NIST SPECIAL PUBLICATION 1800-12B

Derived Personal Identity Verification (PIV) Credentials

Volume B:
Approach, Architecture, and Security Characteristics

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

Michael Bartock
Jeffrey Cichonski
Hildegard Ferraiolo
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

Christopher Brown
Spike E. Dog
Susan Prince
Julian Sexton
The MITRE Corporation
McLean, VA

August 2018

SECOND DRAFT

DISCLAIMER

Certain commercial entities, equipment, products, 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 or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: piv-nccoe@nist.gov

Public comment period: August 1, 2018 through October 1, 2018

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Federal Information Processing Standards (FIPS) Publication 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," establishes a standard for a PIV system based on secure and reliable forms of identity credentials issued by the federal government to its employees and contractors. These credentials are intended to authenticate individuals to federally controlled facilities, information systems, and applications, as part of access management. In 2005, when FIPS 201 was published, authentication of individuals was geared toward traditional computing devices (i.e., desktop and laptop computers) where the PIV Card provides common multifactor authentication mechanisms through integrated or external smart card readers, where available. With the emergence of computing devices,

such as tablets, hybrid computers, and, in particular, mobile devices, the use of PIV Cards has proved to be challenging. Mobile devices lack the integrated smart card readers found in laptop and desktop computers, and require separate card readers attached to devices to provide authentication services. To extend the value of PIV systems into mobile devices that do not have PIV Card readers, NIST developed technical guidelines on the implementation and life cycle of identity credentials that are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV Card. These NIST guidelines, published in 2014, describe Derived PIV Credentials (DPC) that leverage identity proofing and vetting results of current and valid PIV credentials.

To demonstrate the DPC guidelines, the NCCoE at NIST built two security architectures using commercial technology to enable the issuance of a Derived PIV Credential to mobile devices using ICAM shared services One option uses a software-only solution while the other leverages hardware built into many computing devices used today.

This project resulted in a freely available NIST Cybersecurity Practice Guide that demonstrates how an organization can continue to provide multi-factor authentication for users with a mobile device that leverages the strengths of the PIV standard. Although this project is primarily aimed at the federal sector's needs, it is also relevant to mobile device users with smart-card-based credentials in the private sector.

KEYWORDS

cybersecurity; Derived PIV Credential (DPC); enterprise mobility management (EMM); identity; mobile device; mobile threat; multifactor authentication; personal identity verification (PIV); PIV Card; smart card

ACKNOWLEDGMENTS

Name	Organization
Bryan Rosensteel	Entrust Datacard
Dror Shilo	Intel Corporation
Simy Cohen	Intel Corporation
Abhilasha Bhargav-Spantzel	Intel Corporation
Carlton Ashley	Intel Corporation
Alfonso Villasenor	Intel Corporation
Won Jun	Intercede
Alan Parker	Intercede
Allen Storey	Intercede
Iain Wotherspoon	Intercede
Andre Varacka	Verizon
Russ Weiser	Verizon
Emmanuel Bello-Ogunu	The MITRE Corporation
Lorrayne Auld	The MITRE Corporation
Sarah Kinling	The MITRE Corporation
Poornima Koka	The MITRE Corporation

Name	Organization
Matthew Steele	The MITRE Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Entrust Datacard	Entrust IdentityGuard, Entrust Managed Services Public Key Infrastructure (PKI)
Intel Corporation	Intel Authenticate Solution
Intercede	MyID Credential Management System
MobileIron	MobileIron Enterprise Mobility Management (EMM) Platform
Verizon	Verizon Shared Service Provider (SSP) PKI

Contents

List of Figures

List of Tables

96
97
98
99
100
101
102
103
104
105
106

1 Summary

Homeland Security Presidential Directive-12 (HSPD-12) [1] began efforts to deploy Personal Identity Verification (PIV) Cards and their supporting infrastructure in 2004. The goal was to eliminate wide variations in the quality and security of authentication mechanisms used across federal agencies. The mandate called for a common identification standard to promote interoperable authentication mechanisms at graduated levels of security based on the environment and the sensitivity of data. In response, Federal Information Processing Standards (FIPS) 201 specified a common set of credentials in a smart card form factor [2] called a PIV Card. PIV Cards are now used government-wide as a primary credential for federal employees and contractors. PIV Cards enhance security by using a standard issuance process by which agencies perform identity proofing and background checks. PIV Cards provide multifactor authentication as part of both physical and logical access management to government facilities and federal information systems.

When FIPS 201 was published, logical access was geared toward desktop and laptop computers, which enabled multifactor authentication via a PIV Card through integrated or connected card readers. The increased use of mobile phones and tablets as part of logical access makes leveraging the PIV system challenging. Mobile phones and tablets lack integrated smart card readers and require the user to attach a separate card reader whenever they need to authenticate with their PIV Card. To address this challenge, Derived PIV Credentials (DPC) were introduced to extend the value of PIV Cards into today's mobile environment. A DPC is based on a user's proof of possession of a valid PIV Card, which leverages identity proofing and background checks that have already been completed, to issue a new set of credentials stored on a mobile device. A mobile device that contains the user's DPC can authenticate to websites and portals that use verification of PIV Card credentials for access.

The National Cybersecurity Center of Excellence (NCCoE) Cybersecurity Practice Guide *Derived Personal Identity Verification (PIV) Credentials Project* demonstrates how Derived PIV Credentials can be issued to mobile devices by using commercial off-the-shelf products that leverage the PIV standard for remote authentication to information technology (IT) systems in operational environments while meeting policy guidelines. Although the PIV program and the NCCoE Derived PIV Credentials Project are primarily aimed at the federal sector's needs, both are relevant to private-sector organizations that want to extend the value of identity proofing and vetting of a primary identity credential into mobile devices. To that end, the example implementations in this practice guide work from a simple scenario that informs the basis of an architecture tailored to the public and private sectors.

Starting with the National Institute of Standards and Technology (NIST) Cybersecurity Framework [3], the Risk Management Framework (RMF) [4], and security controls from NIST Special Publication (SP) 800-53 [5], this document also references NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* [6]; NIST SP 800-63-3, *Digital Identity Guidelines* [7]; FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors* [2]; Internet Engineering Task Force

143   (IETF) Request for Comments (RFC) 4210; NIST SP 800-181, *National Initiative for Cybersecurity*
144   *Education (NICE) Cybersecurity Workforce Framework* [8]; and NIST's *Mobile Threat Catalogue* [9].

145   We designed the example implementations and architectures to incorporate standards-based,
146   commercially available products. The solutions can be used by any organization deploying DPC that is
147   willing to perform its own risk assessment and ready to implement controls based on the organization's
148   risk posture.

149   **Section 1**: **Summary** presents the challenge addressed in this volume (Volume B: *Approach,*
150   *Architecture, and Security Characteristics*). The example implementations address the challenge and
151   benefits of DPC solutions. The summary also explains how to provide feedback on this guide.

152   **Section 2**: **How to Use This Guide** explains how readers like you—business decision makers, program
153   managers, IT professionals (e.g., systems administrators), and other stakeholders who will be
154   responsible for procuring, designing, implementing, and managing deployments of DPC for mobile
155   devices—might use each volume of the guide.

156   **Section 3**: **Approach** offers a detailed treatment of the scope of the project, describes the assumptions
157   on which the security platform development was based, explains the risk assessment that informed
158   platform development, and provides an overview of the technologies and components that industry
159   collaborators gave us to enable platform development.

160   **Section 4**: **Architecture** describes the functional architecture of our example solution, including
161   Cybersecurity Framework functions supported by each component that our collaborators contributed.

162   **Section 5**: **Security Characteristics Analysis** provides details about the tools and techniques we used to
163   perform risk assessments pertaining to DPC. It also summarizes the test sequences we employed to
164   demonstrate security platform services, the Cybersecurity Framework functions to which each test
165   sequence is relevant, and NIST SP 800-157 [6] controls that applied to the functions being
166   demonstrated.

167   **Section 6**: **Future Build Considerations** is a brief treatment of other applications that NIST and the
168   NCCoE might explore in the future to further support DPC.

169   The appendixes provide a list of acronyms, references, key definitions, and a requirements table derived
170   from NIST Internal Report (IR) 8055 [10].

1.1 Challenge

172   Mobile phones, tablets, and laptop PCs that lack smart card readers are being increasingly deployed by
173   federal agencies. Most of these devices lack a smart card reader that allows the devices to leverage the
174   security and control characteristics of the FIPS 201-2 PIV system standard.

---

175 Implementing DPC in mobile phones and tablets is challenging due to the wide array of mobile device
176 models and platforms, which offer different ways to store the credentials and different key stores,
177 including application containers (i.e., software containers) in credential management systems (CMS) and
178 removable storage options (i.e., Universal Serial Bus (USB) and micro Secure Digital (microSD) cards).
179 This is further complicated by the rapid update cycles of proprietary mobile operating systems for which
180 developers must keep pace with the changes.

181 Additionally, the guidelines in SP 800-157 to manage the DPC Authentication certificate throughout its
182 life cycle (issuance and maintenance) and its interactions with the PIV Card life cycle present challenges
183 to the implementer such as integration efforts between DPC and PIV Card issuing systems. Further, the
184 DPC Authentication certificate is issued at an assurance level for use in PIV-enabled relying applications.
185 Typically, federal agencies choose to use managed services to help ensure that the level of assurance is
186 maintained, and thus DPC implementers also face integration challenges with managed public key
187 infrastructure (PKI) services.

188 Enterprise Mobility Management (EMM) solutions, which implement the mobile security policy
189 requirements of an organization, must also be considered when implementing DPC. Many federal
190 agencies use EMM solutions to secure sensitive enterprise data and provide customizable workflows to
191 manage the life cycle of the mobile device. The alignment of the mobile device life cycle and DPC life
192 cycle steps can prove challenging to agencies that wish to eliminate friction for the end user.

193 1.2 Solution

194 This NIST Cybersecurity Practice Guide demonstrates how commercially available technologies can meet
195 your organization's need to issue multifactor credentials to mobile devices for authentication with IT
196 systems in operational environments.

197 We built an environment that resembles an enterprise network by using commonplace components
198 such as identity repositories, supporting certificate authorities, and web servers. Next, products and
199 capabilities were identified that, when linked together, provide two example implementations
200 demonstrating life cycle guidelines outlined in NIST SP 800-157 [6]. These example implementations
201 leverage cloud services where possible through a Software as a Service (SaaS) component. The federal
202 government encourages the use of SaaS or shared service providers (SSPs) [11] that operate under
203 federal policy, such as certificate authorities operating in accordance with policy developed by the
204 Federal PKI Policy Authority. The security controls for these SSPs are periodically assessed, allowing the
205 organization to focus on its primary mission and avoid the costs associated with ongoing maintenance of
206 these systems.

207 One of our example implementations includes the integration of an EMM and a DPC solution. EMMs are
208 useful in applying SP 800-157 life cycle guidelines by integrating an organization's mobile device
209 issuance process with DPC issuance. EMMs can also assist with terminating the DPC by remotely
210 destroying the EMM's software container.

211 Finally, this practice guide documents two methods of securely storing the DPC on a device,
212 demonstrating the flexibility of SP 800-157 guidance. One option uses a software-only solution while the
213 other leverages hardware built into many computing devices used today.

214 The NCCoE developed a collaborative team uniquely qualified to create two example implementations
215 of DPC. We partnered with the subject matter experts who wrote NIST SP 800-157 to better understand
216 its requirements and to ensure that the integrations of commercial products were within the
217 document's guidelines.

218 Commercial, standards-based products, such as the ones that we used, are readily available and
219 interoperable with existing IT infrastructure and investments.

220 This guide lists all of the necessary components and provides installation, configuration, and integration
221 information so that a federal agency or other private organization can replicate what we have built. The
222 NCCoE does not particularly endorse the suite of commercial products used in our reference designs.
223 These products were used after an open call in the Federal Register to participate. Each organization's
224 security experts should identify the standards-based products that will best integrate with its existing
225 tools and IT system infrastructure. Organizations can adopt one of these solutions or a different one that
226 adheres to these guidelines in whole, or an organization can use this guide as a starting point for
227 tailoring and implementing parts of a solution.

1.3 Benefits

229 For an organization that is planning and looking for solutions to issue DPC to its workforce, the example
230 implementations described in this guide will help the organization navigate through the various options
231 by:

232 ▪ providing visibility into how the different device vendors and CMS vendors are implementing
233 solutions for storing the credentials

234 ▪ demonstrating the use of managed services for the DPC issuance and life cycle management

235 ▪ demonstrating integration with an EMM solution

2 How to Use This Guide

237 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides
238 users with the information they need to replicate the DPC example implementations. This reference
239 design is modular and can be deployed in whole or in part.

240　This guide contains three volumes:

241　　▪　NIST SP 1800-12A: *Executive Summary*

242　　▪　NIST SP 1800-12B: *Approach, Architecture, and Security Characteristics* – what we built and why
243　　　**(you are here)**

244　　▪　NIST SP 1800-12C: *How-To Guides* – instructions for building the example solution

245　Depending on your role in your organization, you might use this guide in different ways:

246　**Business decision makers, including chief security and technology officers,** will be interested in the
247　*Executive Summary, NIST SP 1800-12A*, which describes the following topics:

248　　▪　challenges enterprises face in issuing strong, multifactor credentials to mobile devices

249　　▪　the example solutions built at the NCCoE

250　　▪　benefits of adopting the example solutions

251　**Technology or security program managers** who are concerned with how to identify, understand, assess,
252　and mitigate risk will be interested in this part of the guide, *NIST SP 1800-12B*, which describes what we
253　did and why. The following sections will be of particular interest:

254　　▪　Section 3.5.3, Risk, provides a description of the risk analysis we performed

255　　▪　Section 3.5.4, Security Control Map, maps the security characteristics of the example solutions
256　　　　to cybersecurity standards and best practices

257　You might share the *Executive Summary, NIST SP 1800-12A*, with your leadership team members to help
258　them understand the importance of adopting a standards-based DPC solution.

259　**IT professionals** who want to implement an approach like this will find the whole practice guide useful.
260　You can use the How-To portion of the guide, *NIST SP 1800-12C*, to replicate all or parts of the builds
261　created in our lab. The How-To portion of the guide provides specific product installation, configuration,
262　and integration instructions for implementing the example solutions. We do not re-create the product
263　manufacturers' documentation, which is generally widely available. Rather, we show how we
264　incorporated the products together in our environment to create an example solution.

265　This guide assumes that IT professionals have experience implementing security products within the
266　enterprise. While we have used a suite of commercial products to address this challenge, this guide does
267　not endorse these particular products. Your organization can adopt either solution or one that adheres
268　to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
269　parts of the DPC example solutions. Your organization's security experts should identify the products
270　that will best integrate with your existing tools and IT system infrastructure. We hope you will seek
271　products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists
272　the products we used and maps them to the cybersecurity controls provided by the reference solutions.

273 A NIST Cybersecurity Practice Guide does not describe "the" solution but a possible solution. This is a
274 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and
275 success stories will improve subsequent versions of this guide. Please contribute your thoughts to
276 piv-nccoe@nist.gov.

2.1 Typographic Conventions
277

278 The following table presents typographic conventions used in this volume.

Typeface/ Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; placeholders	For detailed definitions of terms, see the *NCCoE Glossary.*
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit**.
Monospace	command-line input, onscreen computer output, sample code examples, status codes	mkdir
Monospace Bold	command-line user input contrasted with computer output	**service sshd start**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov

3 Approach
279

280 To develop our example solutions, the Derived PIV Credentials project team followed an approach
281 common to projects across the NCCoE. First, a project description was published on the website
282 followed by a Federal Register Notice (FRN) [12]. In response to the FRN, several vendors expressed
283 interest in helping the NCCoE build example solutions. Technology companies with relevant products
284 then signed a cooperative research and development agreement (CRADA) with the NCCoE for the
285 project. After the CRADAs were signed, the NCCoE sponsored a kickoff meeting for the project team,
286 collaborating vendors, and other members of the Derived PIV Credentials community of interest (COI).

287 During the kickoff, we gathered requirements and lessons learned from project stakeholders; this
288 helped establish objectives for our example implementations. In addition to input from collaborators
289 and COI members, we performed a risk assessment during the architecture design phase and on our
290 final DPC example implementations. This assessment includes both risk factors to the functions of the
291 system (e.g., DPC issuance or revocation) and to its parts, such as the mobile devices into which a DPC
292 would be provisioned.

293 The Derived PIV Credential project is using a phased approach that takes direct advantage of previous
294 work by NIST in this area. NIST IR 8055 [10], *Derived Personal Identity Verification (PIV) Credentials (DPC)*
295 *Proof of Concept Research*, presents a scheme for provisioning a DPC to an organization-managed
296 mobile device. This project applied these technologies as a starting point, then sought to expand on the
297 DPC ecosystem to provide greater diversity across mobile device models and platforms, credential
298 storage implementations at level of assurance (LOA) 3, Derived PIV Credential Management Systems
299 (DCMS), and EMM products.

3.1 Audience

301 This guide is intended for IT and security managers and for system administrators responsible for
302 deploying secure solutions to support the evolving mobile ecosystem of an organization. With mobile
303 devices rapidly becoming the computing resources of choice within many organizations, there is growing
304 pressure on IT personnel to ensure that the organization has best practices in place for securely
305 accessing the organization's assets when using these devices. As mentioned previously, DPC solutions
306 are still evolving, and no one solution will fit all organizations.

307 This guide aims to help IT personnel understand the options, capabilities, and limitations of the solutions
308 available in the market today and to deploy the solutions that fit organizational needs.

3.2 Scope

310 The scope of NIST SP 800-157, *Guidelines for Derived PIV Credentials* [6], is to provide PIV-enabled
311 authentication services on the mobile device to authenticate the credential holder to remote systems.
312 The current phase of the Derived PIV Credentials Project and this practice guide focus only on a portion
313 of NIST SP 800-157—the life cycle activities. Specifically, we evaluated the example solutions against the
314 requirements related to initial issuance, maintenance, and termination of DPC.

315 For the proof-of-concept research documented in NIST IR 8055 [10], NIST used a single-vendor CMS
316 product to demonstrate DPC life cycle management. The device platforms documented in NIST IR 8055
317 were Windows, Android, and iOS. The CMS vendor's software key store implementation for Android and
318 iOS devices was used for the research effort, and Microsoft's Virtual Smart Card implementation was
319 used for the Windows platform. For the first phase of the NCCoE project, we documented an additional
320 CMS product to demonstrate DPC life cycle management.

321   As of this writing, only DPC Authentication certificates that can be issued at LOA 3 are addressed. To
322   support LOA 4, we would need to address additional in-person life cycle requirements that were
323   deemed out of scope for this project. Section 6 offers some future build considerations.

324   This project integrates an EMM component into one of our documented example implementations.
325   EMMs are essential to securing mobile endpoints; however, this project defers to the Mobile Device
326   Security for Enterprise Project at the NCCoE for specific security control recommendations. Section 3.5,
327   Risk Assessment, includes threats specific to DPC issued to authenticators contained within mobile
328   devices. For privacy considerations as they pertain to risk, readers of this publication are encouraged to
329   review the SP 800-63-3 discussion on privacy.

