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
The MITRE Corporation
McLean, VA

September 2017

DRAFT

This publication is available free of charge from:
https://nccoe.nist.gov/projects/building-blocks/piv-credentials

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.

National Institute of Standards and Technology Special Publication 1800-12B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-12B, 57 pages, (September 2017), CODEN: NSPUE2

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: September 29, 2017 through November 29, 2017

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

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

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 this example solution 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://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 implementation 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 who require access to federally controlled facilities, information systems, and applications. In 2005, when FIPS 201 was published, logical access was geared toward traditional computing devices (i.e., desktop and laptop computers) where the PIV card provides common multifactor authentication mechanisms through integrated smart card readers across the federal government. With the emergence of computing devices such as tablets, convertible

computers, and in particular mobile devices, the use of PIV cards has proved 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 lifecycle 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 (DPCs) which leverage identity proofing and vetting results of current and valid PIV credentials.

To demonstrate the DPCs guidelines, the National Cybersecurity Center of Excellence (NCCoE) at NIST built a security architecture using commercial technology to manage the lifecycle of DPCs demonstrating the process that enables a PIV Card holder to establish DPCs in a mobile device which then can be used to allow the PIV Card holder to access websites that require PIV authentication.

This project resulted in a freely available NIST Cybersecurity Practice Guide which demonstrates how an organization can continue to provide two-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; network/software vulnerability; Personal Identity Verification (PIV); PIV card; smart card

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Walter Holda	MobileIron
Loay Oweis	MobileIron
Sean Frazier	MobileIron
Dan Miller	Entrust Datacard

Name	Organization
Bryan Rosensteel	Entrust Datacard
Emmanuel Bello-Ogunu	The MITRE Corporation
Sarah Kinling	The MITRE Corporation
Poornima Koka	The MITRE Corporation
Matthew Steele	The MITRE Corporation

The technology vendors who participated in this build submitted their capabilities in response to a notice in the Federal Register. Companies with relevant products 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 PKI
MobileIron	MobileIron Enterprise Mobility Management Platform

The NCCoE also wishes to acknowledge the special contributions of Intercede for providing us with feedback on the risk assessment section of this practice guide, including risk mitigation and residual risk association with a Derived PIV Credential system.

Contents

1 Summary 1

1.1 Challenge 2

1.2 Solution 3

1.3 Benefits 4

2 How to Use This Guide 4

2.1 Typographical Conventions 6

3 Approach 6

3.1 Audience 7

3.2 Scope 8

3.3 Assumptions 9

3.3.1 Modularity 9

3.3.2 Security 9

3.3.3 Existing Infrastructure 9

3.4 Risk Assessment 10

3.4.1 Threats 11

3.4.2 Vulnerabilities 16

3.4.3 Risk 17

3.4.4 Security Control Map 18

4 Architecture 19

4.1 Architecture Components 19

4.1.1 Credential Management System 19

4.1.2 PKI Managed Service 20

4.1.3 Enterprise Mobility Management 20

4.2 Technologies 20

4.2.1 Entrust Datacard 20

4.2.2 MobileIron 21

4.2.3 Mobile Devices 22

4.3 Managed Architecture with EMM Integration 23
5 Security Characteristics Analysis 24
5.1 Assumptions and Limitations 25
5.2 Build Testing 25
5.2.1 Example Solution Initial Issuance 25
5.2.2 Example Solution Maintenance 32
5.2.3 Example Solution Termination 32
5.2.4 DPC Certificate Issuance 33
5.3 Scenarios and Findings 34
5.3.1 PR.AC-1: Identities and Credentials Are Managed for Authorized Devices and Users 34
5.3.2 PR.AC-3: Remote Access is Managed 34
5.3.3 PR.DS-2: Data-in-Transit Is Protected 35
5.3.4 PR.DS-5: Protections Against Data Leaks Are Implemented 35
5.3.5 PR.IP-3: Configuration Change Control Processes Are in Place 35
6 Future Build Considerations 35
Appendix A List of Acronyms 37
Appendix B Glossary 39
Appendix C NISTIR 8055 [9] Requirements Enumeration and Implementation Mappings 42
Appendix D References 48

