
242 decrease the portability of these devices and hinder the usability, requiring users to insert
243 their PIV Cards into the devices to authenticate to an information system. Also, while
244 use of wireless Bluetooth readers would slightly mitigate some of the usability concerns,
245 it would do so at the detriment of battery life. In addition, while these readers are
246 commercially available, they are fairly niche devices, and as such, are relatively
247 expensive.

248 3.1.2 Possible Near-Term Approaches

249 *Near Field Communication (NFC)*

250 **Description:** Near Field Communication (NFC) uses radio frequency to establish
251 communication between NFC-enabled devices. An NFC-enabled mobile device could
252 interact with a PIV Card and its keys over its contactless antenna at very close range,
253 allowing the mobile device to use the PIV keys without a physical connection. The user
254 would need to hold or place the card next to the mobile the device as she or she enters the
255 PIN protecting the keys on the PIV Card.

256 **Availability:** Limited – Many mobile devices on the market do not include NFC. Of those
257 that do, platforms do not necessarily provide the capabilities needed to interact with a PIV
258 Card.

259 **Benefits:** Assuming NFC is built into a device, this approach allows the use of the PIV
260 Card without a relatively bulky internal or external card reader.

261 **Considerations:** Current PIV Cards greatly restrict the keys that are accessible via the
262 contactless interface, as these cards do not support the establishment of a secure channel
263 between the card and an NFC reader. Revisions to the PIV standards under development at

264 NIST will include a secure channel specification, enabling the use of these keys over the
265 contactless interface when both the card and reader support the secure channel.

266 3.2 Using Derived PIV Credentials

267 As specified in SP 800-63, derived credentials are designed to leverage identity proofing and
268 vetting processes of a user's primary credential. Identity proofing and vetting processes do not
269 have to be repeated to issue a derived credential. Instead, the user proves possession of a valid
270 primary credential as the basis to receive a derived credential. The new derived credentials do
271 not need to be the same type or in the same token as the primary credential.

272 For the purpose of PIV, possession of a valid PIV Card is the basis to issue Derived PIV
273 Credentials for mobile devices. To achieve interoperability with the PIV infrastructure and its
274 applications, the Derived PIV Credentials are PKI-credentials. The form factor, however, is
275 different than the PIV Card's smart-card form factor by design. While PIV Cards are functionally
276 compatible with mobile devices, they are mechanically incompatible for one reason: the credit
277 card sized PIV Card's packaging is much too big. To address these limitations, Derived PIV
278 Credentials can be issued in form factors that are easier to use with mobile devices. In particular,
279 the approaches proposed below embed or integrate them in mobile devices. They could be
280 remotely provisioned (at a lower assurance level) to users who successfully authenticate with
281 their PIV Cards (possibly using the card on some other device). These approaches can greatly
282 improve the usability of the electronic authentication mechanisms.

283 The technical details of Derived PIV Credentials are specified in Draft SP 800-157 [SP800-157].
284 The goal of the Derived PIV Credential is to allow for PIV-enabled e-authentication services
285 from mobile devices to remote systems. Draft SP 800-157 offers several technical solutions in
286 order to accommodate a variety of mobile devices in the market today.

287 3.2.1 Current Technology Supported Approaches

288 *Software Tokens*

289 **Description:** Rather than using specialized hardware to store and use PIV keys, this
290 approach stores the keys in flash memory on the mobile device protected by a PIN or
291 password. Authentication operations are done in software provided by the application
292 accessing the IT system, or the mobile OS.

293 **Availability:** High – all major mobile platforms provide interfaces for storing and using
294 software-based certificates. However, additional security and interoperability testing may
295 need to be done to ensure suitability for government use, as intended by HSPD-12

296 **Benefits:** This approach could be used on any mobile device and does not require
297 specialized hardware.

298 **Considerations:** Protecting and using the Derived PIV Credential's corresponding
299 private key using software-based mechanisms potentially increases the risk that the key
300 could be stolen. This approach may provide a lower level of assurance of identity than
301 other methods describe in this document.

302

303 *MicroSD Tokens*

304 **Description:** Specialized microSD cards (or similar expansion cards) exist that contain a
305 hardware cryptographic module capable of storing and using a private key. To the mobile
306 device, the microSD with such a cryptographic module would function similarly to a
307 smart card.

308 **Availability:** Moderate – Not all mobile devices include microSD slots. While microSD
309 smart card tokens are commercially available, additional security and interoperability

310 testing may need to be done to ensure suitability for government use, as intended by
311 HSPD-12. Furthermore, mobile OS and application software support is very limited at
312 this time.