330   PIV Card life-cycle management is not within the scope of the project. However, tests were conducted
331   on PIV Card credentials to start issuing DPC and to validate that a DCMS performs all required checks of
332   a DPC subscriber's PIV Card and associated PIV Authentication certificate per NIST SP 800-157.

3.3   Relationship to NIST SP 800-63-3

334   The NIST SP 800-63-3 series of documents published in June 2017 retired the LOA concept and in its
335   place introduced Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), and federation
336   assurance level components to assist in risk management decisions. At the time of this writing, FIPS 201-
337   2 [2] and NIST SP 800-157 refer to the earlier LOA terminology for electronic authentications. However,
338   we have mapped the authenticators used in this project to an AAL in Section 5.4. IAL is not applicable in
339   the context of DPC because deriving identity is accomplished by proving possession and successful
340   authentication of an authenticator (on the PIV Card) that is already bound to the original, proofed digital
341   identity [7].

3.4   Assumptions

343   To implement this practice guide, readers should have a thorough understanding of NIST SP 800-157
344   and other supporting standards and guidelines. In addition, readers should be aware that the example
345   implementations presented have the following assumptions:

346   ▪   If you are an implementer who works for a U.S. federal agency, you will be complying with FIPS
347   201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors* [2].

348   ▪   The mobile devices in your DPC solution are organization-provided [13], and your organization
349   centrally manages them with security policies and controls.

3.4.1   Modularity

351   Specific assumptions on modularity are based on one of the NCCoE core operating tenets: that
352   organizations already have the PIV Card issuance solution and the associated PKI services in place. We
353   make no further assumptions regarding how the solutions have been deployed; they may combine on-

354 premises operations, cloud deployments, and managed services. Instead, we intend this guide to offer
355 options for adding the DPC life-cycle management solution into a diverse set of existing deployments.

3.4.2 Security

356

357 A second assumption is that adopters of our example implementations have already invested in the
358 security of the organization's network and IT systems. We assume that the existing PIV CMS is
359 implemented in a manner consistent with the Cybersecurity Framework and the guidelines presented in
360 NIST SP 800-63-3. Further, we assume that the security features of each product integrated into our
361 example implementations will perform as described by the respective product vendor.

3.4.3 Existing Infrastructure

362

363 This guide may help in designing an entirely new infrastructure. However, it is geared toward
364 organizations with an established infrastructure, as that represents the largest portion of readers.
365 Federal agencies and other organizations that are mature enough to implement DPC are likely to have
366 some combination of the capabilities described in the example implementations, such as solutions to
367 manage mobile devices. Before applying any measures addressed in this practice guide, we recommend
368 reviewing and testing them for applicability to the existing environment. No two organizations are the
369 same, and the impact of applying security controls will differ.

3.4.4 Architecture Components

370

371 We have chosen to align the components, where possible, used in this project to the architectural
372 components described in the Federal Identity, Credential, and Access Management (FICAM) program,
373 which helps federal agencies enable access to systems and facilities. The FICAM architecture is the
374 federal government's approach for designing, planning for, and implementing identity, credential, and
375 access management (ICAM). Figure 3-1 presents a view of the different ICAM solutions, applications,
376 and software components that work together to run a functional, secure ICAM program.

377   **Figure 3-1 Federal ICAM Enterprise Architecture**

378
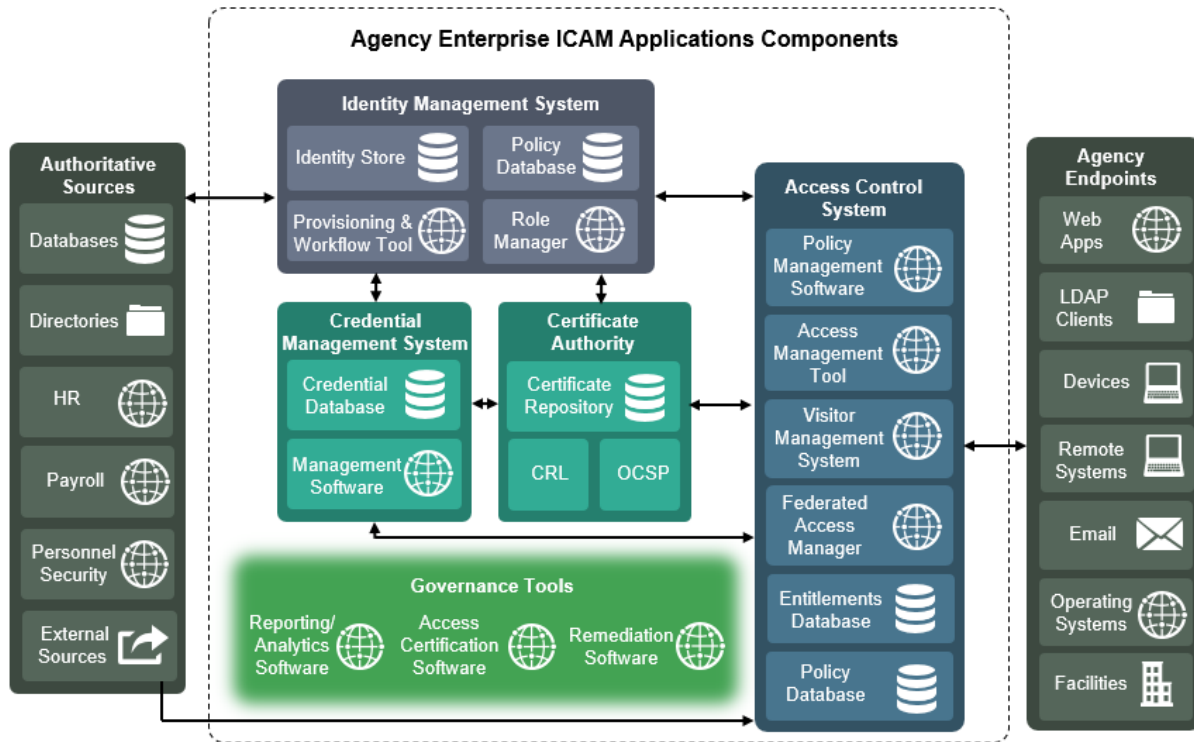
3.4.4.1   Credential Management System

380   A CMS contains management software and is central to executing the life-cycle operations, typically
381   sponsorship, registration, issuance, maintenance, and termination of authentication credentials. Usually,
382   information related to the life-cycle operations is stored within a database. In our architecture, we
383   depict two types of CMSs: PIV and Derived PIV. The PIV CMS is responsible for enforcing life-cycle
384   activities in accordance with FIPS 201-2, and the DCMS enforces the life-cycle activities in accordance
385   with NIST SP 800-157. Readers will need to be familiar with the PIV standard [2] and associated
386   guidelines before implementing a DPC solution.

3.4.4.2   Public Key Infrastructure

388   The PKI (also referred to as the certificate authority [CA]) issues, maintains, and revokes digital
389   certificates issued to PIV Cards and mobile devices. The PKI can be operated as part of an on-premises
390   infrastructure and is also offered as a managed service. PIV CMS service providers partner with PKI
391   service providers for issuing the digital certificates that are provisioned to the PIV Card and the mobile
392   device. Typically, certificate status services such as a certificate revocation list (CRL) repository and
393   Online Certificate Status Protocol (OCSP) services are also offered by PKIs.

3.4.4.3 Enterprise Mobility Management

An EMM is typically used by organizations to provide security services commonly needed for security management of mobile devices such as remotely device wiping, device encryption enforcement, and application restrictions. An EMM within the DPC context enforces the use of secure container solutions and eases the issuance process of the DPC. For example, a DPC enrollment can be combined with the enrollment of a device with an EMM (assuming PIV Card issuance and activation have been completed before mobile device enrollment). This reduces the complexity of the enrollment process for the DPC applicant. A tight integration between the DCMS and the EMM also potentially reduces maintenance life-cycle tasks of the DPC. For instance, if a mobile device is lost by the DPC subscriber, an EMM administrator initiates revocation of the DPC Authentication certificate and destroys the software container that stores the DPC.

3.4.4.4 Mobile Device

For the purposes of this publication, the term *mobile device* refers to a device that stores the DPC. Typically, this is a device such as a smartphone or a tablet running a rich operating system, as defined in NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations:*

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

Alternatively, DPC can be used in personal computer (PC) laptops or hybrid devices that run a desktop operating system. In this use case, the endpoint does not have a built-in smart card reader that can leverage PIV Card capabilities.

3.4.4.5 Authenticator

This publication uses the definition from NIST SP 800-63-3B:

> Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity.

The authenticator in the context of DPC is a cryptographic module, referred to in SP 800-157 as a cryptographic token.

3.5 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* [4]—material that is available to the public. The risk management framework (RMF) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

This section discusses risk from two perspectives. First, we review the risk mitigation that a DPC system is meant to address in terms of Cybersecurity Framework functions. Next, we address the residual risk of an implemented DPC system.

Allowing users access to services from a mobile device leads to a more efficient and effective workforce. There are risks, however, and the security objectives [13] of confidentiality, integrity, and availability need to be maintained on the mobile endpoint. The threats to weak single-factor authentication mechanisms, such as passwords, are well documented by industry [14] and government [9]. Further, the 2017 Department of Homeland Security (DHS) *Study on Mobile Device Security* [15] found the failure to use strong multifactor authentication mechanisms to protect critical cloud services to be a gap in the defense of current mobile devices. This finding is underscored by the move of organizations to cloud services that provide critical services such as email and calendaring. The DHS study recommends enhancing mobile Federal Information Security Modernization Act (FISMA) metrics for authentication methods.

A DPC solution is part of an overall mobile security architecture that protects enterprise data by using strong multifactor authentication to access remote resources. A DPC solution also supplements a basic centralized enterprise mobility security policy, as NIST SP 800-124 recommends. The publication further recommends that organizations design and acquire one or more solutions that collectively mitigate current workforce mobile device security risk. For an in-depth discussion on digital identity risk management, we encourage review of Section 3.5.1, which presents a list of possible identity risks and how they are covered by DPC, based on NIST SP 800-63-3 guidelines related to digital identity risk. An

461   organization can apply the guidelines while executing all relevant Cybersecurity Framework and RMF
462   life-cycle phases [7].

463   Federal cybersecurity risk management has taken on increased emphasis with the release of the
464   Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical
465   Infrastructure [16]. In this memo, the president directs each agency head to use NIST's *Framework for*
466   *Improving Critical Infrastructure Cybersecurity*, or any successor document, to manage the agency's
467   cybersecurity risk.

468   In response, NIST released NIST Internal Report (IR) 8170, *The Cybersecurity Framework:*
469   *Implementation Guidance for Federal Agencies* [17]. The NIST IR guides agencies on how the
470   Cybersecurity Framework can be used to augment current NIST security and privacy risk management
471   publications. We recommend that organizations, especially federal agencies that implement a DCMS,
472   follow the recommendations presented in NIST IR 8170. For instance, the framework's Example 1—
473   Integrate Enterprise and Cybersecurity Risk Management—recommends using five cybersecurity
474   functions (identify, protect, detect, respond, and recover) to organize cybersecurity risk management
475   activities at the highest level. Section 3.5.4 presents a list of possible functions that a DPC
476   implementation can address. We recommend that this information be used when communicating risk
477   throughout an organization.

3.5.1 Threats

479   NIST SP 800-63-3 provides a general identity framework by incorporating authenticators, credentials,
480   and assertions into a digital system [7]. Included in the publication are threat analyses in the areas of
481   authenticator and life-cycle threats. This section uses these threats as a basis for a discussion of threats
482   applicable to a DPC system.

483   **Table 3-1 Enrollment and Identity Proofing Threats**

Activity	Threat/ Attack	Example	Applicability to DPC
Enrollment	Falsified identity proofing evidence	An applicant attempts to use a forged PIV Card to obtain a DPC.	PKI-AUTH check by DCMS rejects forged PIV Card (e.g., determines that the certificates were not issued by a trusted CA or user cannot prove control of the private key corresponding to the certificate).

Activity	Threat/Attack	Example	Applicability to DPC
	Fraudulent use of another's identity	An applicant attempts to use a PIV Card associated with a different individual to obtain a DPC.	Multifactor authentication performed as part of the PKI-AUTH prevents the malicious actor from activating the PIV Card.
	Repudiation of enrollment	A subscriber denies enrollment, claiming that they did not enroll with the credential service provider (CSP).	Denial of DPC enrollment, while possible, would be difficult due to PKI-AUTH authentication and validation requirements during enrollment.
	Use of revoked credential	A subscriber attempts to use a PIV Card authentication certificate that is revoked to obtain a DPC.	The PKI-AUTH check determines the credential is revoked. To mitigate against the possibility of the PIV Card being very recently revoked and not being detected as such during enrollment, the seven-day revocation check will cause the DPC to be revoked.
Issuance	Disclosure	A key created by the CSP for a subscriber is copied by an attacker as it is transported from the CSP to the subscriber during authenticator issuance.	Not applicable if key is generated within the subscriber's mobile device. If the key is generated by the CSP and transported to the subscriber, then mutually authenticated secure transport as required by NIST SP 800-157 will protect the key.
	Tampering	A new password created by the subscriber to protect the private key is modified by an attacker to a value of the attacker's choosing.	A DPC subscriber's mobile device could contain malware that intercepts the PIN/password for a software container-based DPC. Use mobile security best practices to prevent and/or detect malware on the endpoint.
	Unauthorized issuance	A person falsely claiming to be the subscriber is issued	An attacker could steal a one-time password (OTP) through a man-in-the-middle attack or other means. Use an

Activity	Threat/ Attack	Example	Applicability to DPC
		credentials for that subscriber.	EMM to authenticate the device requesting the DPC. Further, ensure an appropriate channel is used to distribute the OTP, and ensure the OTP is resistant to attempts by an attacker to brute force attack (or use other means) to discover the value of the OTP.
	Social engineering	A malicious person manipulates an individual at the CSP responsible for issuance to obtain a credential bound to another valid subscriber.	An attacker could manipulate an administrator of the DCMS to make a PIV subscriber eligible for a DPC. Use an EMM to authenticate the device and verify it is operated by the person requesting the DPC.

484

485   **Table 3-2 Authenticator Threats to DPC**

Authenticator Threats/Attacks	Examples	Applicability to DPC
Theft	A hardware cryptographic device is stolen.	An external USB or microSD can be readily stolen. Multifactor authentication prevents unauthorized use of the private key.
	A cell phone is stolen.	A mobile device that stores the DPC in software or an embedded cryptographic token can be readily stolen. Use mobile locking mechanisms, remote wipe, and other mobile device security best practices to mitigate risk of a stolen device. Further, multifactor authentication prevents unauthorized use of the private key.

Authenticator Threats/Attacks	Examples	Applicability to DPC
Duplication	A software PKI authenticator (private key) is copied.	A DPC stored in a software-based container on a mobile device could be copied from the device. Use device sandboxing mechanisms, cryptographic techniques, and malware detection mechanisms as mitigation.
Eavesdropping	Memorized secrets are obtained by watching keyboard entry.	Through shoulder surfing, an attacker could observe a PIN/password that protects the cryptographic token. Educate users to be mindful of surroundings when entering PINs/passwords. Use authentication endpoints that employ trusted input and trusted display capabilities. Note: This attack compromises only one factor of the multifactor authentication mechanisms provided by DPC.
	Memorized secrets or authenticator outputs are intercepted by keystroke-logging software.	An attacker could use malware to intercept a PIN/password that protects the cryptographic token. Use mobile security best practices to prevent and/or detect malware on the endpoint. Also, native cryptographic token storage on some devices can leverage trusted paths for PIN/password entry.
Offline cracking	A software PKI authenticator is subjected to a dictionary attack to identify the correct password or PIN to use to decrypt the private key.	A DPC stored in a software-based container on a mobile device could be copied from the device and would be subject to offline cracking. Use PIN/password throttling, device encryption, and malware detection mechanisms as mitigation.
Side channel attack	A key is extracted by differential power analysis on a hardware cryptographic authenticator.	A mobile device is susceptible to side channel attacks only if the PIN/password has been successfully entered. Use key

Authenticator Threats/Attacks	Examples	Applicability to DPC
		and/or PIN usage timeout/limits and adopt other countermeasures described in NIST SP 800-63-3B and PHY-5 [9].
	A cryptographic authenticator secret is extracted by analysis of the response time of the authenticator over many attempts.	A mobile device is susceptible to side channel attacks only if the PIN/password has been successfully entered. Use key and/or PIN usage timeout/limits and adopt other countermeasures described in NIST SP 800-63-3B and PHY-5 [9].
Endpoint compromise	A cryptographic authenticator connected to the endpoint is used to authenticate remote attackers (i.e., malicious code on the endpoint is used as a proxy for remote access to a connected authenticator without the subscriber's consent).	A DPC that leverages an external token, such as a USB token, may be vulnerable to this threat. Multifactor authentication prevents unauthorized use of the DPC private key.
	Authentication is performed on behalf of an attacker rather than the subscriber.	An attacker could use malware to intercept a PIN/password that protects the cryptographic token. Use sandboxing and mobile security best practices to prevent and detect malware on the endpoint. Also, native cryptographic token storage on some devices can leverage trusted paths for PIN/password entry.
	Malicious code is used as a proxy for authentication or exports authenticator keys from the endpoint.	A DPC stored in a software-based container on a mobile device could be copied from the device and would be subject to offline cracking. Use sandboxing, device encryption, and malware detection mechanisms as mitigation.

486

3.5.1.1 Other Threats

Mobile devices like those featured in our example implementations are subject to the broader set of mobile ecosystem threats. From NIST IR 8144 [18]:

> Mobile devices pose a unique set of threats to enterprises. Typical enterprise protections, such as isolated enterprise sandboxes and the ability to remote wipe a device, may fail to fully mitigate the security challenges associated with these complex mobile information systems. With this in mind, a set of security controls and countermeasures that address mobile threats in a holistic manner must be identified, necessitating a broader view of the entire mobile security ecosystem. This view must go beyond devices to include, as an example, the cellular networks and cloud infrastructure used to support mobile applications and native mobile services.

We strongly encourage organizations implementing the reference architectures in whole or part to consult the NIST Mobile Threat Catalogue (MTC) [9] when assessing relevant threats to their own organization. Each entry in the MTC contains several pieces of information: an identifier, a category, a high-level description, details on its origin, exploit examples, examples of common vulnerabilities and exposures (CVEs), possible countermeasures, and academic references.

In broad strokes, the MTC covers 32 different threat categories that are grouped into 12 distinct classes as shown in Table 3-3. Of these categories, two in particular, highlighted in green in the table, are covered by the guidance presented in this practice guide and, if implemented correctly, will help mitigate those threats.