List of Figures

Figure 3-1 Project Phased Approach 7
Figure 4-1 PIV and DPC Cloud Service Lifecycle Management with EMM Integration 24
Figure 5-1 PIV Authentication Certificate Selection for PKI-AUTH 26
Figure 5-2 Password-Based Subscriber Authentication via PIN 27
Figure 5-3 Entrust IdentityGuard DPC Activation Codes 28
Figure 5-4 MobileIron PIV-D Entrust App 29
Figure 5-5 Entrust DPC Activation 30
Figure 5-6 PIV-D App 31
Figure 5-7 PIV-D Passcode Entry 32
Figure 5-8 PIV-D App Termination 33

List of Tables

Table 3-1 Enrollment and Identity Proofing Threats 11
Table 3-2 Authenticator Threats 13
Table 3-3 AAL Vendor Mappings 18
Table 3-4 Security Control Mappings 18
Table 4-1 Products and Technologies 21
Table 4-2 Mobile Devices 22

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 Standard (FIPS) 201 specified a common set of credentials in a smart card form factor [2], known as the *Personal Identity Verification (PIV) Card.* PIV Cards are now used government-wide as a primary credential for federal employees and contractors. PIV Cards enhance security using a standard issuance process by which agencies perform identity proofing and background checks. The PIV Cards are used for both physical access to government facilities and logical access to federal information systems, providing multi-factor authentication.

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 for 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 (DPCs) 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 DPCs 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 using commercial off the shelf (COTS) products so that the DPC can be used as intended leveraging the security of the PIV system: for remote authentication to information technology 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 identity proofing and vetting of a primary identity credential into mobile devices. To that end, the example solution in this practice guide works from a simple scenario that informs the basis of an architecture tailored to either the public or private sector, or both.

Starting with the NIST's Cybersecurity Framework [3], the Risk Management Framework (RMF) [4], and security controls from NIST Special Publication 800-53 [5], this document also references NIST Special Publication 800-157 *Guidelines for Derived Personal Identity Verification (PIV) Credentials* [6], NIST

Special Publication 800-63-3 *Digital Identity Guidelines* [7], Federal Information Processing Standards Publication 201-2 [2], Public Key Cryptography Standards, and NIST's *Mobile Threat Catalogue* [8].

We built the example solution and architecture on standards-based, commercially available products. The solutions can be used by any organization deploying Derived PIV Credentials, willing to perform their own risk assessment, and ready to implement controls based on their risk posture.

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

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

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

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

Section 5: Security Characteristics Analysis provides details about the tools and techniques we used to perform risk assessments pertaining to Derived PIV Credentials. It also summarizes the test sequences we employed to demonstrate security platform services, the Cybersecurity Framework functions to which each test sequence is relevant, and NIST Special Publication 800-157 (SP 800-157) [6] controls that applied to the functions being demonstrated.

Section 6: Future Build Considerations is a brief treatment of other applications that NIST and the NCCoE might explore in the future to further support Derived PIV Credentials.

The appendices provide a list of acronyms, references, key definitions, and a requirements table derived from NIST Internal Report (NISTIR) 8055 [9].

1.1 Challenge

Mobile phones and tablets are being increasingly deployed by federal agencies. Most of these devices lack a smart card reader that allow the devices to leverage the security and control characteristics of the FIPS 201-2 personal identity verification system standard.

FIPS 201-2 is a U.S. federal government standard that specifies PIV requirements for federal employees and contractors. FIPS 201-2 requires using credentials in the form of X.509 digital certificates, stored on

smart cards, in conjunction with personal identification numbers (PINs) and biometrics to provide multi-factor authentication to federal information systems [2]. The FIPS 201-2 standard contains the minimum requirements for a federal personal identity verification system that meets the control and security objectives of HSPD-12 [1], including identity proofing, registration, and issuance. The standard also provides detailed specifications that support technical interoperability among PIV systems of federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up the PIV identity credentials are specified in this standard. PIV Cards are used for both physical access to government facilities and logical access to federal information systems, providing multifactor authentication.