313 **Benefits:** These cards could be deployed on devices after purchase to add security
314 features. They would provide better protection of the private keys corresponding to
315 Derived PIV Credentials than a software only approach. The token can be ported to other
316 devices supporting microSD tokens.

317 **Considerations:** microSD cards can be cumbersome to remove from mobile devices. In
318 normal operation, they would remain in the device at all times, but the removable nature
319 of microSD cards put them at increased risk of theft.

320 **3.2.2 Possible Near-Term Approaches**

321 *USB Security Token*

322 **Description:** This approach uses a cryptographic hardware token, similar to the chip
323 found on smart cards, in a small device that could be plugged into a mobile device's
324 power/data connector. This would typically be a micro-USB connector, although many
325 devices use proprietary connectors. To the mobile device, the USB security token would
326 look like a smart card reader with an inserted PIV Card.

327 **Availability:** While commercial availability of full-sized USB security tokens is
328 relatively high, there are few products available for use in mobile devices. Furthermore,
329 mobile OS and application software support is very limited at this time.

330 **Benefits:** USB security tokens could be removed when not in use, and could add
331 authentication services to mobile devices after purchase (assuming compatibility by the
332 device and underlying OS). The token can be ported to other devices supporting USB
333 tokens.

334 **Considerations:** USB tokens tend to be relatively small and therefore may be easily lost
335 when removed from the handset. Usability could be a major issue. In many cases the
336 micro-USB port is also the charging port for the devices, so USB security tokens would
337 need to be removed to charge the device; preventing the use of the Derived PIV
338 Credential token while charging.

340 *UICC Tokens*

341 **Description:** Universal Integrated Circuit Cards (UICC), the new generation of SIM
342 cards, are removable cryptographic hardware tokens used by most wireless carriers to
343 authenticate mobile devices to their networks. The UICC can also support a variety of
344 additional applications and authentication services.

345 **Availability:** Deployment requires the cooperation of the wireless carrier, mostly likely
346 at additional expense.

347 **Benefits:** This approach leverages a cryptographic token that will likely be found in
348 nearly all mobile devices attached to a wireless carrier. The token may be ported to other
349 mobile devices controlled by the same carrier.

350 **Considerations:** While technically removable, in practice users would not be able to
351 remove the token without disabling the phone. Some mobile devices (e.g., tablets) may
352 not have or use UICCs.

354 *Embedded Hardware Tokens*

355 **Description:** Increasingly, mobile devices are being built with embedded hardware security
356 modules built into the device itself, either as a separate chip or built into the SoC at the heart
357 of the device. These modules typically have the ability to securely store cryptographic keys,

358 including private keys, and have some cryptographic capabilities. These modules could
359 provide for an embedded hardware token, providing authentication capabilities without
360 adding additional hardware to the device.

361 **Availability:** While some mobile devices have a form of an embedded hardware security
362 module, currently they are either unavailable for use or do not provide the specific set of
363 features needed to support PKI credentials.

364 **Benefits:** An integrated solution would likely provide better user experience at a lower
365 deployment cost. This approach could also provide unique security features not supported
366 by other approaches (see Section 4).

367 **Considerations:** Specific approaches will depend on whatever hardware/firmware/software
368 support is provided by individual device manufacturers and mobile operating systems.
369 Software for managing and using credentials would likely not be portable between devices.

370 4. Analysis and Recommendations

371 Any of the options discussed above could support agency electronic authentication needs,
372 depending on the sensitivity of data being protected and the deployed mobile devices and
373 infrastructure. While some of the options are not supported by commercially available
374 technology and services, current trends in the mobile ecosystem suggest these options will be
375 available by at least some mobile devices and service providers in the next one-to-three years. As
376 any of these options can be made interoperable with the existing PIV architecture, agencies
377 should deploy and use the mechanisms that best meet their needs, balancing security, cost and
378 ease-of-use. The best solutions for a particular agency may change over time, as the capabilities
379 of mobile devices evolve.

380 Nonetheless, as we select, implement and deploy these solutions, we should certainly embrace the
381 unique capabilities of mobile devices, while also recognizing their inherent constraints, in order
382 to identify the approaches that will serve us best in the long-term. We need to be cognizant of the
383 user experiences of these approaches, as users tend to work around even the most technically
384 sound security mechanisms if they impede their ability to get their jobs done.