Table 3-3 Mobile Threat Classes and Categories

Threat Class	Threat Category
Application	Malicious or Privacy-Invasive Application
	Vulnerable Applications
Authentication	Authentication: User or Device to Network
	Authentication: User or Device to Remote Service
	Authentication: User to Device
Cellular	Carrier Infrastructure
	Carrier Interoperability
	Cellular Air Interface

Threat Class	Threat Category
LAN & PAN	Network Threats: Bluetooth
	Network Threats: NFC
	Network Threats: Wi-Fi
Payment	Application-Based
	In-App Purchases
	NFC-Based
Physical Access	Physical Access
Privacy	Behavior Tracking

	Consumer-Grade Femtocell		**Supply Chain**	Supply Chain
	SMS/MMS/RCS			Baseband Subsystem
	USSD			Boot Firmware
	VoLTE			Device Drivers
Ecosystem	Mobile Application Store		**Stack**	Isolated Execution Environments
	Mobile OS and Vendor Infrastructure			Mobile Operating System
EMM	Enterprise Mobility			SD Card
GPS	GPS			USIM/SIM/UICC Security

507

508 The other categories, while still important elements of the mobile ecosystem and critical to the health of
509 an overall mobility architecture, are out of scope for this document. The entire mobile ecosystem should
510 be considered when analyzing threats to the architecture; this ecosystem is depicted below in
511 Figure 3-2, taken from NIST IR 8144. Each player in the ecosystem—the mobile device user, the
512 enterprise, the network operator, the app developer, and the original equipment manufacturer—can
513 find suggestions to deter other threats by reviewing the MTC and NIST IR 8144. Many of these share
514 common solutions, such as using EMM software to monitor device health, and restricting installation of
515 apps from only authorized sources.

516   **Figure 3-2 The Mobile Ecosystem**

517
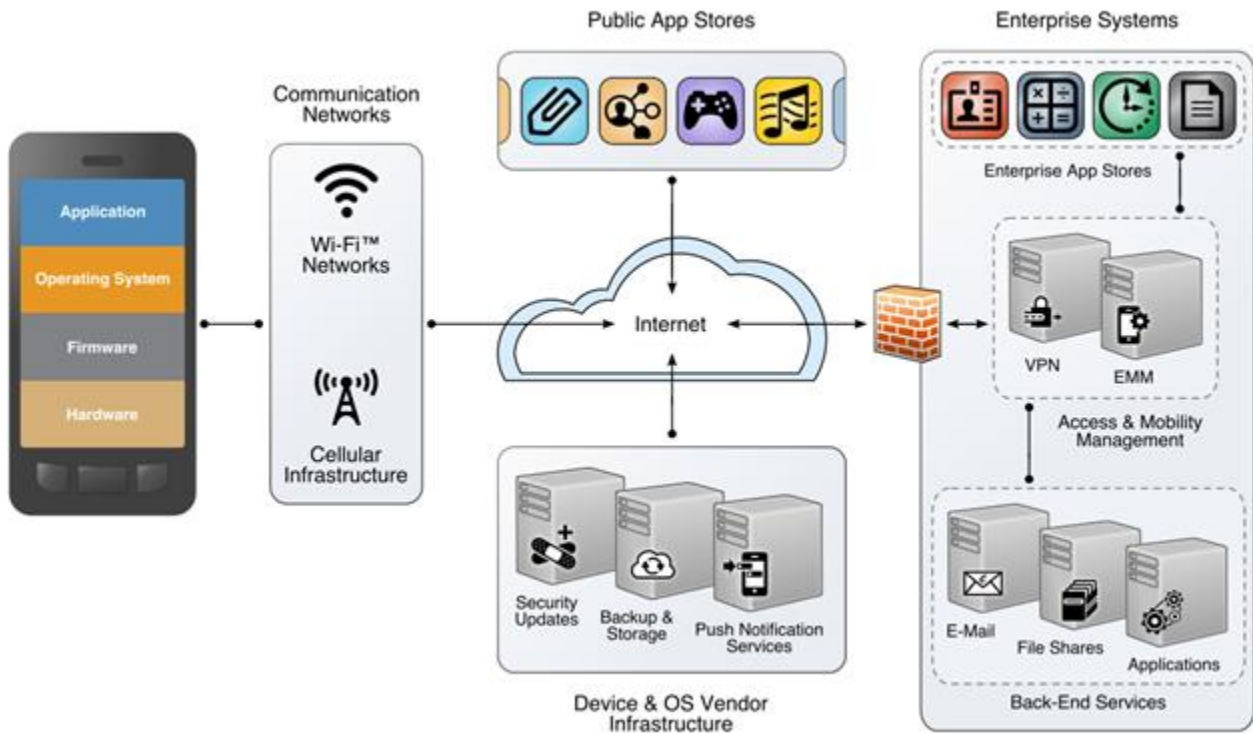
518   Because threats to organizationally controlled infrastructure are addressed by normal computer security
519   controls (e.g., separation of duties, record keeping, independent audits), they are outside the scope of
520   this practice guide. See NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information*
521   *Systems and Organizations* [5], for appropriate security controls.

522   3.5.2 Vulnerabilities

523   Vulnerabilities can exist within mobile applications, mobile and desktop operating systems, and network
524   applications that are employed in the storage and use of a mobile credential. Vulnerabilities can be
525   exploited at all levels in the information stack. For up-to-date information regarding vulnerabilities, this
526   guide recommends that security professionals leverage the National Vulnerability Database (NVD) [19].
527   The NVD is the U.S. government repository of standards-based vulnerability management data.

528   *3.5.2.1 Mobile Device Vulnerabilities*

529   Vulnerabilities discovered within mobile applications and rich operating systems are important to any
530   deployment of DPC. The DPC issuer must ensure strong protections on the use of the credential via a
531   PIN or pass phrase [6, Section 3] while also making sure that other applications on the device cannot

532 access the credential. Sensitive cryptographic material can be stored in software at AAL-2, leaving the
533 mobile device open to exploits that attack vulnerable code. To thwart these types of attacks, it is
534 common for mobile applications to be sandboxed in some manner to prevent unexpected and
535 unwanted interaction among the system, its applications, and data access between disparate
536 applications (including user data) [18]. However, a search of the NVD yields examples of software
537 vulnerabilities [20] that might allow exploits to *break* sandboxing protections. A full discussion on these
538 topics, including mitigations, can be found in NIST IR 8144, *Assessing Threats to Mobile Devices &*
539 *Infrastructure: the Mobile Threat Catalogue* [18] and NIST SP 800-163, *Vetting the Security of Mobile*
540 *Applications* [21]. Vulnerabilities are also introduced by downloading nonapproved applications. We
541 recommend that only vetted and approved applications be downloaded. NIST's AppVet is an example of
542 an application vetting platform.

3.5.2.2 Network Vulnerabilities

544 Considering that DPC enrollment may happen remotely [6], issuing organizations will want to mitigate
545 network vulnerabilities before deploying a DPC solution for the organization. For example, a DPC
546 applicant may be required to enter an OTP into the DPC mobile provisioning app to complete enrollment
547 as described in NIST SP 800-157 (Section C.1, Appendix C). The organization will want to maintain
548 confidentiality, integrity, and authenticity of the OTP as it traverses potentially untrustworthy networks.

549 This guide suggests two resources to assist network vulnerability analyses as input to a risk assessment.
550 The CVE database [22] lists more than 100,000 vulnerabilities that can affect web servers, Structured
551 Query Language (SQL) servers, Domain Name System (DNS) servers, firewalls, routers, and other
552 network components. These vulnerabilities include denial of service, code execution, overflow, cross-
553 site scripting, directory traversal, process bypass, unauthorized gaining of information, SQL injection, file
554 inclusion, memory corruption, cross-site request forgery, and Hypertext Transfer Protocol (HTTP)
555 response splitting.

556 Many of these vulnerabilities are operating system- or application-based. Others are protocol-based
557 (e.g., vulnerabilities inherent in IP6, Transport Layer Security [TLS], DNS, Border Gateway Protocol [BGP],
558 Simple Mail Transfer Protocol [SMTP], and other network protocols). The U.S. NVD is an additional
559 resource that builds upon the information included in CVE entries to provide enhanced information for
560 each CVE Identifier. As in the case of mobile device vulnerabilities, NIST frequently updates the NVD so it
561 remains a viable source of vulnerabilities that affect network servers.

3.5.3 Risk

563 As with the topic of threats, a discussion on DPC risk closely parallels that of risk management when
564 implementing a PIV program within an organization. As such, this document defers to NIST SP 800-63-3
565 [7, Section 5] on the topic of digital identity risk management.

566 An implementer of DPC should refer to the NIST SP 800-63-3 discussion of digital identity risk
567 management and the corresponding risk assessment guidelines that supplement the RMF. Specifically,
568 this section provides guidelines on the selection of the DPC vendor AAL based on risk.

3.5.4 Security Control Map

570 An organization may benefit from examples in NIST IR 8170 [17]. For instance, the framework's
571 Example 1—Integrate Enterprise and Cybersecurity Risk Management—recommends using five
572 cybersecurity functions (identify, protect, detect, respond, and recover) to organize cybersecurity risk
573 management activities at the highest level. Table 3-4 presents a list of possible functions that a DPC
574 implementation can address. In addition, for each Cybersecurity Framework subcategory, a mapping
575 was made to NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity*
576 *Workforce Framework* [8], to show what types of work roles are needed to implement and maintain a
577 DPC solution. We recommend that this information be used when communicating risk throughout an
578 organization.

579 **Table 3-4 Security Control Mappings**

Cybersecurity Framework Function	Cybersecurity Framework Category	Cybersecurity Framework Subcategory	NIST SP 800-53 Rev. 4	NIST SP 800-181 Work Roles
PROTECT (PR)	Access Control (PR.AC)	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	IA-2, IA-4, IA-5, AC-2	Software Developer SP-DEV-001), Product Support Manager (OV-PMA-003)
		PR.AC-3: Remote access is managed.	AC-17, AC-19	Information Systems Security Developer (SP-SYS-001), System Administrator (OM-ADM-001)
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	AC-2, AC-19, IA-2, IA-4, IA-5, IA-8	Security Control Assessor (SP-RSK-002), Product Support Manager (OV-PMA-003)

Cybersecurity Framework Function	Cybersecurity Framework Category	Cybersecurity Framework Subcategory	NIST SP 800-53 Rev. 4	NIST SP 800-181 Work Roles
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction	AC-7, AC-11, IA-2, IA-5	Systems Requirements Planner (SP-SRP-001), Information Systems Security Manager (OV-MGT-001)
	Data Security (PR.DS)	**PR.DS-2:** Data in transit is protected	SC-8, SC-12	Data Analyst (OM-DTA-002), Cyber Defense Analyst (PR-CDA-001)
		PR.DS-5: Protections against data leaks are implemented	SC-13	Research and Development Specialist (SP-TRD-001), Cyber Defense Analyst (PR-CDA-001)
	Information Protection (PR.IP)	**PR.IP-3:** Configuration change control processes are in place	CM-3	Software Developer (SP-DEV-001), Systems Security Analyst (OM-ANA-001)

580

The framework's Example 3—Integrate and Align Cybersecurity and Acquisition Processes—may help in acquiring and integrating a DCMS into an organization's environment. As the framework notes, an organization could ask a vendor to include its Cybersecurity Framework Profile in response to a request for information (RFI) for a DPC solution. Receiving this data allows an objective comparison of solutions.

3.6 Technologies

We built the example implementations by using products from vendors who signed CRADAs with the NCCoE for the DPC project. Products for the supporting infrastructure components are from vendors who are National Cybersecurity Excellence Partnership partners. The NCCoE does not endorse or recommend these products. Each organization should determine if these or other products on the market with similar capabilities best meet its own requirements and integrate well with its existing IT system infrastructure.

The following sections describe the vendors and products we used for our example implementations.

3.6.1 Entrust Datacard

Entrust Datacard, provider of trusted identity and secure transaction technologies, offers solutions for PKI and for PIV Card life-cycle management activities within its portfolio. Organizations can choose to operate these solutions in-house or use Entrust Datacard's managed service offerings. Entrust's IdentityGuard product is an identity-based authentication platform that includes a web-based self-service module (SSM). It supports a wide range of authenticators, including smart cards.

Following NIST SP 800-157, Entrust expanded IdentityGuard and SSM products to support DPC issuance and life-cycle management. The solution includes a mobile smart credential application and is available for use on Apple iOS, Google Android, and Blackberry operating systems.

The Entrust Datacard Managed PKI solution is a trusted service managed through legal and technology agreements, and regular auditing of the services, procedures, and practices [23]. Through a set of standard protocols, the PKI service issues and manages credentials for identities of individual persons. In this project, the Entrust Managed PKI issued X.509 credentials for PIV and Derived PIV identities.

3.6.2 Intel Authenticate

Intel Authenticate is a hardware-based multifactor authentication solution that allows for IT to define an authentication policy that is secured and enforced in the Intel® client hardware systems. Intel Authenticate provides hardware to protect multiple user factors (protected PIN, fingerprint, phone, location, etc.) and to secure IT-defined authentication policies. These policies are evaluated and enforced on the client hardware, leading to the release of cryptographic tokens (e.g., PKI-based signatures as used in DPC) to meet the authentication needs of the applications based on DPC.

The technology uses the DPC Authentication certificate where the private key is stored in a hybrid firmware/hardware solution. The PKI authentication key is released for the cryptographic operations only when the multifactor authentication condition, as defined by enterprise IT, has been met. The multiple factors that protect the DPC Authentication private key are protected by a PIN. The PIN is protected by a technology called Protected Transaction Display, which is based on a PIN pad that is directly rendered by the graphics engine and verified in hardware. In this way, it adds security features beyond native operating systems mechanisms.

Intel Authenticate technology is available on all Ultrabook devices and other PC devices with sixth, seventh, and eighth generation and higher Intel Core vPro processors running Microsoft Windows 7, 8, and 10.

3.6.3 Intercede

Intercede contributed an identity and credential management product for PIV Card credentials that additionally supports DPC and MyID as a software solution that can be hosted in the cloud or deployed in-house. The MyID server platform comprises an application server, a database, and a web server. It provides connectors to infrastructure components such as network shares and PKI, and application programming interfaces (APIs) to enable integration with the organization's identity and access management system. For mobile devices, the MyID Identity Agent runs as an app and interfaces with the MyID server to support iOS and Android mobile devices and credential stores, including the device native key store, software key store, and microSD.

3.6.4 MobileIron

Vendors that provide products and solutions to manage mobile devices may enter into partnerships with identity and credential management product vendors to deliver integrated solutions. MobileIron, one such vendor, has partnered with Entrust Datacard and is offering an integrated solution for the life-cycle management of DPC for mobile device users.

MobileIron offers an EMM platform that enables organizations to secure and manage mobile devices, applications, and content. Three tools of the EMM product suite—Core, Sentry, and Mobile@Work—are relevant to the integration with Entrust Datacard's IdentityGuard for supporting DPC. MobileIron Core, the software engine, enables organizations to set policies for managing mobile devices, applications, and content. It integrates with an organization's back-end IT platforms and can be deployed on-premises or in the cloud.

MobileIron Sentry functions as an inline gateway to manage and secure the traffic between mobile devices and back-end systems, such as Microsoft Exchange Server with ActiveSync. The third component, the Mobile@Work app, interfaces with MobileIron Core and configures the device, creates a secure container, and enforces the configuration and security policies set by the organization. As a suite, the MobileIron EMM platform protects enterprise data and applications.

3.6.5 Verizon Shared Service Provider

The Verizon SSP solution is a trusted PKI service for federal agencies managed through legal and technology agreements, and regular auditing of the services, procedures, and practices. Through a set of standard protocols, the PKI service issues and manages credentials for identities of individual persons. The following edited description is taken from the General Services Administration (GSA) IT Schedule 70 contract:

> The SSP solution is built as a scalable architecture that may be complemented (at the Agency's option) with Card Management Services, Lightweight Directory Access Protocol (LDAP)-based Directory services, and Simple Certificate Validation Protocol

657   (SCVP) Validation Services. The core Verizon SSP offering provides all the digital
658   certificate profiles required to be implemented on FIPS-201 approved smart cards.

659   Verizon SSP PKI services offer fully managed options to archive and recover end user
660   encryption keys, post certificates and CRLs to a publicly accessible directory, and
661   validate certificate status in real-time through OCSP. Verizon SSP service platforms are
662   built on open standards, they are well integrated and highly interoperable.

3.6.6 Mobile Endpoints

664 Table 3-5 lists the devices used to complete our example implementations. Operating system (OS)
665 versions are current as of the writing of this document. Readers should consult vendor documentation
666 for the latest compatibility requirements.

667 **Table 3-5 Mobile Endpoints**

Manufacturer	Model	OS/Version
Apple	iPhone	iOS 11.0.3
Apple	iPad Mini	iOS 11.0.3
Samsung	Galaxy S6	Android 6.0.1
Lenovo	ThinkPad	Windows 10

3.6.7 Technology Mapping

669 Table 3-6 lists all the technologies we incorporated into the example implementations and maps the
670 generic application term (component) to the specific product we used and to the Cybersecurity
671 Framework subcategories that the product addresses. Note: Some of our components are marked in the
672 version column as not applicable. This is due to the use of SaaS [24] cloud services.

Table 3-6 Products and Technologies

Component	Product	Version	Function	Cybersecurity Framework Subcategories
PKI Certificate Authority	Entrust Datacard Managed PKI	Not applicable	Entity that issues an authentication certificate, which is an X.509 public key certificate that has been issued in accordance with the requirements of NIST SP 800-157 and the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [25]	PR.AC-1
PKI Certificate Authority	Verizon Shared Service Provider	Not applicable	Entity that issues an authentication certificate, which is an X.509 public key certificate that has been issued in accordance with the requirements of NIST SP 800-157 and the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [25]	PR.AC-1
Derived PIV Credential Management System	Entrust Datacard IdentityGuard	Not applicable	Entity that implements Derived PIV life-cycle activities in accordance with NIST SP 800-157	PR.AC-1, PR.IP-3
Derived PIV Credential Management System	Intercede MyID	10.8	Entity that implements Derived PIV life-cycle activities in accordance with NIST SP 800-157	PR.AC-1, PR.IP-3
PIV Credential Management System	Entrust Datacard IdentityGuard	Not applicable	Entity that implements PIV life-cycle activities in accordance with FIPS 201-2	PR.AC-1, PR.IP-3
PIV Credential Management System	Intercede MyID	10.8	Entity that implements PIV life-cycle activities in accordance with FIPS 201-2	PR.AC-1, PR.IP-3
Enterprise Mobility Management System	MobileIron Core	9.3	Entity that provides security services commonly needed for security management of mobile devices [13]	PR.AC-1, PR.AC-3

Component	Product	Version	Function	Cybersecurity Framework Subcategories
Authenticator	Entrust PIV-D	1.3.0.4	Software component that stores the Derived PIV Authentication private key	PR.DS-2, PR.DS-5
Authenticator	Intercede Identity Agent	3.14	Software component that stores the Derived PIV Authentication private key	PR.DS-2, PR.DS-5
Authenticator	Intel Authenticate	Not applicable	Hybrid component that stores the Derived PIV Authentication private key	PR.DS-2, PR.DS-5

4   Architecture

In this section, we describe how the components defined in Section 3.4.4, as implemented by our partner technologies (see Section 3.6, Technologies), were integrated to produce the final example implementations (Section 4.2 and Section 4.3). Note that these architectures were based on time and resource constraints and are focused on supporting DPC life-cycle activities. In future phases of the project, architectures may be expanded to include a managed PIV Card component, broader application of DPC to mobile apps, and other enhancements. Refer to Section 6 for further details.

Though these capabilities are implemented as integrated solutions in this guide, organizational requirements may dictate that only a subset of these capabilities be implemented. These reference architectures were designed to be modular to support such use cases.