To address the issues of using PIV Cards with mobile devices, NIST Special Publication 800-157 (SP 800-157) [6] provides guidelines on issuing credentials in an alternate form factor on mobile devices that leverage the identity proofing performed for issuing the PIV Card. NISTIR 8055 [9] documents a proof of concept research showing that DPCs can be used to PIV enable these devices and provide multi-factor authentication for federal mobile device users.

Implementing Derived PIV Credentials in mobile phones and tablets is challenging due to the wide array of mobile device models and platforms that offer different ways to store the credentials and different key stores that include application containers (i.e., software containers) in credential management systems (CMS) and removable storage options (i.e., USB and micro Secure Digital cards).

Few efforts have been undertaken to explore Derived PIV Credentials implementation scenarios and the ability of those scenarios to adhere to PIV system standards.

1.2 Solution

This NIST Cybersecurity practice guide demonstrates how commercially available technologies can meet your organization's need to issue two-factor credentials to mobile devices for authentication with IT systems in operational environments.

We built an environment that resembles an enterprise network using commonplace components such as identity repositories, supporting certificate authorities, and web servers. Next products and capabilities were identified that, when linked together, provide an example solution demonstrating lifecycle functions outlined in NIST SP 800-157 [6]. This example solution leverages cloud services where possible through a Software as a Service (SaaS) component. The federal government encourages the use of SaaS or Shared Service Providers (SSP) [10]that operate under federal policy, such as certificate authorities operating in accordance with policy developed by the Federal Public Key Infrastructure (PKI) Policy Authority. The security controls for these SSPs are periodically assessed, allowing the organization to focus on its primary mission and avoid the costs associated with ongoing maintenance of these systems.

The NCCoE developed a collaborative team uniquely qualified to create an example solution of Derived PIV Credentials. We partnered with the subject matter experts who wrote NIST SP 800-157 to better understand its requirements and ensure that the integrations of commercial products were within the document's guidelines. Any aspects of the example solution that do not adhere to NIST SP 800-157 guidelines were noted.

1.3 Benefits

For organizations like yours that are planning and looking for solutions to issue DPCs to their workforce, the example solution described in this guide will help you navigate through the various options by:

- providing visibility into how the different device vendors and CMS vendors are implementing solutions for storing the credentials
- demonstrating the use of managed services for the DPC issuance and lifecycle management
- demonstrating an integration with an Enterprise Mobility Management (EMM) solution

2 How to Use This Guide

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

This guide contains three volumes:

- NIST SP 1800-12a: *Executive Summary*
- NIST SP 1800-12b: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-12c: *How-To Guides* – instructions for building the example solution

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

Business decision makers, including chief security and technology officers will be interested in the *Executive Summary (NIST SP 1800-12a)*, which describes the:

- challenges enterprises face in issuing strong, two-factor credentials to mobile devices
- example solution built at the NCCoE
- benefits of adopting the example solution

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

- Section 3.4.3, Risk, provides a description of the risk analysis we performed
- Section 3.4.4, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

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

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

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of Derived PIV Credentials example solutions. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Section 4.2, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

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

2.1 Typographical Conventions

The following table presents typographic conventions used in this volume.

Typeface/ Symbol	Meaning	Example
Italics	filenames and pathnames references to documents that are not hyperlinks, new terms, and 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, on-screen 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 http://nccoe.nist.gov