385 It is not practical to restrict the approach to electronic authentication in mobile devices to
386 previous policies for desktop and laptop personal computers (PCs). While many users, with
387 different access privileges, often share PCs, mobile devices are rarely shared, and people
388 increasingly carry smart phones wherever they go. In a world of just PCs and flash card physical
389 access control, it was logical to consolidate all credentials into a single PIV Card. In a world with
390 individual mobile devices, often more than one per person, it's more logical for each device to
391 have its own credentials. While this may sound like a major deviation from the PIV Card, this
392 would still be re-using the same PKI infrastructure and building upon the trust and identity-
393 proofing that was already performed to issue PIV Cards to millions of Federal employees and
394 contractors. This is more of an evolutionary approach than a revolutionary one.

395 As mobile device vendors compete and innovate in this industry, we have seen them integrate an
396 increasing number of features, including security features, into the mobile operating system,
397 firmware, and underlying hardware. This trend will almost certainly continue, and is one of the
398 great opportunities for success in this space. Use of Derived PIV Credentials in mobile devices,
399 integrating the protection and use of these credentials into the lower layers of the mobile device
400 software/hardware stack, will provide capabilities, features, and security benefits that we don't
401 have today.

402 Currently, compatibility and commercial availability for any of the hardware-based approaches
403 identified in this paper is quite limited. The only approach discussed offering broad compatibility
404 and relative ease-of-use is the use of software tokens, essentially emulating the functions of the

405 PIV Card in software running on mobile devices. This approach provides the same identity
406 assurance as PIV Cards in every respect except one: software does not protect credentials' private
407 keys as well as hardware-based tokens like the PIV Card. While this provides a lower assurance
408 of identity than the PIV credentials in hardware-based tokens like the PIV Card, it likely provides
409 sufficient security for many applications and environments, given the sensitivity of most data
410 accessed from mobile devices. While data being accessed from mobile devices is increasing, the
411 most common IT resources accessed from mobile devices are e-mail, calendar and contact lists.

412 In the longer-term, federal agencies should look to adopt hardware-supported security
413 mechanisms in mobile devices, such as the Roots of Trust identified in NIST SP 800-164,
414 *Guidelines on Hardware-Rooted Security in Mobile Devices*. Use of security tokens embedded in
415 the hardware of the mobile device can support stronger assurance of identity.

416 In reality, there is a spectrum of choices between solutions based entirely in software and those
417 based entirely in hardware. While dedicated hardware solutions, like those envisioned in Section
418 3.2.2, are not commercially available at this time, many mobile devices on the market do provide
419 hardware-backed features that can protect keys of credentials that are stored on mobile devices.
420 Typically these features can protect keys using hardware-based mechanisms, but a software
421 cryptographic module uses the key during an authentication operation. This hybrid approach
422 provides many security benefits over software-only approaches, and should be used whenever
423 supported by mobile devices and applications.

424 The tighter integration of the security token holding the credential's private key and the device
425 itself presents many usability and, perhaps paradoxically, security benefits. The major usability
426 benefit is quite clear: the user does not need to use special card readers or tokens separate from
427 the device in order to access information. The security benefits are less clear on the surface, but
428 equally compelling. Once users unlock the private keys on the card, the keys are at the mercy of
429 the machine into which the card was inserted. The card has no context for whether it should be
430 performing the actions requested by the machine. If malware is present on that machine, malware
431 could use the private key. Closer integration with the device could provide the token greater
432 insight into context. It could, for instance, be tied to the state of the device, only being available
433 for use if the operating system and firmware have not been tampered with. The mobile device
434 could also confirm authentication and digital signing operations with users, showing a message
435 on the screen with certain transaction details (a property sometimes called "What You See Is
436 What You Sign"), which can help detect misuse of a credential. These properties are not
437 achieved with PIV Cards as they are implemented and deployed today.

438 The M-07-16 [M0716] security requirements for protecting personally-identifiable information
439 (PII) should be reconsidered in light of mobile device technology developments, such as
440 hardware-supported security features, the always-on, always-connected nature of the devices, and
441 the continued pace of innovation. The "Control Remote Access" provision of M-07-16 requiring
442 two-factor authentication, where one factor is separate from the device, is not consistent with
443 several Derived PIV Credential approaches described in this paper that make use of security
444 features and capabilities built into mobile devices. Electronic authentication policies will need to
445 be updated in order to give agencies the flexibility they need to take advantage of these
446 technologies.

447 **5. A Look at the Future**

448 Current technology trends point to a convergence of laptops and tablets, with those systems
449 inheriting many of the capacities and constraints of mobile devices. In the future, the desktop
450 computer may become less important as we conduct more of our daily business on mobile

451 devices that continue to become more and more capable. The decisions we make today on
452 electronic authentication on mobile devices will likely become the de-facto required
453 authentication mechanisms of the future.