4.1   Architecture Description

Many federal agencies have opted to use a managed shared solution for issuing PIV Cards for their employees rather than deploy and operate their own PKI. GSA's Managed Service Office established the USAccess program to offer federal agencies a managed shared service solution for PIV Card issuance to help agencies meet the HSPD-12 mandate [1]. USAccess provides participating agencies with a comprehensive set of services, including issuance and life-cycle management of PIV Card credentials, administration, and reporting [1].

Assuming that many agencies use a managed service for their PIV Card issuance and a shared service provider for the PKI services, we considered a few of the different deployment architectures while planning our example implementations. Further, managing mobile devices with EMM products is an integral part of the mobile device security for most organizations. Therefore, we considered architectures for DPC provisioning solutions both independent of and integrated with an EMM solution.

696 As a result, this practice guide documents two reference architectures that are described in the
697 following sections. To assist readers in putting our architectures in the context of the Federal ICAM
698 Enterprise Architecture, as discussed in Section 3.4.4, below we have highlighted the components that
699 are used within each architecture. Note that Figure 4-1 is slightly modified from the original FICAM
700 architecture to allow for an EMM component to be included within the access control system. An EMM
701 can execute the access processes from policy stored within an access management database.

702 **Figure 4-1 Federal ICAM Enterprise Architecture**

703
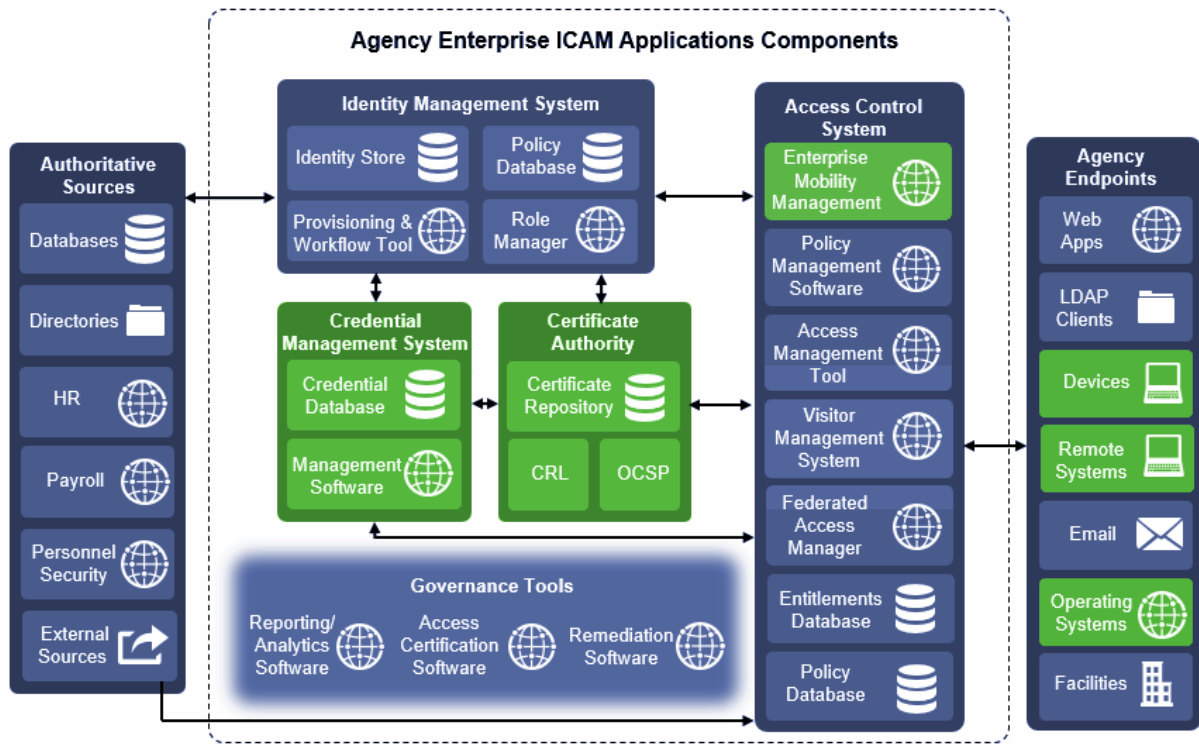
## 4.2 Managed Architecture with EMM Integration

705 Figure 4-2 depicts the finalized example implementation for this reference architecture, in which cloud
706 services are used to manage the PIV and DPC life-cycle activities. It also introduces an EMM into the
707 workflow, recognizing the need for organizations to apply a consistent set of security policies on the
708 device. In this scenario, the same vendor operates the PIV and DPC management services to simplify the
709 life-cycle linkage requirements between the DPC and PIV so that integration efforts across two solutions
710 are not necessary. This simplification also allows for recovery of the PIV user's key management key
711 onto the mobile device with relatively little difficulty, again because of the single vendor solution. This
712 type of scenario, however, may not be suitable if an organization prefers a more modular architecture.

713 The back-end EMM components, MobileIron Core and MobileIron Sentry, were deployed on-premises in
714 the demilitarized zone (DMZ) of a simulated enterprise network. MobileIron Core allows administration
715 of users and devices by applying policies and configurations to them based on their assigned labels.
716 MobileIron Sentry provides a virtual private network (VPN) endpoint, which creates an authenticated
717 and protected channel between managed devices and on-premises resources, such as internal email.
718 Sentry was included in this architecture to explore DPC usage scenarios as discussed in Section 6.
719 However, as Sentry is not required for any life-cycle management activities of DPC, it is not further
720 documented by this guide. The enterprise network also includes Active Directory (AD) and an Exchange
721 server. The instance of AD was used to store the identities of the test users in this scenario. The EMM
722 used AD as its trusted repository of authorized mobile device owners.

723 **Figure 4-2 PIV and DPC Cloud Service Life-Cycle Management with EMM Integration**

724
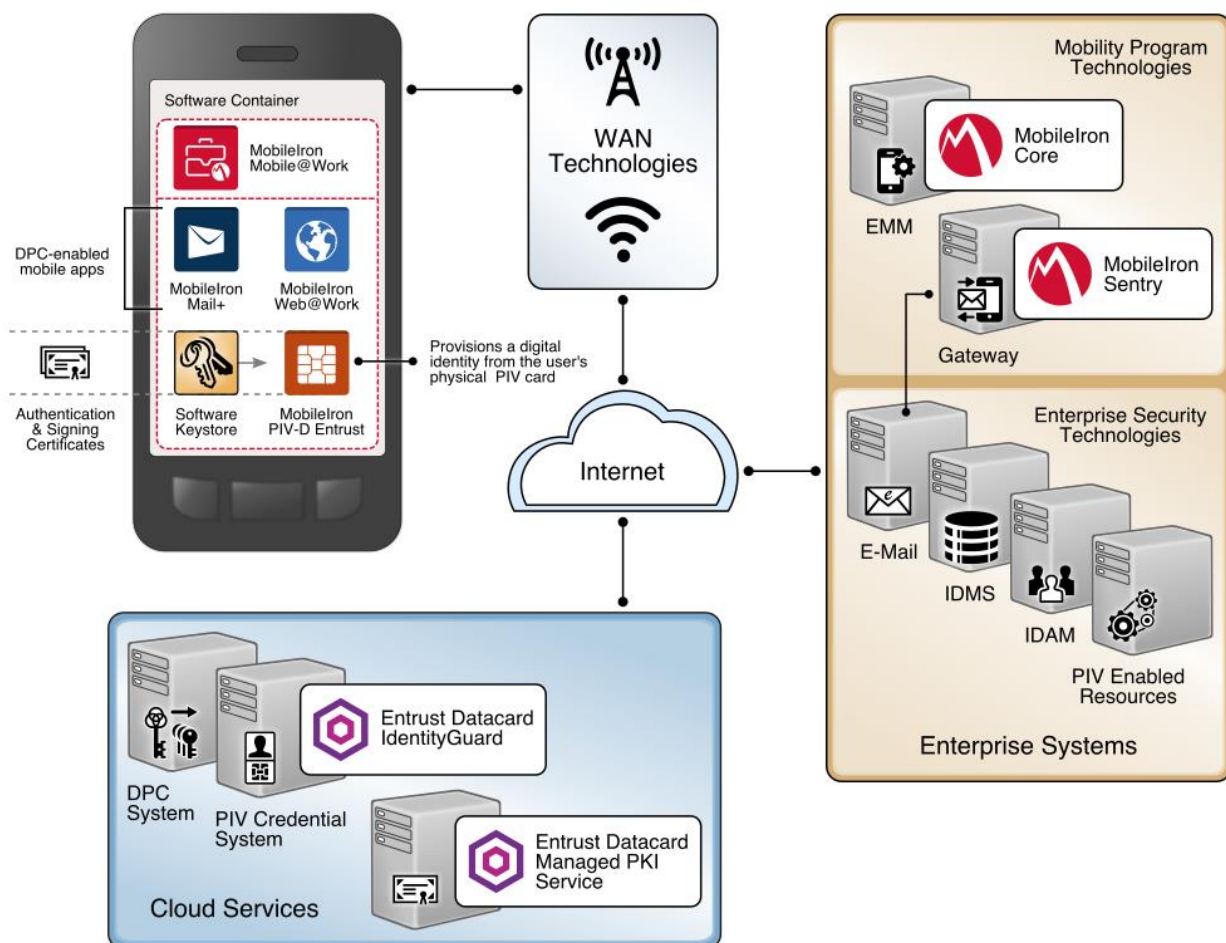
4.3 Hybrid Architecture for PIV and DPC Life-Cycle Management

This architecture is described as *hybrid,* in that it utilizes resources that are located both on-premises and in the cloud. Organizations have chosen this architectural path to leverage previous investments in enterprise systems, such as identity management solutions, while simultaneously gaining efficiencies and agility from cloud services. In this scenario, the PIV Card and Derived PIV Credential Management Systems are deployed within a simulated internal enterprise network. A self-service kiosk, which serves as the enrollment station for DPC initial issuance, is also deployed on the internal network. The cloud-based managed PKI service is integrated with the on-premises CMS through a toolkit available for the CMS software.

In this example implementation, the life-cycle management capabilities of the DPC are an extension of the PIV issuance capabilities of a vendor product. PIV Card and DPC life-cycle management are tightly integrated, and the DPC applicant interacts with the same self-service portal that is used for PIV Card issuance. Fulfillment of PIV Card linkage requirements is simplified because of the close integration between PIV Card and DPC issuance. There is also a level of transparency and familiarity for users as they access the self-service capabilities of the solution.

This architecture supports traditional mobile devices and hybrid devices that run full desktop operating systems. Hybrid devices, sometimes referred to as convertible laptops, exhibit characteristics of both traditional laptops and mobile devices, such as having both integrated keyboards and touchscreens. Thus, two embedded cryptographic tokens are documented: software tokens for Android/iOS-based mobile devices and Intel processor-based hybrid devices that meet the hardware requirements documented in Section 3.6.2. Additionally, there are also Intel-specific support software versioning requirements that are documented in Part C of this guide that an implementer should consider.

This architecture also includes the Verizon SSP managed PKI service for issuing DPC Authentication certificates, which can be reached by traversing the Internet. While the selected CMS software can integrate with on-premises or cloud-based certificate authorities, in this example implementation the PKI service is cloud-based.

The DPC applicant downloads and installs the MyID Identity Agent application from Intercede. The architecture uses the MyID Identity Agent application, which manages provisioning the DPC Authentication certificate to the device and other life-cycle activities, and can be downloaded and installed by using Google Play and the Apple App Store.

This architecture supports options for mobile and Intel-based devices, which use software- and hardware-backed authenticators, respectively. The DPC applicant experience for initial issuance differs slightly, depending on the authenticator type. When requesting a DPC for a mobile device, the applicant is prompted to scan a quick response (QR) code by using the enrollment application once the back-end system has validated the PIV Authentication certificate. In Intel-based hybrid devices, however, the applicant is sent an OTP through an out-of-band notification scheme, which in this example

761 implementation uses email. Knowledge of the OTP verifies that the user attempting to collect the DPC is
762 the same user who requested it. More details of this process can be found in Section 5.2.2.1.

763 An implementer should consider using an EMM to automatically deploy the Identity Agent application to
764 mobile devices and to take advantage of secure application containers provided by the EMM. This
765 capability was not implemented due to project constraints but may be included in future revisions of
766 this guide. The Identity Agent communicates directly with the MyID CMS for provisioning and other
767 functions over the network. The back-end MyID CMS system is composed of components that can be
768 deployed in a layered fashion if desired to support a large user population. Table 4-1 lists the
769 components and corresponding descriptions.

770 **Table 4-1 MyID CMS Component Descriptions**

MyID Web Server	Hosts the MyID web services used to deliver functions to the MyID Self-Service Kiosk and MyID Identity Agent application
MyID Application Server	Hosts the MyID business object layer and connector to the Verizon SSP
MyID Database	Hosts the MyID database (SQL Server) used to store information credential policy, key management information, and audit records

771

772 Implementers of similar architectures should consider the deployment options that are available after
773 assessing existing infrastructure and security requirements. For instance, the web server component
774 used to provision DPC can be deployed on a separate web server to communicate with the self-service
775 kiosk. For remote enrollment this allows the web server component to be placed on a DMZ, isolating the
776 traffic from local networks. Additionally, this configuration supports a reverse proxy that can be placed
777 between the mobile device and the MyID web service. This breaks the connection between the mobile
778 device and the web service, allowing the traffic to be inspected before it is forwarded to the web
779 service.

780 The figures below depict high-level views of the example implementations of the hybrid architecture
781 used for this solution for DPC. Detailed, system-level figures can be found in Part C of this guide.
782 Figure 4-3 focuses on the mobile device implementation. Here, the Identity Agent application is used to
783 manage the DPC. The DPC Authentication key is stored in a software key store within the secure
784 container. The supporting cloud and enterprise systems as described above are also shown. Figure 4-4
785 depicts the architecture when an Intel-based device that supports Intel Authenticate is used to store the
786 DPC. Here, the Intercede self-service application is used to manage issuing the DPC. The DPC is then
787 available for smart card logon and VPN authentication. In this implementation, we exercised smart card
788 logon to observe the usage of the DPC.

789 **Figure 4-3 Mobile Device Hybrid Architecture for Both PIV Card and DPC Life-Cycle Management**

790
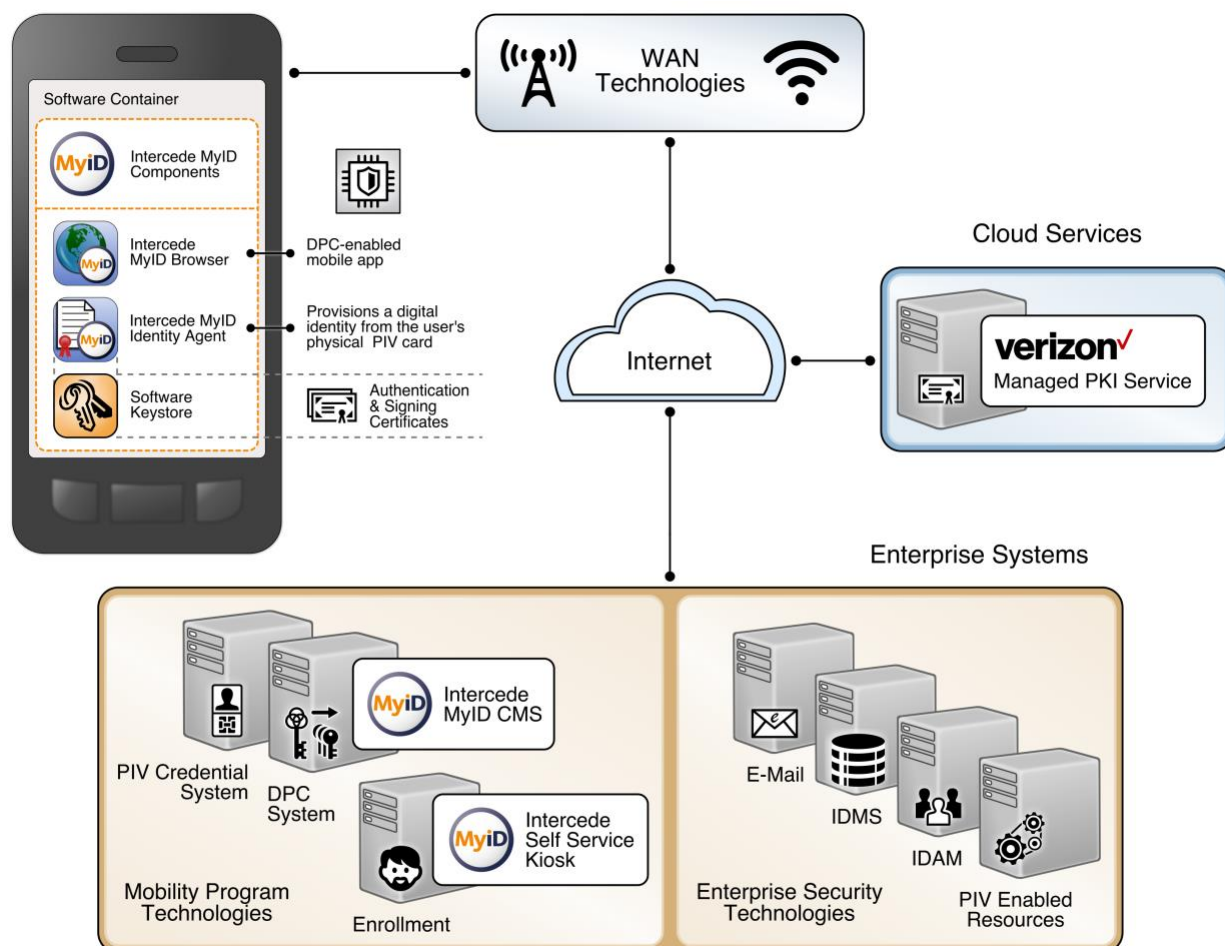
791 **Figure 4-4 Intel-Based Hybrid Architecture for Both PIV Card and DPC Life-Cycle Management**

792

793
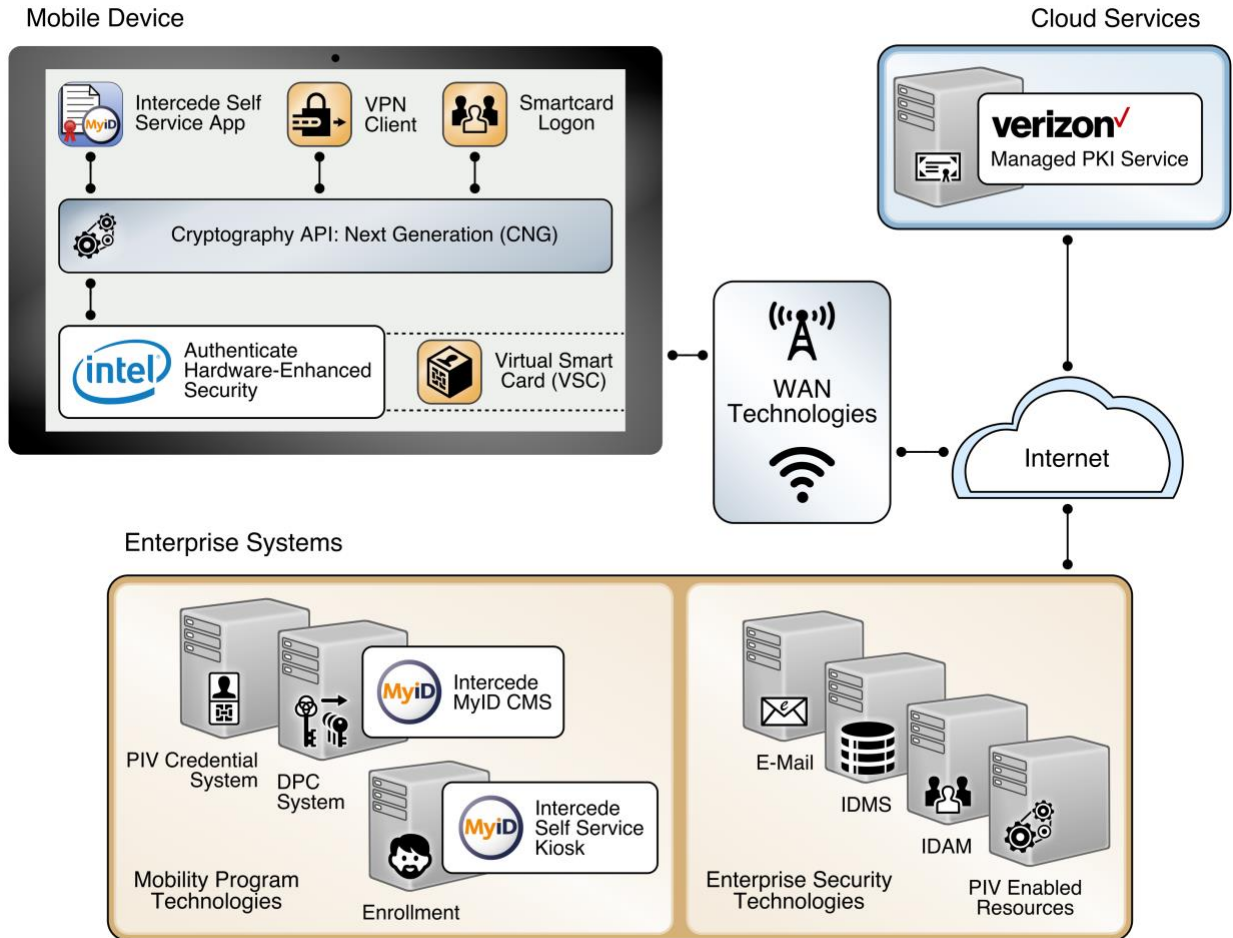
5 Security Characteristics Analysis

795 The purpose of the security characteristics analysis is to understand the extent to which the project
796 meets its objective of demonstrating the life cycle of DPC requirements specified in NIST SP 800-157. In
797 addition, it seeks to understand the security benefits and drawbacks of the example implementations.
798 Readers may also find Section 3.5 helpful when evaluating DPC security characteristics for their own
799 organization.