3 Approach

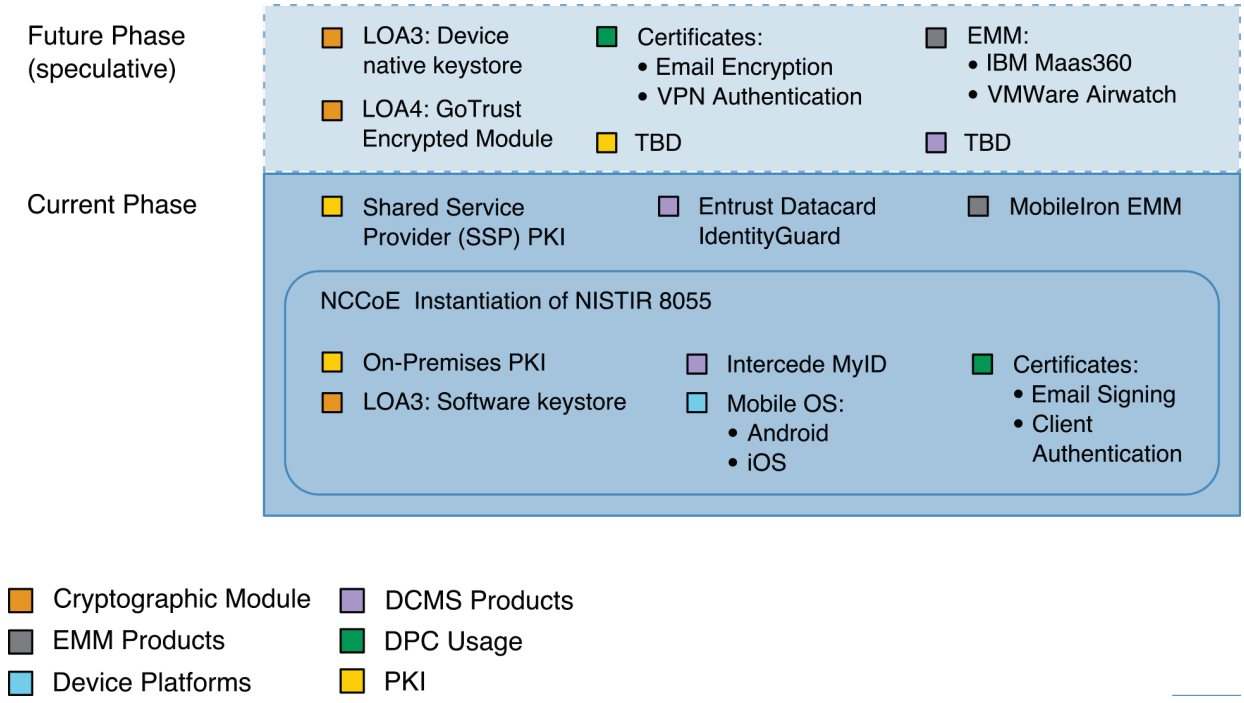
To develop our example solution, the Derived PIV Credential project team followed an approach common to projects across the NCCoE. First, a project description was published on the website followed by a Federal Register Notice (FRN) [11]. In response to the FRN, several vendors expressed interest in helping NCCoE build example solutions. Technology companies with relevant products then signed a CRADA with the NCCoE for the project. Following the signing of CRADAs, the NCCoE sponsored a kick-off meeting for the project team, collaborating vendors, and other members of the Derived PIV Credential Community of Interest (COI).

During the kick-off, we gathered requirements and lessons learned from project stakeholders; this helped establish objectives for our example solution. In addition to input from collaborators and COI members, we performed a risk assessment during the architecture design phase and on our final DPC example solution. This assessment thus includes both risks to the functions of the system (e.g., DPC

issuance or revocation) and to its parts, such as the mobile devices into which a Derived PIV Credential would be provisioned.

The Derived PIV Credential project is using a phased approach that takes direct advantage of previous work by NIST in this area. NISTIR 8055 [9], *Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research*, presents a scheme for provisioning a Derived PIV Credential to an organization-managed mobile device. This project applied the technologies used in that work as a starting point, then sought to expand on its Derived PIV Credential ecosystem to provide greater diversity across mobile device models and platforms, credential storage implementations at Level of Assurance (LOA) 3, Derived PIV Credential Management Systems (DCMS), and EMM products as pictured in Figure 3-1.

Figure 3-1 Project Phased Approach



3.1 Audience

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

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

3.2 Scope

The scope of NIST SP 800-157 *Guidelines for Derived PIV Credentials* [6] is to provide PIV-enabled authentication services on the mobile device to authenticate the credential holder to remote systems. The current phase of the Derived PIV Credentials project and this practice guide focus only on a portion of the special publication – the lifecycle activities. Specifically, we evaluated the example solution against the requirements related to initial issuance, maintenance, and termination of Derived PIV Credentials.