454 In many ways mobile devices are in their adolescence. While they are highly capable devices
455 that are challenging the normal ways of doing business, we are still learning how to control and
456 manage these devices, sometimes failing to fully understand their true potential. Yet it is clear
457 they provide a glimpse at what the future will bring.

458 At the time of HSPD-12 and PIV, a natural assumption was that the one thing that government
459 employees would always have with them while working was their identity token. Moving
460 forward, it is easy to imagine a future where the one thing carried everywhere is a smart phone. It
461 is already true for many Federal employees, either in their personal or professional lives. Thus, it
462 is natural to question what role mobile devices, or smart phones in particular, may have as an
463 authentication token itself.

464 For the foreseeable future, we should expect a need for an identity token to support physical
465 access control, and there are many benefits to implementing such as card as we have done with
466 PIV. Furthermore, there is large set of infrastructure and computers currently deployed to support
467 and use PIV. There's little reason to replace such a capable authentication token. Nonetheless,
468 we see devices and environments that are not well suited to the use of PIV Cards. For instance,
469 consider small, lightweight laptop computers that lack integrated smart card readers. In these
470 cases, we can imagine using our smart phones with our laptops, employing the PIV credentials in
471 the phones to authenticate ourselves from our laptops. Alternatively, we can imagine using our
472 next-generation mobile phones with NFC for physical access where we would use our PIV Cards
473 today.

474 While such approaches may have long-term cost or usability benefits, it would place a great deal
475 of trust in the mobile device itself. These ideas should be considered and pursued cautiously, and
476 only after we have assured ourselves in the security of the mobile devices that would support
477 these use cases.

478 **6. Conclusion**

479 This document analyzed several current and near-term approaches for authentication from mobile
480 devices, such as smart phones and tablets. These approaches leverage the current investment in
481 the PIV infrastructure for electronic authentication. They also build upon the solid foundation of
482 well-vetted and trusted identity of the PIV cardholder – achieving substantial cost savings by
483 leveraging the identity-proofing results that were already performed to issue PIV Cards.
484 However, in order to accommodate mobile devices, and benefit from their unique security
485 features and capabilities, this document considered a number of approaches that use alternative
486 form factors for the authentication tokens. Any of the options discussed in this paper could
487 support government security and interoperability requirements, however current trends in the
488 mobile device ecosystem argue for a flexible approach to authentication from mobile devices that
489 leverages security features built into these devices.

490 When computers were too bulky to carry around most of the time, and were often shared with
491 others, it was logical to consolidate authentication credentials into a separate token. However, the
492 always-on, always-connected nature of mobile devices, combined their use by typically a single
493 person, argues for each device to have its own credentials. Closer integration between the
494 authentication credentials and mobile devices can provide a better, more convenient experience
495 for users while also supporting security features not found in approaches that use a separate PIV
496 Card and reader. In particular, closer integration with the device could support mechanisms

497 designed to detect or prevent the misuse of PIV credentials. Moving forward, as mobile devices
 498 increasingly work their way into the daily lives of Federal employees, we can continue to
 499 consider other ways to leverage mobile devices to support identity management.

500 **Appendix A—Acronyms**

501	BYOD	Bring Your Own Device
502	HSPD	Homeland Security Presidential Directive
503	IT	Information Technology
504	NFC	Near Field Communication
505	NIST	National Institute of Standards and Technology
506	NISTIR	National Institute of Standards and Technology Interagency Report
507	PC	Personal Computer
508	PDA	Personal Digital Assistant
509	PIN	Personal Identification Number
510	PIV	Personal Identity Verification
511	SIM	Subscriber Identity Module
512	SP	Special Publication
513	SoC	System on Chip
514	USB	Universal Serial Bus UICC
515	UICC	Universal Integrated Circuit Card

516 **Appendix B—References**

517	[FIPS201]	Federal Information Processing Standard 201-2, <i>Personal Identity Verification (PIV) Federal Employees and Contractors</i> , August 2013.
518		
519	[M0716]	OMB Memorandum M-07-16, <i>Safeguarding Against and Responding to the Breach of Personally Identifiable Information</i> , OMB, May 2007.
520		
521	[SP800-63]	NIST Special Publication 800-63-2, <i>Electronic Authentication Guideline</i> , August 2013.
522		
523	[SP800-157]	Draft NIST Special Publication 800-157, <i>Guidelines for Derived Personal Identity Verification (PIV) Credentials</i> , March 2014
524		
525	[SP800-164]	NIST Special Publication 800-164, <i>Guidelines on Hardware-Rooted Security in Mobile Devices</i> , October 2012.
526		