5.1 Assumptions and Limitations

801 The security characteristics analysis has the following limitations:

802 - It is neither a comprehensive test of all security components nor a red team exercise.

803 - It cannot identify all weaknesses.

804 - It does not include lab infrastructure. It assumes that devices and infrastructure are hardened.

5.2 Build Testing

806 This project uses Table 5, Requirements Definition and Implementation Mappings, from NIST IR 8055
807 [10] as a basis for testing the example implementations. Using the table as a foundation (see Appendix
808 C), we created a test plan that specifies test cases with traceability to DPC requirements. We collected
809 artifacts from each test case execution, such as screen captures and network packet traces, and
810 documented the results. In cases where a requirement could not be tested from our lab environment,
811 we collaborated with our build partners to document how a requirement could be fulfilled in a
812 production environment.

813 The sections below are a summary of the test case execution structured by NIST SP 800-157 life-cycle
814 stages: initial issuance, maintenance, and termination. Screenshots of certain operations aid the
815 narrative. Detailed workflow steps for these example implementations are found in Volume C of this
816 practice guide. Finally, our granular test results are available from the NCCoE website library:
817 https://nccoe.nist.gov/library/derived-piv-credentials-nist-sp-1800-12-practice-guide.

5.2.1 Managed Architecture Build Testing

5.2.1.1 Initial Issuance

820 With our Entrust Datacard example solution, the mobile device connects to the IdentityGuard system,
821 and the IdentityGuard connects to the CA, thereby handling delivery of the public certificate to the
822 mobile device, which follows the same process for issuing a PIV Card except that a QR is involved. In this
823 case, the DPC key pairs are generated on the mobile device, and the user's public key and certificate
824 signing request are securely passed to the CA for certificate issuance by IdentityGuard.

825 To test this example implementation, Entrust Datacard gave us access to a development instance of its
826 IdentityGuard service and populated it with identities of users who were issued test PIV Cards. These
827 users were also granted pre-approval to request a DPC. We observed that the prescribed DPC initial
828 issuance workflow, summarized below, adhered to the requirements in NIST SP 800-157 [6]. Note that
829 the figures below are screenshots from a shared IdentityGuard test infrastructure and feature an
830 AnyBank Self-Service logo. This image is configurable and is not intended to exclude federal agencies
831 from using this service.

832 As a prerequisite to issuance, we added our test DPC applicant's user account to an Active Directory
833 group associated with users authorized to use DPC. Users of this group are managed by a MobileIron
834 AppConnect policy configured to achieve compliance with NIST SP 800-157. The policy enforces multiple
835 issuance requirements, such as the need for a DPC applicant to create a six- to eight-digit password to
836 protect access to the private key associated with the DPC's PIV Authentication certificate. Additionally,
837 the test applicant has a mobile device enrolled into management by MobileIron Core. Two MobileIron
838 applications are employed: PIV-D Entrust, which is used in the DPC issuance workflow, and
839 Mobile@Work, which maintains the target software token where the DPC will be stored.

840 Issuance begins with the test DPC applicant (Matteo) authenticating to the Entrust IdentityGuard self-
841 service portal via PKI-AUTH multifactor authentication by using a computer and the applicant's valid PIV
842 Card (Figure 5-1 and Figure 5-2). The applicant then makes appropriate selections within the portal to
843 request issuance of a new DPC.

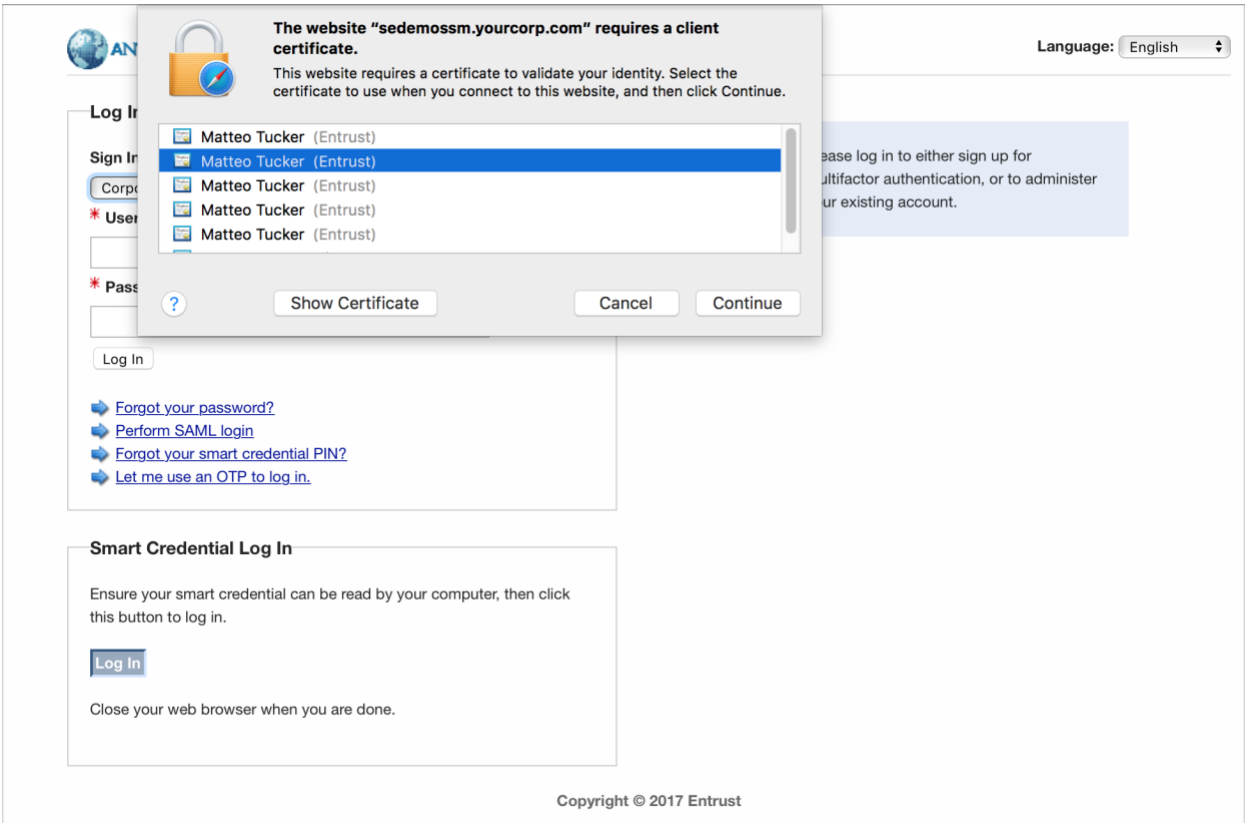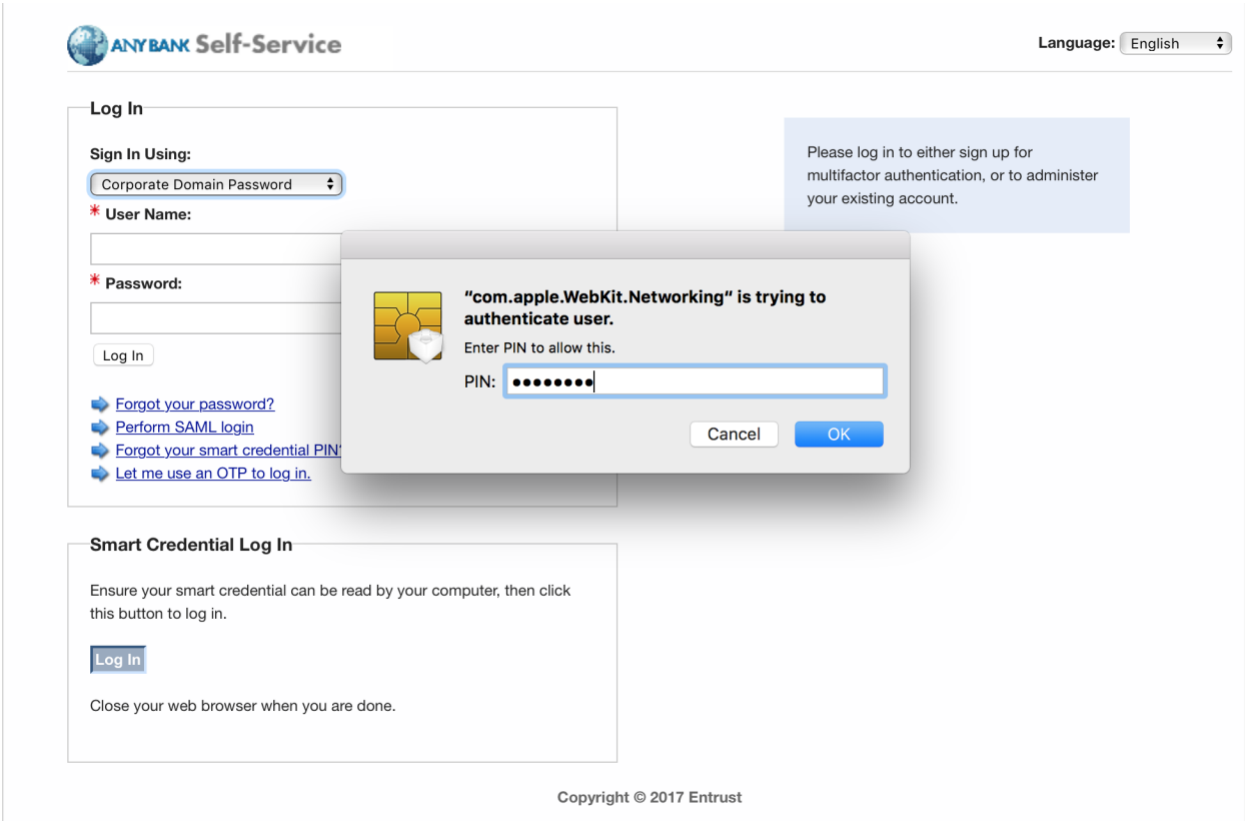844 **Figure 5-1 PIV Authentication Certificate Selection for PKI-AUTH**

845

846

847   **Figure 5-2 Password-Based Subscriber Authentication via PIN**


848
849   Entrust IdentityGuard presents a QR code and a numeric OTP (see [Figure 5-3](#)). These time-limited shared
850   secrets link Matteo's (the DPC applicant's) session from a computer to the Entrust IdentityGuard self-
851   service portal to the subsequent session between his target mobile device and Entrust IdentityGuard.

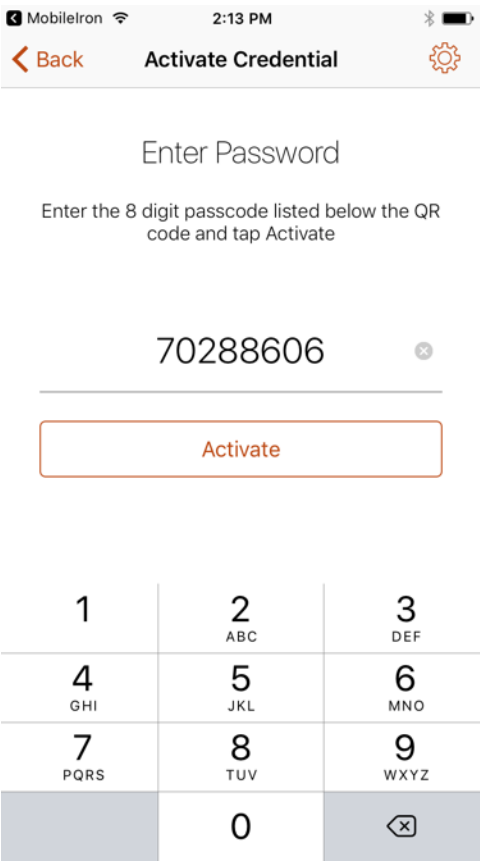852 **Figure 5-3 Entrust IdentityGuard DPC Activation Codes**
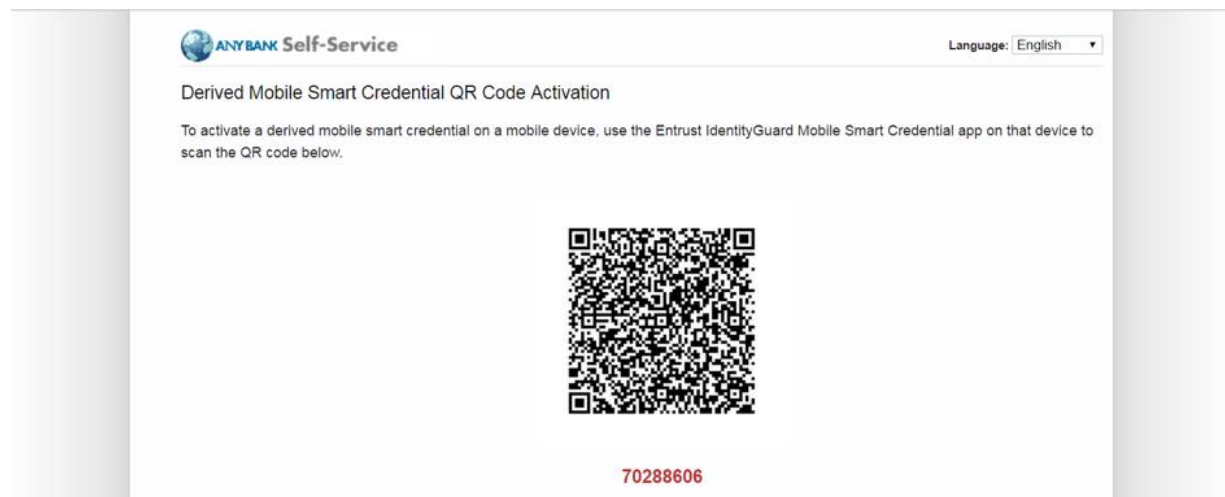
853
854 The applicant launches the MobileIron PIV-D Entrust application on the mobile device and uses it to scan
855 the QR code and enter the OTP. See Figure 5-4 and Figure 5-5.

856   **Figure 5-4 MobileIron PIV-D Entrust App**
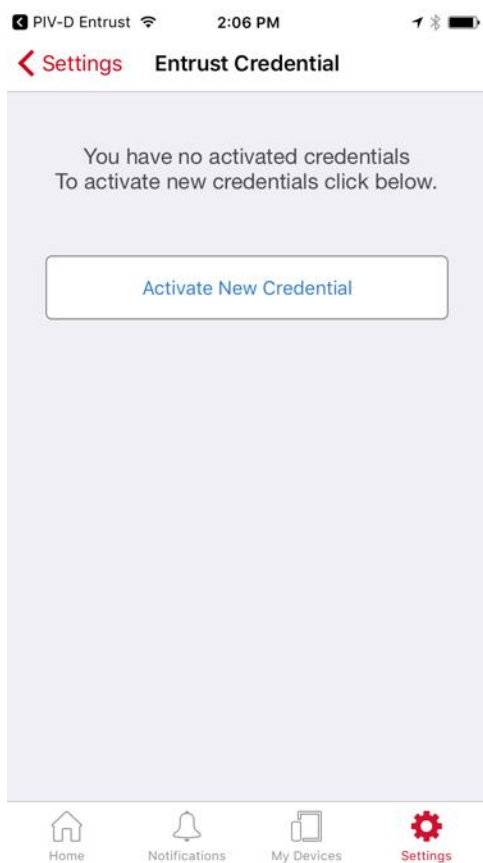

857

858   **Figure 5-5 Entrust DPC Activation**

859

860   The application then creates a TLS 1.2-secured session with Entrust IdentityGuard and authenticates
861   with the OTP. Once authenticated, the application generates asymmetric key pairs for Derived PIV
862   Authentication and digital signing certificates and transmits the certificate requests to Entrust
863   IdentityGuard. The IdentityGuard service verifies that the requested certificates match information on
864   file for the PIV subscriber for whom the OTP was generated (i.e., Matteo). Once verified, it forwards the
865   certificate requests to the Entrust CA, receives the DPC certificates, then relays them to the MobileIron
866   PIV-D Entrust application, where they are stored in the software token. The DPC subscriber must
867   authenticate to the MobileIron PIV-D Entrust container by using the created password before DPC
868   certificates or their associated private keys can be used by any application integrated with MobileIron.
869   See Figure 5-6 and Figure 5-7.

870   **Figure 5-6 PIV-D Application**

871
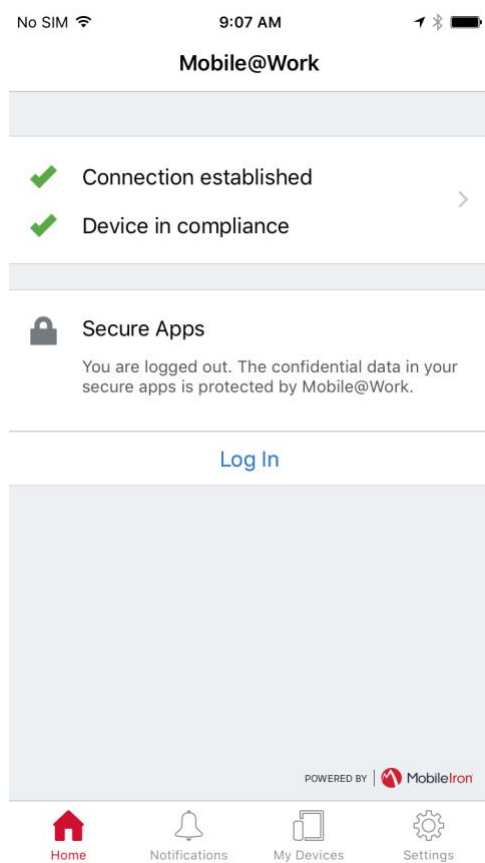
872　**Figure 5-7 PIV-D Passcode Entry**
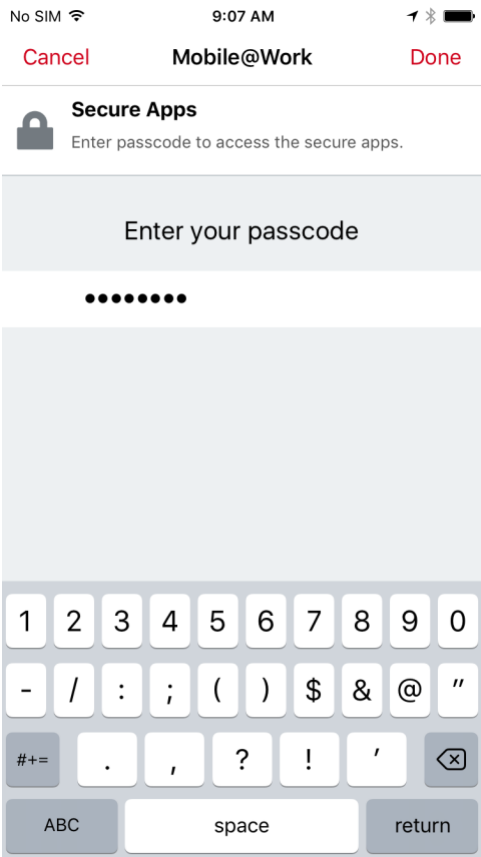
873

5.2.1.2　Maintenance

875　Maintenance activities for a DPC issued within this architecture are managed in two ways. Operations
876　that require generating a new PIV Authentication certificate (certificate modification or rekey) require
877　the DPC subscriber to repeat the initial issuance process as described in Section 5.2.1.1.

878　Linkage requirements between the status of the subscriber's PIV Card and DPC are covered by both the
879　CA and CMS being under control of Entrust Datacard. These systems exchange identity management
880　system data, and any necessary changes to the status of the subscriber's DPC will occur automatically.

5.2.1.3　Termination

882　Should the mobile device with a software token be lost or compromised, a DPC sponsor-initiated
883　workflow will specifically destroy the DPC by triggering the Retire Device operation available through the
884　MobileIron administrative console. This process removes the MobileIron and all Web@Work
885　applications, and cryptographically wipes the MobileIron PIV-D Entrust software token containing the
886　DPC. Triggering a remote wipe of all data on the device will also achieve this result. Further, the DPC

887 Authentication certificate can be directly revoked from the Entrust IdentityGuard interface (see Figure
888 5-8).

Figure 5-8 DPC IdentityGuard Termination

890

5.2.1.4 DPC Authentication Certificate Management

892 PKI management instructions between the Entrust IdentityGuard service and the Entrust Datacard
893 Managed CA use a combination of the Public Key Infrastructure X.509 - Certificate Management
894 Protocol (PKIX-CMP) and the XML Administration Protocol (XAP). PKIX-CMP [26] provides online
895 interactions between PKI components, including an exchange between a CA and a client system—in this
896 case, the Entrust IdentityGuard service. PKIX-CMP is defined as a standard by the IETF, which
897 standardizes many network-based protocols, in RFC 4210. The XAP protocol was developed by Entrust
898 Datacard and is used for administration tasks within the Entrust Datacard Managed CA.

899 The Entrust IdentityGuard service uses an XAP credential to securely communicate with the XAP
900 subsystem on the Entrust Datacard Managed CA. The Entrust IdentityGuard service uses XAP to obtain
901 an activation code, which is then used to create a PKIX-CMP General Message. The DPC certificate
902 request is then forwarded to the Entrust Datacard Managed CA in the Public Key Cryptography

903 Standards (PKCS) #10 format over PKIX-CMP. The Entrust Datacard Managed CA returns the signed DPC
904 certificate to the Entrust IdentityGuard service.

5.2.2 Hybrid Architecture Build Testing

5.2.2.1 Initial Issuance

907 Issuing the DPC in this test scenario is based upon the subscriber's ownership of a PIV credential and
908 DPC eligibility. In this example solution, the MyID CMS fulfills the role of a PIV Card issuer, a prerequisite
909 to enrollment for a DPC, having been configured with profiles that were compatible with the test PIV
910 Cards used in the example implementation. Next, we uploaded test PIV identities to the MyID CMS
911 through a specialized application that included required PIV data to be stored on the card. An Issue Card
912 workflow completed the PIV issuance within the MyID Desktop administrative console. PIV holders were
913 eligible for a Derived PIV when the identities were mapped to a local MyID group. See Figure 5-9 for a
914 screenshot of the test PIV Card user.

915 **Figure 5-9 Test PIV Card User**

916

917   The DPC issuance process begins with a DPC applicant using the PKI-AUTH authentication mechanism
918   from Section 6.2.3.1 of FIPS 201-2 [1] at the MyID Self-Service Kiosk. Once the applicant's PIV Card is
919   inserted into the kiosk, the applicant is prompted for the PIV Card PIN as depicted in Figure 5-10. After
920   successful PIV Card authentication, the kiosk transmits PIV Card information to the MyID CMS through
921   secure transport, where a job is created to handle the second phase of issuance to the endpoint.

922   **Figure 5-10 Kiosk Workflow**

923
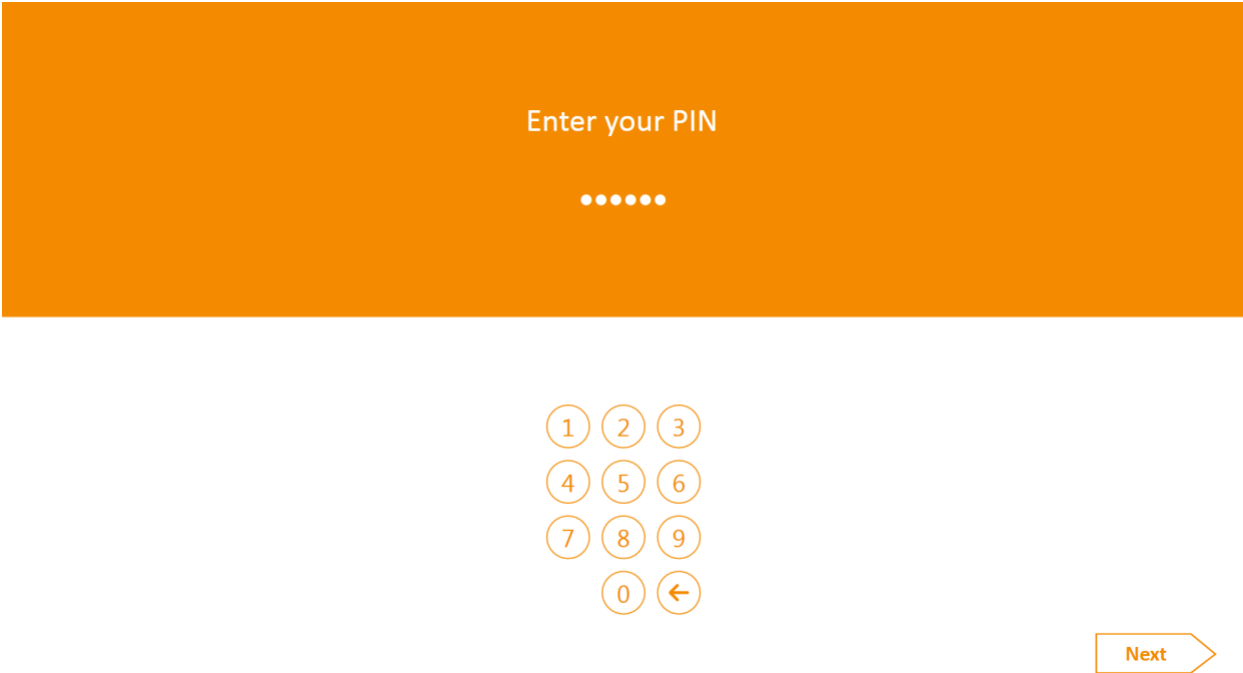
924   The DPC issuance process requires the use of the Identity Agent mobile application or the self-service
925   application to complete the workflow. In the case of an iOS or Android-based mobile device, the
926   applicant launches the Identity Agent application and scans a QR code presented by the self-service
927   kiosk. The QR code contains the information needed for the Identity Agent mobile application to
928   communicate securely with the MyID CMS back-end. After the MyID CMS has received and validated the
929   OTP obtained from the scanned QR code, the Identity Agent creates containers and generates a key pair
930   on the device by using a third-party FIPS 140-2-certified OpenSSL library for cryptographic services. The
931   public key is transmitted to the Intercede MyID back-end in the form of a PKCS #10 request. We
932   configured our MyID back-end instance to run within a local Internet Information Services instance that
933   uses a TLS endpoint. An implementer should consult NIST SP 800-52, Revision 1, *Guidelines for the*
934   *Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* for configuration
935   guidance in this area [27].

936 The authentication certificate request is then relayed to the Verizon Managed PKI. We used a test
937 instance of the Verizon Managed PKI in this project; however, the production version for U.S. federal
938 agencies has been granted an authority to operate (ATO) that requires a security controls assessment.
939 We encourage reviewing the ATO and associated security certification as part of an organization's risk
940 management process.

941 The DPC credential stored within the software container was protected with a PIN that can be
942 configured to more complex schemes within the MyID Desktop console. A PIN is required before the
943 certificate is delivered to the endpoint. The MyID Identity Agent mobile application displays a virtual
944 image of the associated PIV Card, as shown in Figure 5-11.

945 **Figure 5-11 DPC in MyID Identity Agent**

946
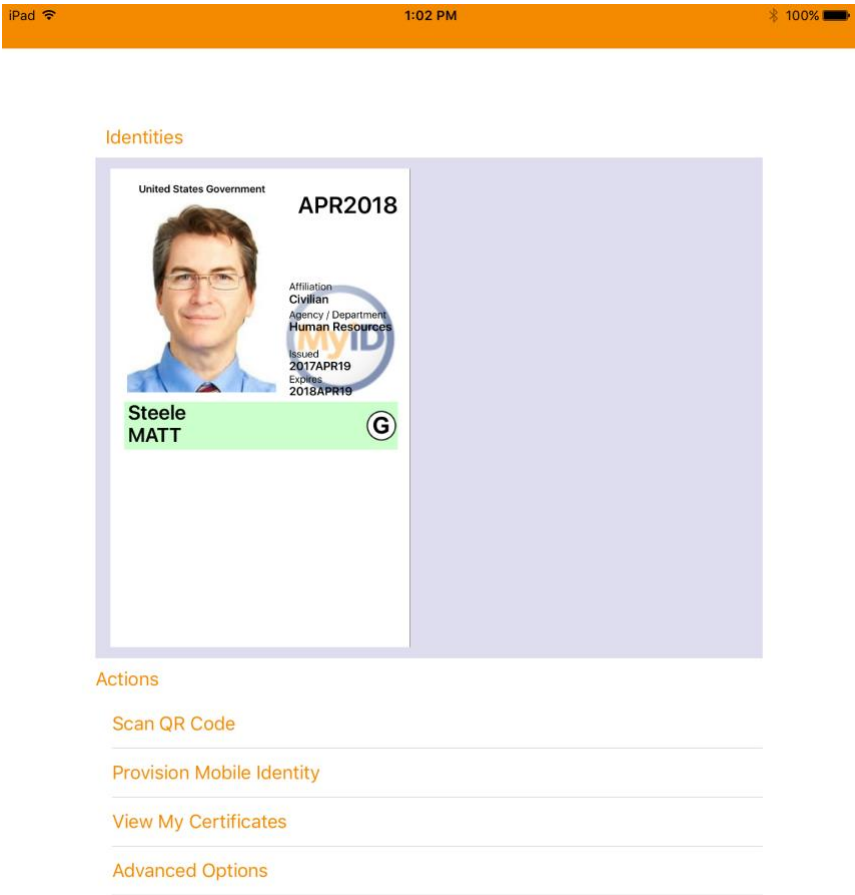
947 For Windows-based devices, the initial issuance process starts with the self-service kiosk, the same as
948 for mobile devices. Figure 5-12 shows an example.

949 **Figure 5-12 DPC Applicant Chooses Intel Credential Profile**

Select Credential Profile

- Derived PIV Profile
- DPC for iOS Native Keystore
- Entrust CA Derived PIV Profile
- Intel Authenticate DEBUG via MSCA
- Intel Authenticate DPC via Verizon CA
- Verizon Unicert DPC
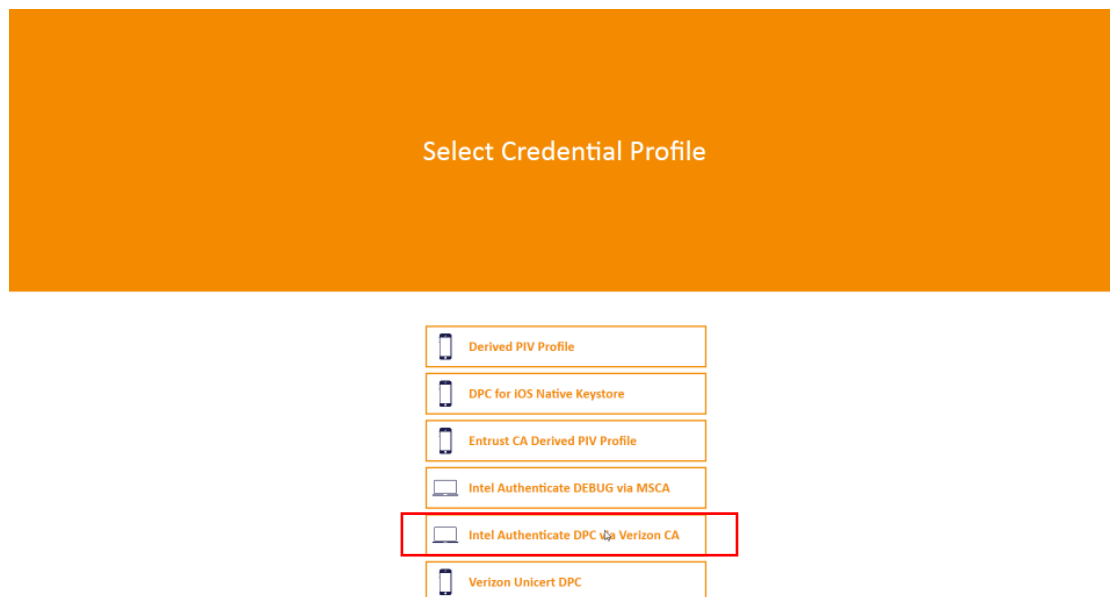
950

951 Instead of a QR code, however, an OTP is emailed to the DPC applicant (see Figure 5-13).

952 **Figure 5-13 Email Notification Message via Self-Service Kiosk**

An email has been sent to you with instructions for collecting your credential.

Remove your card
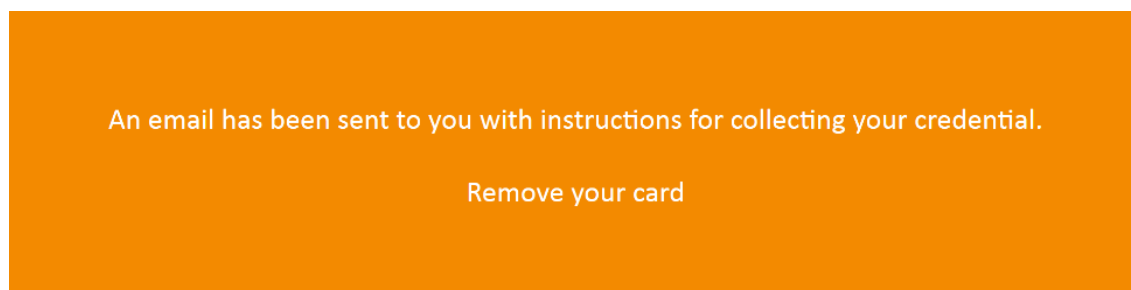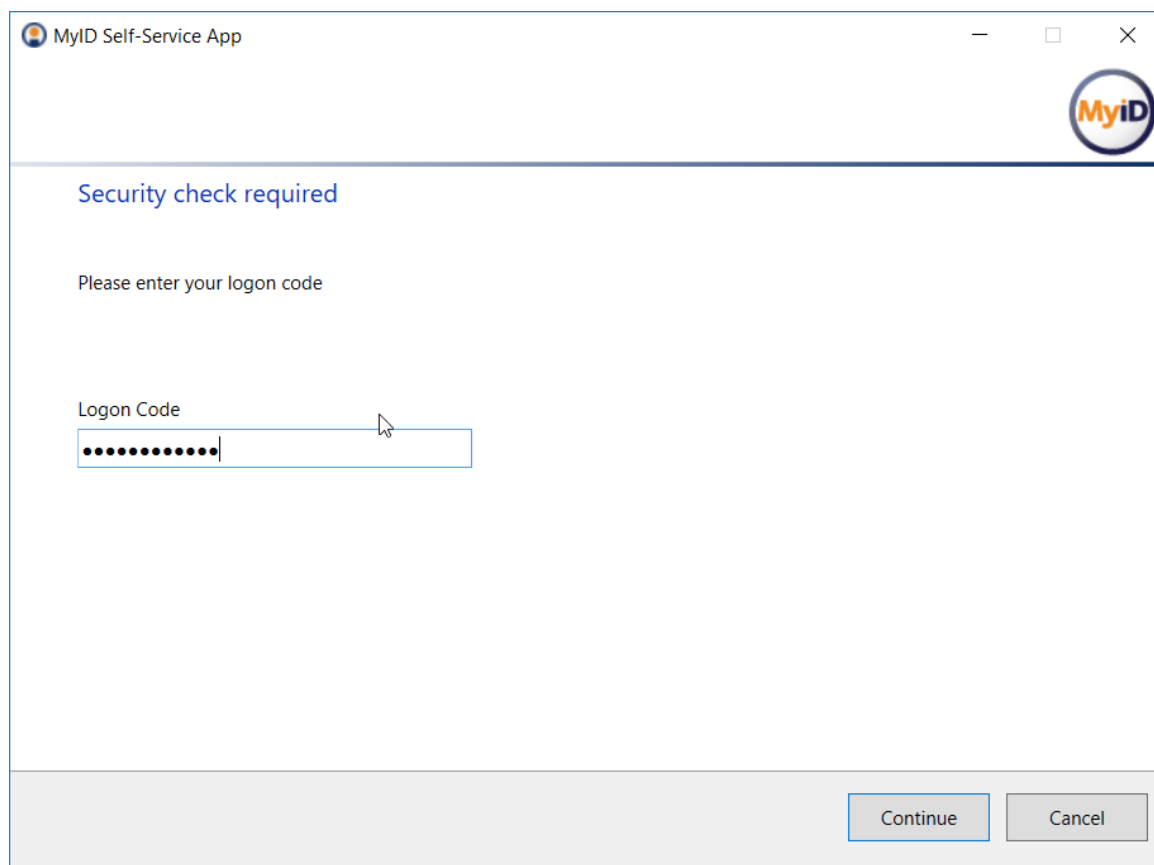
www.intercede.com

intercede

953

954 The DPC applicant then starts the self-service application on the device to collect the DPC credential (see
955 Figure 5-14).

956 **Figure 5-14 DPC Applicant Inputs the One-Time Code**

957

958 Once the DPC credential is issued to the Intel Authenticate token, it can be activated only by using a PIN
959 set by the DPC applicant through the Intel Authenticate client (see Part C for details). The client allows
960 the user to choose one or more additional *factors* to protect PKI-based keys; however, the PIN-based
961 protection scheme was chosen in this implementation to meet the guidelines in SP 800-157 and SP 800-
962 63-3. Further, there is an additional layer of security provided by the Intel-protected PIN input user
963 interface. The PIN pad exhibits the following security enhancements:

964 ▪ Software-based screen scraping or malware attacks that attempt to perform a screen capture of
965 the keypad cannot view the actual layout of the numbers. Instead, the entire keypad is blacked
966 out.

967 ▪ Each time the keypad window is presented, the numeric keypad is randomized. This means the
968 locations used to enter the PIN change every time. An attacker that captures the PIN entry
969 pattern for successful authenticator activation cannot use it for subsequent PIN entries.

970	▪	Authenticator activation input for the PIN entry is translated and used within the protective
971		hardware. The actual PIN value is not exposed outside the hardware.
972	▪	A "PIN throttling" mechanism tracks the number of incorrect PIN entry attempts, and at specific
973		intervals will refuse additional PIN attempts for a specific period. This feature minimizes brute
974		force attacks on the PIN.
975	▪	Keyboard entry of the PIN is not allowed. This feature minimizes keyboard logger attacks.

976 Post-issuance, the DPC Authentication certificate, along with an indication that the user controls the
977 associated private key, is visible through the Windows certificate Microsoft Management Console in the
978 Personal folder as shown below in Figure 5-15.

979 **Figure 5-15 Verizon SSP DPC Authentication Certificate**
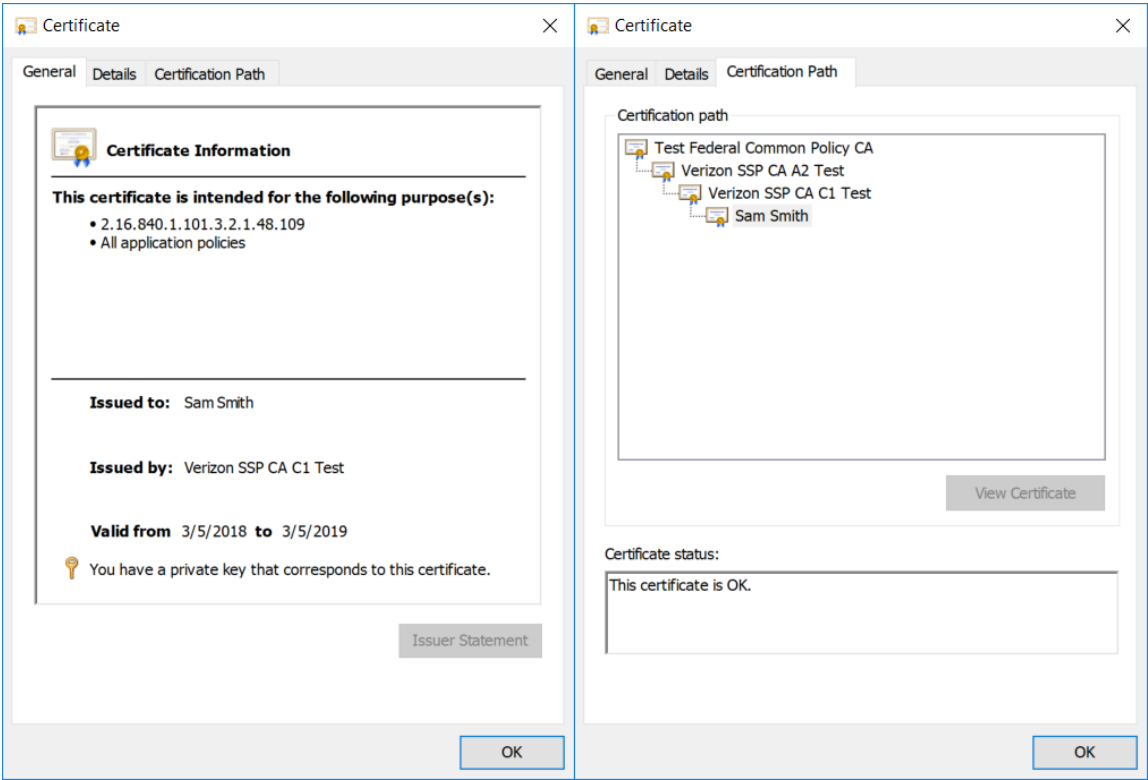
980

5.2.2.2 Maintenance

982 Maintenance activities for a DPC issued within this architecture are managed in two ways. Operations
983 that require generating a new PIV Authentication certificate (modification, rekey) require the DPC
984 subscriber to repeat the initial issuance process as described in Initial Issuance.

985 Linkage requirements between the status of the subscriber's PIV Card and DPC are covered by both the
986 PIV and DCMS database being shared within the same system; therefore, DPC processes have direct
987 access to PIV Card information.

5.2.2.3 Termination

989 Direct termination of the DPC is managed through the MyID Desktop console by executing the *Cancel*
990 *Credential* workflow. An administrator first finds the DPC subscriber within the database. After the
991 subscriber is found, all credentials issued to them are displayed, including the PIV credential linked to
992 the DPC. An administrator then selects the DPC targeted for termination. This action revokes all
993 certificates associated with the DPC for the target mobile device.

5.2.2.4 DPC Authentication Certificate Management

995 In this reference architecture, the Verizon SSP issued X.509 credentials for PIV and Derived PIV
996 identities. The Verizon SSP is integrated with the Intercede CMS through a software development kit
997 called the UniCERT Programmatic Interface (UPI) Java Toolkit. This toolkit communicates to the Verizon
998 SSP through an API that provides PKI functions (enrollment, management, and termination of
999 certificates). Confidentiality, integrity, and authenticity are protected by using TLS 1.2 to protect all
1000 operations. In a production setting, availability is ensured through load balancing, redundant systems,
1001 and disaster recovery sites. Contact a Verizon SSP representative to received detailed infrastructure
1002 diagrams.

5.3 Scenarios and Findings

1004 One aspect of our security evaluation involved assessing how well the reference architecture addresses
1005 the security characteristics it was intended to support. The Cybersecurity Framework subcategories
1006 were used to provide structure to the security assessment by consulting the specific sections of each
1007 framework component that are cited in reference to that subcategory. The cited sections provide
1008 validation points that the example implementations would be expected to exhibit. Using the
1009 Cybersecurity Framework subcategories as a basis for organizing our analysis allowed us to
1010 systematically consider how well the reference design supports the intended security characteristics.

1011 Our reference architectures primarily support the *Protect* (PR) function of the Cybersecurity Framework,
1012 which features Identity Management and Access Control (AC) as an outcome subcategory. We discuss
1013 the associated subcategories in the following subsections.

5.3.1 PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

To address the *Protect* function of the Cybersecurity Framework, users of the Derived PIV CMS in the *managed architecture* are administered through group and role membership. In this reference architecture, a privileged user managed the CMS configuration and security options in the Entrust Datacard IdentityGuard administrative website. Further, the on-premises deployment of MobileIron Core used a local privileged credential to manage configuration of the mobile device policies.

In the managed architecture, we worked with Entrust Datacard engineers to populate sample PIV information within IdentityGuard. This sample PIV user data was linked to local user data in an Active Directory repository that was also leveraged by the MobileIron Core user management system.

Similarly, in the hybrid architecture, access privileges for administrative functions are managed through group and role membership. For instance, the administrator role, which has the highest level of privilege, is separately defined from the manager role that is only responsible for requests from individual DPC holders.

The hybrid architecture also supports management of DPC users by obscuring authenticator feedback through a protected PIN pad when the DPC Authentication keys are stored by Intel Authenticate. The protected PIN pad reduces the threat of shoulder surfing from unauthorized individuals by randomizing the numeric keypad.

When an organization is ready for its own production deployment, we encourage a review of security controls mapped to this subcategory and for organizations to use *Best Practices for Privileged User PIV Authentication* [28] as a resource.

5.3.2 PR.AC-3: Remote Access Is Managed

To address the *Protect* function, the organizationally owned mobile devices of DPC subscribers are managed through an EMM to establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices [5]. While we used a basic set of security policies in our project to enforce DPC requirements, such as using an application passcode to unlock the DPC before use, holistic mobile device security implementation is out of scope for the example implementations within this practice guide. Readers should refer to the Mobile Device Security for Enterprises Project at the NCCoE for guidance that will enable tailoring the work in this practice guide for their organization's needs.

5.3.3 PR.AC-6: Identities Are Proofed and Bound to Credentials and Asserted in Interactions

To address the *Protect* function, a DPC solution can help authenticate nonorganizational users to logical systems. Implementers of systems that require PIV Authentication as part of access control can (if appropriate) accept DPC credentials from outside their organization. This is due to the DPC linkage to the PIV Card that leverages the processes and technical standards documented in NIST SP 800-63-3 and FIPS 201-2.

5.3.4 PR.AC-7: Users, Devices, and Other Assets Are Authenticated (e.g., Single-Factor, Multifactor) Commensurate with the Risk of the Transaction (e.g., individuals' security and privacy risks and other organizational risks)

To address the *Protect* function, the managed architecture with EMM integration example implementation allows an organization to create a policy to lock and/or wipe the device after an organization-set number of unsuccessful authenticator unlock attempts. This results in the DPC becoming unusable until an administrator acts to either unlock the device or force re-enrollment for the DPC.

5.3.5 PR.DS-2: Data-in-Transit Is Protected

To address the *Protect* function, the example implementations protect data in transit by ensuring the integrity and confidentiality through client/server mutually authenticated internet protocols. For example, network traffic originating from the mobile device transmitted to the EMM server and cloud services is protected through logical means by using TLS. Further, the cryptographic modules used in the DPC provisioning applications on the mobile device were validated to FIPS 140-2 Level 1. Table 5-1 lists the FIPS-validated modules used in the reference architectures.

Table 5-1 FIPS 140-2 Validation of Cryptographic Modules

Cryptographic Token FIPS 140-2 Validation	Cryptographic Token Type	Module Name	Module Type	Source
Level 1	MobileIron Container Software Token	OpenSSL FIPS Object Module	Software	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1747
Level 1	Intercede Container Software Token	OpenSSL FIPS Object Module	Software	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1747
Level 1	Intel Authenticate	Cryptographic Module for Intel vPro Platforms' Security Engine Chipset	Firmware-Hybrid	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2720

5.3.6 PR.DS-5: Protections Against Data Leaks Are Implemented

To address the *Protect* function, we used the client/server mutually authenticated internet protocols as mentioned in Section 5.3.5 as a boundary protection device, enforcing the flow control of DPC-related life-cycle information. The example implementations also protect against data leaks by restricting privileged accounts to specific personnel and by using local accounts. We also used subnetworks and DMZs to logically separate sensitive systems from other internal enterprise workstations.

5.3.7 PR.IP-3: Configuration Change Control Processes Are in Place

To address the *Protect* function, DPC processes and procedures in NIST SP 800-157 are managed through technical controls provided by the Derived PIV Credential Management Systems (Entrust Datacard IdentityGuard, Intercede MyID CMS). For example, if the PIV Card status is terminated, there is a process in place to revoke the DPC Authentication certificate.

5.4 Authenticator AAL Mapping

The strength of an authentication transaction is measured by the AAL. A higher AAL authenticator, such as the DPC means strong multifactor authentication. It requires more resources and capabilities by attackers to subvert the authentication process. Section 5.1.8.1 in SP 800-63-3B gives us the requirements for the AAL-2 software multifactor authenticator, which are applicable to the DPC AAL-2 (LOA-3) multifactor software example implementations documented in this practice guide. As such, Table 5-2 lists the authenticator requirements at AAL-2, which provide high confidence that the claimant controls the authenticator(s) bound to the subscriber's account and maps it to the corresponding requirement in SP 800-157. Readers may find this section helpful in their own risk assessments when evaluating authenticators to support AAL-2 authentication transaction requirements in SP 800-63-3B. See Table 4-1.

Table 5-2 AAL-2 Authenticator Requirements Mapping

Requirement Identifier	SP 800-63-3 Authenticator Requirement	SP 800-157 Guideline
1	Multifactor software cryptographic authenticators encapsulate one or more secret keys that are unique to the authenticator and are accessible only through the input of an additional factor—either a memorized secret or a biometric.	Use of the Derived PIV Authentication private key, or access to the plain text or wrapped private key, shall be blocked prior to password-based subscriber authentication….The required password length shall be at least six characters.
2	The key SHOULD be stored in suitably secure storage available to the authenticator application (e.g., key chain storage, Trusted Platform Module, Trusted Execution Environment).	Many mobile devices on the market provide a hybrid approach where the key is stored in hardware, but a software cryptographic module uses the key during an authentication operation….Therefore, the hybrid approach is recommended when supported by mobile devices and applications.
3	The key SHALL be strongly protected against unauthorized disclosure by access controls that limit access to the key to only those software components on the device requiring access.	No mapping exists.

Requirement Identifier	SP 800-63-3 Authenticator Requirement	SP 800-157 Guideline
4	Multifactor cryptographic software authenticators SHOULD discourage and SHALL NOT facilitate cloning of the secret key onto multiple devices.	For Derived PIV Authentication certificates issued under id-fpki-common-pivAuth-derived (LOA-3), the Derived PIV Authentication key pair shall be generated within a cryptographic module that has been validated to [FIPS 140] Level 1 or higher.
5	Any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric value at least six decimal digits in length or other memorized secret meeting the requirements of Section 5.1.1.2 (Memorized Secret Verifiers).	Use of the Derived PIV Authentication private key or access to the plain text or wrapped private key shall be blocked prior to password-based subscriber authentication….The required password length shall be at least six characters.
6	Any memorized secret used by the authenticator for activation SHALL be rate limited as specified in Section 5.2.2.	Throttling mechanisms may be used to limit the number of attempts that may be performed over a given period.
7	A biometric activation factor SHALL meet the requirements of Section 5.2.3, including limits on the number of consecutive authentication failures.	Biometric activation is outside the bounds of SP 800-157.
8	The unencrypted key and activation secret or biometric sample, and any biometric data derived from the biometric sample such as a probe produced through signal processing, SHALL be zeroized immediately after an authentication transaction has taken place.	No mapping exists. Biometric sample not collected for activation of the authenticator.

1091

1092 In Table 5-3, we have documented how each authenticator used in the reference architectures satisfies
1093 AAL-2 requirements identified in Table 5-2.

1094   **Table 5-3 AAL Technology Mappings**

Requirement Identifier	Authenticator		
	MobileIron Container Software Token	Intercede Container **Software Token**	**Intel Authenticate**
1	PIN required to activate token	PIN required to activate token	PIN required to activate token
2	Encrypted software container	Encrypted software container	Hardware/firmware protection
3	Authentication key available only to other MobileIron secure container applications with PIN	Authentication key available only to other Intercede secure container applications with PIN	Authentication key available for domain logon and VPN with PIN
4	No export mechanism available and device encryption discourages cloning	No export mechanism available and device encryption discourages cloning	Authentication key binds to unique Hardware key
5	Configurable PIN length and complexity rules	Configurable PIN length and complexity rules	Configurable PIN length and complexity rules
6	Configurable PIN lock after failed attempts	Configurable PIN lock after failed attempts	Protected PIN input has built-in throttling mechanism
7	Not applicable to a DPC implementation	Not applicable to a DPC implementation	Not applicable to a DPC implementation

6   Future Build Considerations

1095

1096   Mobile technologies such as DPC are constantly evolving. This project seeks to keep reasonable pace
1097   with the changing mobile landscape while sustaining an attainable scope bound by current policies.
1098   Moving forward, we will consider additional challenges for future DPC projects, including:

1099   ▪   **Application Enablement –** To leverage DPC, an organization needs to enable applications on its
1100   mobile devices and from the relying-party perspective. Mobile device application development
1101   is complicated by the various operating systems, cryptographic token options, and third-party
1102   software development kits provided by software containers. Further, modifying the source code
1103   of third-party closed mobile applications can be difficult or impossible. Relying parties face
1104   similar challenges with legacy systems that can be difficult to make ready for DPC. Future work

1105   might focus on adopting native embedded cryptographic tokens provided by hardware
1106   manufacturers and on using federations for relying parties such as cloud service providers.

1107 ▪ **Architecture Expansion –** Integrate with an identity management system (IDMS), which retains
1108   identity data that is retrieved from authoritative sources, to provide DPC subscriber PIV
1109   eligibility status information. NIST SP 800-157 recommends that the issuer of the DPC prevent
1110   further use of the DPC when the subscriber is no longer eligible for a PIV Card. Integration with
1111   an IDMS would store the eligibility of the DPC subscriber to help determine when DPC could be
1112   revoked, and it allows for DPC status to remain independent of the PIV Card status. This is
1113   helpful in the case of lost or stolen cards to allow a DPC subscriber to keep working without a
1114   PIV Card.

1115 ▪ **Key Management Key Recovery –** Mobile users should be able to recover key management keys
1116   from escrow. Unlike a signature key, the same key management key that is stored on the PIV
1117   Card is necessary to decrypt encrypted email stored on the device, for example.

1118 The NCCoE DPC project team welcomes submissions of use cases, noting that such input could become
1119 the basis for additional challenges for future projects. Please submit your use cases to
1120 piv-nccoe@nist.gov.

1121

Appendix A   List of Acronyms

AAL	Authenticator Assurance Level
AD	Active Directory
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATO	Authority to Operate
BGP	Border Gateway Protocol
CA	Certificate Authority
CMS	Credential Management System
COI	Community of Interest
CRADA	Cooperative Research and Development Agreement
CRL	Certificate Revocation List
CSP	Credential Service Provider
CVE	Common Vulnerabilities and Exposures
DCMS	Derived PIV Credential Management System
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNS	Domain Name System
DPC	Derived PIV Credential
EMM	Enterprise Mobility Management
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FRN	Federal Register Notice
GPS	Global Positioning System
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive-12
HTTP	Hypertext Transfer Protocol
IAL	Identity Assurance Level
ICAM	Identity, Credential, and Access Management
IDMS	Identity Management System
IETF	Internet Engineering Task Force

IR	Internal Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LOA	Level of Assurance
microSD	Micro Secure Digital
MMS	Multimedia Messaging Service
MTC	Mobile Threat Catalogue
NCCoE	National Cybersecurity Center of Excellence
NFC	Near-Field Communication
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OCSP	Online Certificate Status Protocol
OS	Operating System
OTP	One-Time Password
PC	Personal Computer
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX-CMP	Public Key Infrastructure X.509—Certificate Management Protocol
QR	Quick Response
RCS	Rich Communication Services
RFC	Request for Comments
RFI	Request for Information
RMF	Risk Management Framework
SaaS	Software as a Service
SCVP	Simple Certificate
SD	Secure Digital
SIM	Subscriber Identity Module
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol

SP	Special Publication
SQL	Structured Query Language
SSM	Self-Service Module
SSP	Shared Service Provider
TLS	Transport Layer Security
UICC	Universal Integrated Circuit Card
UPI	UniCERT Programmatic Interface
URL	Uniform Resource Locator
U.S.	United States
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
USSD	Unstructured Supplementary Service Data
VoLTE	Voice over Long-Term Evolution
VPN	Virtual Private Network
XAP	XML Administration Protocol

Appendix B   Glossary

All significant technical terms used within this document are defined in other key documents, including NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* [6], and NIST SP 800-63-3, *Digital Identity Guidelines* [7]. As a convenience to the reader, terms critical to an understanding of DPC are in this glossary.

applicant	An individual who has applied for, but has not yet been issued, a Derived PIV Credential.
asymmetric keys	Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
authenticated protected channel	An encrypted channel that uses approved cryptography where the connection initiator (client) has authenticated the recipient (server).
authentication	The process of establishing confidence of authenticity. In this case, it is the validity of a person's identity and the PIV Card.
card	An integrated circuit card.
cardholder	An individual possessing an issued PIV Card.
card management system	The system that manages the life cycle of a PIV Card application.
card reader	An electronic device that connects an integrated circuit card and the card applications therein to a client application.
certificate revocation list	A list of revoked public key certificates created and digitally signed by a certification authority.
Certification Authority	A trusted entity that issues and revokes public key certificates.
credential	Evidence attesting to one's right to credit or authority. In this standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.
cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.
demilitarized zone	Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's information assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Derived PIV Application	A standardized application residing on a removable hardware cryptographic token that hosts a Derived PIV Credential and associated mandatory and optional elements.
Derived PIV Credential	An X.509 Derived PIV Authentication certificate with associated public and private key that is issued in accordance with the requirements specified in this document where the PIV Authentication certificate on the applicant's PIV Card serves as the original credential. The Derived PIV Credential is an additional common identity credential under HSPD-12 and FIPS 201 that is issued by a federal department or agency and is used with mobile devices.
e-authentication assurance level	A measure of trust or confidence in an authentication mechanism defined in publications OMB-04-04 and NIST SP 800-63 in terms of four levels: ▪ Level 1: LITTLE OR NO confidence ▪ Level 2: SOME confidence ▪ Level 3: HIGH confidence ▪ Level 4: VERY HIGH confidence
Federal Information Processing Standards	A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST. A FIPS covers a specific topic in information technology to achieve a common level of quality or some level of interoperability.
identity	The set of physical and behavioral characteristics by which an individual is uniquely recognizable.
identity management system	One or more systems or applications that manage the identity verification, validation, and issuance process.
identity proofing	The process of providing sufficient information (e.g., identity history, credentials, documents) to establish an identity.
identity verification	The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those credentials previously proven and stored in the PIV Card or system and associated with the identity being claimed.
issuer	The organization that is issuing the PIV Card (or DPC) to an applicant. Typically, this is an organization for which the applicant is working.

level of assurance	OMB Memorandum M-04-04 describes four levels of identity assurance and references NIST technical standards and guidelines, which are developed for agencies to use in identifying the appropriate authentication technologies that meet their requirements.
mobile device	A portable computing device that (1) has a small form factor so it can easily be carried by a single individual; (2) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (3) possesses local, non-removable or removable data storage; and (4) includes a self-contained power source. Mobile devices may also include voice communication capabilities, onboard sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and e-readers.
multifactor authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
personal identification number	A secret number that a cardholder memorizes and uses to authenticate his or her identity as part of multifactor authentication.
personal identity verification (card)	A physical artifact (e.g., identity card, "smart" card) issued to an individual, which contains a PIV Card application that 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).
PKI-PIV Authentication key (PKI-AUTH)	A PIV Authentication mechanism that is implemented by an asymmetric key challenge/response protocol by using the PIV Authentication key of the PIV Card and a contact reader or a contactless card reader that supports the virtual contact interface.
private key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.
public key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.
public key infrastructure	A support service to the PIV System that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of enterprise data.

sponsor	Submits a Derived PIV Credential request on behalf of the applicant.
subscriber	The individual who is the subject named or identified in a Derived PIV Authentication certificate and who holds the token that contains the private key that corresponds to the public key in the certificate.

Appendix C   NIST IR 8055 [10] Requirements Enumeration and Implementation Mappings

Regulatory Requirement	Req. Number	Req. Section Number	Requirement Name
RC1—Device and Cryptographic Token	RC1.1	2.3.1.1	Private key in cryptographic module
	RC1.2	2.3.1.2	Alternative tokens
	RC1.3	2.3.1.7	Only digital signatures demonstrated (Section 4.8.2)
	RC1.4	2.3.3.5.1	Zeroize or destroy the token due to lost, stolen, damaged, or compromised device
	RC1.5	2.3.3.5.2	Zeroize or destroy the token due to transfer of token or device to another individual
	RC1.6	2.3.3.5.3	Zeroize or destroy the token due to no longer being eligible to have a PIV Card
	RC1.7	2.3.3.5.4	Zeroize or destroy the token due to no longer being eligible to have a DPC
	RC1.8	2.3.5.3.1.1	Removable hardware cryptographic tokens: interface of PIV Card
	RC1.9	2.3.5.3.1.2	Removable hardware cryptographic tokens: secure element
	RC1.10	2.3.5.3.1.3	Removable hardware cryptographic tokens: NIST SP 800-157 Appendix B Application Protocol Data Unit command interface
	RC1.11	2.3.5.3.1.4	Removable hardware cryptographic tokens: NIST SP 800-157 Appendix B digital signature, key management, authentication private key, and its corresponding certificate
	RC1.12	2.3.5.3.1.5.1	Removable hardware cryptographic tokens: Secure Digital (SD) card with cryptographic module: onboard secure element or security system
	RC1.13	2.3.5.3.1.5.2	Removable hardware cryptographic tokens: SD card with cryptographic module: NIST SP 800-157 Appendix B interface with the card commands

Regulatory Requirement	Req. Number	Req. Section Number	Requirement Name
	RC1.14	2.3.5.3.1.6.1	Removable hardware cryptographic tokens: Universal Integrated Circuit Card (UICC): separate security domain for Derived PIV Application
	RC1.15	2.3.5.3.1.6.2	Removable hardware cryptographic tokens: UICC: NIST SP 800-157 Appendix B application protocol data unit (APDU) command interface
	RC1.16	2.3.5.3.1.6.3	Removable hardware cryptographic tokens: UICC: *Global Platform Card Secure Element Configuration v1.0*
	RC1.17	2.3.5.3.1.7.1	Removable hardware cryptographic tokens: USB token with cryptographic module: integrated secure element with *Smart Card Integrated Circuit Card Devices Specification for USB Integrated Circuit Card Devices*
	RC1.18	2.3.5.3.1.7.2	Removable hardware cryptographic tokens: USB token with cryptographic module: NIST SP 800-157 Appendix B application protocol data units command interface with bulk-out and bulk-in command pipe
	RC1.19	2.3.5.3.1.7.2	Removable hardware cryptographic tokens: USB token with cryptographic module: NIST SP 800-96 for APDU support for contact card readers
	RC1.20	2.3.5.3.2.1	Embedded cryptographic tokens: hardware or software cryptographic module
	RC1.21	2.3.5.3.2.2	Embedded cryptographic tokens: software cryptographic module at LOA-3
	RC1.22	2.3.5.3.2.3	Embedded cryptographic tokens: key stored in hardware with a software cryptographic module using the key at LOA-3
	RC1.23	2.3.5.3.2.4	Embedded cryptographic tokens: id-fpki-common-pivAuth-derived-hardware or id-fpki-common-pivAuth-derived for certificates

Regulatory Requirement	Req. Number	Req. Section Number	Requirement Name
	RC1.24	2.3.5.3.2.5	Embedded cryptographic tokens: other keys stored in the same cryptographic module
	RC1.25	2.3.5.4.6	Embedded cryptographic tokens: authentication mechanism implemented by hardware or software mechanism outside cryptographic boundary at LOA-3
	RC1.26	2.3.5.4.7	Implementation and enforcement of authentication mechanism by cryptographic module at LOA-4
	RC1.27	2.3.5.4.10	Support password reset per Appendix B of NIST SP 800-157 for removable token and new issuance of certificate for LOA-3
RC2—PIV Card	RC2.1	2.3.1.4	Identity proofing
	RC2.2	2.3.1.5	Proof of possession of a valid PIV Card
	RC2.3	2.3.2.1	Verification of applicant's PIV Authentication for issuance
	RC2.4	2.3.2.2	Revocation status of PIV Authentication certificate checked after seven days of issuance
	RC2.5	2.3.2.10	Issuance of multiple DPC
RC3—PKI	RC3.1	2.3.1.3	PKI-based DPC at LOA-3 and LOA-4
	RC3.2	2.3.1.6	X.509 public key certificate
	RC3.3	2.3.3.6	Issuance of Derived PIV Authentication certificate because of subscriber name change
	RC3.4	2.3.5.1.2	Worksheet 10: Derived PIV Authentication certificate profile found in *X.509 Certificate and Certificate Revocation List Profile for the Shared Service Providers Program*
	RC3.5	2.3.5.1.3	No dependency with expiration date of the Derived PIV Authentication certificate with PIV Card
	RC3.6	2.3.5.2.1	NIST SP 800-78 cryptographic algorithm and key size requirements for the Derived PIV Authentication certificate and private key

Regulatory Requirement	Req. Number	Req. Section Number	Requirement Name
RC4—Level of Assurance	RC4.1	2.3.2.3	LOA-3 or LOA-4
	RC4.2	2.3.2.4	LOA-3 DPC issued in person or remotely
	RC4.3	2.3.2.5	Authenticated and protected channel for remote issuance
	RC4.4	2.3.2.6	Identification of each encounter in issuance process involving two or more electronic transactions
	RC4.5	2.3.2.7	Identification of applicant by using biometric sample for LOA-4
	RC4.6	2.3.2.8	Identification of each encounter in issuance process involving two or more electronic transactions of applicant by using biometric sample for LOA-4
	RC4.7	2.3.2.9	Retain biometric sample of applicant for LOA-4
	RC4.8	2.3.3.1	Communication over mutually authenticated secure sessions between issuer and cryptographic module for LOA-4
	RC4.9	2.3.3.2	Encrypted and integrity checks for data transmitted between issuer and cryptographic module for LOA-4
	RC4.10	2.3.3.3	Rekey of and expired or compromised DPC
	RC4.11	2.3.3.4	Rekey of and expired or compromised 2.3.3.4 DPC to new hardware token at LOA-4
	RC4.12	2.3.5.1.1	id-fpki-common-pivAuth-derived-hardware (LOA-4) or id-fpki-common-pivAuth-derived (LOA-3) policy of the X.509 Certificate Policy
	RC4.13	2.3.5.2.2	Key pair generated in hardware cryptographic module validated to FIPS 140 level 2 or higher with level 3 physical security protection for LOA-4
	RC4.14	2.3.5.2.3	Key pair generated in cryptographic module validated to FIPS 140 level 1 or higher for LOA-3

Regulatory Requirement	Req. Number	Req. Section Number	Requirement Name
RC5—Credential Management System	RC5.1	2.3.4.1	Issuance of a DPC based on information of applicant's PIV Card
	RC5.2	2.3.4.2	Periodically check the status of the PIV Card
	RC5.3	2.3.4.3.1	Termination status of PIV Card checked every 18 hours via notification system
	RC5.4	2.3.4.3.2	Termination of the PIV and DPC record on an integrated management system
	RC5.5	2.3.4.4	Track beyond the revocation of the PIV Authentication certificate
	RC5.6	2.3.4.5.1	Direct access to the PIV Card information for integrated PIV and DPC system
	RC5.7	2.3.4.5.2.1	Access to the back-end attribute exchange
	RC5.8	2.3.4.5.2.2	Notification of DPC system issuer with issuer of PIV Card
	RC5.9	2.3.4.5.2.3	Access to the Uniform Reliability and Revocation Service for termination status
	RC5.10	2.3.5.4.1	Password-based subscriber authentication for Derived PIV Authentication private key
	RC5.11	2.3.5.4.2	Password is not guessable or individually identifiable
	RC5.12	2.3.5.4.3	Minimum password length of six characters
	RC5.13	2.3.5.4.4	Block use of Derived PIV Authentication key after a number of consecutive failed activation attempts
	RC5.14	2.3.5.4.5	Limit number of attempts over period of 2.3.5.4.5 time with throttling mechanisms
	RC5.15	2.3.5.4.8.1	Password reset in person: authentication via PKI-AUTH mechanism with subscriber's PIV Card
	RC5.16	2.3.5.4.8.2	Password reset in person: biometric match on subscriber PIV Card or stored in the chain of trust

Regulatory Requirement	Req. Number	Req. Section Number	Requirement Name
	RC5.17	2.3.5.4.9.1	Password reset remotely: authentication via PKI-AUTH mechanism with subscriber's PIV Card
	RC5.18	2.3.5.4.9.2	Password reset remotely: strong linkage between the PKI-AUTH session and reset session
	RC5.19	2.3.5.4.9.3	Password reset remotely: same subscriber for the DPC and the PIV Card
	RC5.20	2.3.5.4.9.4	Password reset remotely: reset completed over a protected session

Appendix D   References

[1]   *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, Department of Homeland Security [Website], https://www.dhs.gov/homeland-security-presidential-directive-12 [accessed 7/27/18].

[2]   U.S. Department of Commerce, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Federal Information Processing Standards (FIPS) Publication 201-2, August 2013. https://doi.org/10.6028/NIST.FIPS.201-2 [accessed 7/27/18].

[3]   *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, National Institute of Standards and Technology [Website], https://www.nist.gov/cyberframework [accessed 7/27/18].

[4]   Joint Task Force Transformation Initiative, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*, NIST Special Publication (SP) 800-37 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2010. https://doi.org/10.6028/NIST.SP.800-37r1 [accessed 7/27/18].

[5]   Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013. https://doi.org/10.6028/NIST.SP.800-53r4 [accessed 7/27/18].

[6]   H. Ferraiolo, D. Cooper, et al., *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, NIST Special Publication (SP) 800-157, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2014. https://doi.org/10.6028/NIST.SP.800-157 [accessed 7/27/18].

[7]   P. Grassi, M. Garcia, and J. Fenton, *Digital Identity Guidelines*, NIST Special Publication (SP) 800-63-3, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2017. https://doi.org/10.6028/NIST.SP.800-63-3 [accessed 7/27/18].

[8]   W. Newhouse, S. Keith, et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, NIST Special Publication (SP) 800-181, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2017. https://doi.org/10.6028/NIST.SP.800-181 [accessed 7/27/18].

[9]   *Mobile Threat Catalogue*, National Institute of Standards and Technology [Website], https://pages.nist.gov/mobile-threat-catalogue/ [accessed 7/27/18].

[10] M. Bartock, J. Cichonski, et al., *Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research,* NIST Internal Report (IR) 8055, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2016. https://doi.org/10.6028/NIST.IR.8055 [accessed 7/27/18].

[11] *Government Identity and Credentials*, IDManagement.gov [Website], https://www.idmanagement.gov/trust-services/#gov-identity-credentials [accessed 7/27/18].

[12] "Derived Personal Identity Verification Credentials Building Block," 80 *Federal Register* 157 (August 14, 2015). https://www.federalregister.gov/documents/2015/08/14/2015-20039/national-cybersecurity-center-of-excellence-derived-personal-identity-verification-credentials [accessed 7/27/18].

[13] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* NIST Special Publication (SP) 800-124 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2013. https://doi.org/10.6028/NIST.SP.800-124r1 [accessed 7/27/18].

[14] *Top 10 2014-I2 Insufficient Authentication/Authorization*, OWASP [Website], https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization [accessed 7/27/18].

[15] Department of Homeland Security, *Study on Mobile Device Security*, April 2017. https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf [accessed 7/27/18].

[16] Executive Order no. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal. [accessed 7/27/18]

[17] M. Barrett, J. Marron, et al., *The Cybersecurity Framework: Implementation Guidance for Federal Agencies,* Draft NIST Interagency Report (IR) 8170, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2017. https://csrc.nist.gov/publications/detail/nistir/8170/draft [accessed 7/27/18].

[18] C. Brown, S. Dog, et al., *Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue,* Draft NIST Interagency Report (IR) 8144, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2016. https://csrc.nist.gov/publications/detail/nistir/8144/draft [accessed 7/27/18].

[19] *National Vulnerability Database*, National Institute of Standards and Technology [Website], https://nvd.nist.gov/ [accessed 7/27/18].

[20] *CVE-2016-6716 Detail*, National Vulnerability Database [Website], https://nvd.nist.gov/vuln/detail/CVE-2016-6716 [accessed 7/27/18].

[21] S. Quirolgico, J. Voas, et al., *Vetting the Security of Mobile Applications*, NIST Special Publication (SP) 800-163, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2015. https://doi.org/10.6028/NIST.SP.800-163 [accessed 7/27/18].

[22] *Common Vulnerabilities and Exposures (CVE)*, CVE [Website], https://cve.mitre.org/ [accessed 7/27/18].

[23] U.S. General Services Administration, *Decision for Standard Assessment & Authorization*, Authorization to Operate Letter, November 3, 2016. https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/entrust-ato.pdf [accessed 7/27/18].

[24] E. Simmon, DRAFT - Evaluation of Cloud Computing Services Based on NIST 800-145, NIST Special Publication (SP) 500-322, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2017. https://www.nist.gov/sites/default/files/documents/2017/05/31/evaluation_of_cloud_computing_services_based_on_nist_800-145_20170427clean.pdf [accessed 7/27/18].

[25] Federal Public Key Infrastructure Policy Authority, *X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework*, *Version 1.24,* May 7, 2015. https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/Common-Policy-Framework.pdf [accessed 7/27/18].

[26] C. Adams, S. Farrell, et al., *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*, Internet Engineering Task Force (IETF) Request for Comments (RFC) 4210, September 2005. https://tools.ietf.org/html/rfc4210 [accessed 7/27/18].

[27] T. Polk, K. McKay, and S. Chokhani, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, NIST Special Publication (SP) 800-52 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2014. https://doi.org/10.6028/NIST.SP.800-52r1 [accessed 7/27/18].

[28] Computer Security Division and Applied Cybersecurity Division, *Best Practices for Privileged User PIV Authentication,* NIST Cybersecurity White Paper, National Institute of Standards and Technology, Gaithersburg, Maryland, April 21, 2016. https://doi.org/10.6028/NIST.CSWP.04212016 [accessed 7/27/18].