For the proof-of-concept research documented in NISTIR 8055 [9], NIST used a single vendor CMS product to demonstrate DPC lifecycle management. The device platforms documented in NISTIR 8055 [9] comprised Windows, Android, and iOS. The CMS vendor's software key store implementation for Android and iOS devices was used for the research effort as well as the Microsoft's Virtual Smart Card (VSC) implementation for the Windows platform. For the first phase of the NCCoE project, we demonstrated an additional CMS product to demonstrate DPC lifecycle management.

As of this writing, only DPC authentication certificates that can be issued at LOA 3 are addressed. To support LOA 4, we would need to address additional in-person lifecycle requirements that were deemed out of scope for the current phase of the project. These may be addressed in subsequent phases as described in Section 6, Future Build Considerations.

This project integrates an EMM component into this documented example solution. EMMs are essential to securing mobile endpoints; however, this project defers to the Mobile Device Security for Enterprise project at the NCCoE for specific security control recommendations. Section 3.4, Risk Assessment, includes threats specific to Derived PIV Credentials issued to tokens contained within mobile devices.

PIV Card lifecycle management is not within the scope of the project, which means background checks or vetting PIV Card applicant identities were not performed. However, tests were conducted on PIV Card credentials to initiate the issuance of Derived PIV Credentials and to validate that a Derived PIV Credential Management System (DCMS) performs all required checks of a DPC subscriber's PIV Card and associated PIV authentication certificate per NIST SP 800-157.

3.3 Assumptions

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

- If you are an implementer who works for a U.S. federal agency, then you will be complying with FIPS 201-2 *Personal Identity Verification of Federal Employees and Contractors*. [2]
- The mobile devices in your Derived PIV Credential solution are organization-provided [12], and your organization centrally manages them with security policies and controls.

3.3.1 Modularity

Specific assumptions on modularity are based on one of the NCCoE core operating tenets: that organizations already have the PIV Card issuance solution and the associated PKI services in place. We make no further assumptions regarding how the solutions have been deployed; they may combine on-premises operations, cloud deployments, and managed services. Instead, we intend this guide to offer options for adding the DPC lifecycle management solution into a diverse set of existing deployments.

3.3.2 Security

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

3.3.3 Existing Infrastructure

This guide may help you in designing an entirely new infrastructure. However, it is geared toward those with an established infrastructure, as that represents the largest portion of readers. Federal agencies and other organizations that are mature enough to implement Derived PIV Credentials are likely to have some combination of the capabilities described in this example solution. Before applying any measures addressed in this practice guide, we recommend that you review and test them for applicability to your existing environment. No two organizations are the same and the impact of applying security controls will differ.

3.4 Risk Assessment

NIST SP 800-30, Risk Management Guide for Information Technology Systems states, "Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level." The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, material available to the public. The RMF guidelines as a whole proved invaluable in giving a baseline to assess risks, from which we the project was developed, the security characteristics of the build, and this guide.

This section discusses risk from two perspectives. First, we review the risk mitigation that a Derived PIV Credential 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 [12] of confidentiality, integrity, and availability need to be maintained on the mobile endpoint. The threats to weaker one factor authentication mechanisms, such as passwords, are well documented by industry [13] and government [8]. Further, the 2017 DHS Study on Mobile Device Security [14] found failure to use strong multi-factor 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 Management Act 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 you to review NIST SP 800-63-3 for guidance related to digital identity risk; your organizations can apply the guidance while executing all relevant Cybersecurity Framework and RMF lifecycle phases [7].

Federal cybersecurity risk management has taken on increased emphasis with the release of the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [15]. In this memo, the President directs each agency head to use NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, or any successor document, to manage the agency's cybersecurity risk.

411 In response, NIST released NISTIR 8170, *Cybersecurity Framework Implementation Guidance for Federal*
412 *Agencies* [16]. The NISTIR guides agencies on how the Cybersecurity Framework can be used to augment
413 current NIST security and privacy risk management publications. We recommend that organizations,
414 especially federal agencies that implement a DCMS, follow the recommendations presented in NISTIR
415 8170.

416 Your organization may benefit from examples in NISTIR 8170. For instance, the framework's
417 Example 1—*Integrate Enterprise and Cybersecurity Risk Management*—recommends using five
418 cybersecurity functions (identify, protect, detect, respond, and recover) to organize cybersecurity risk
419 management activities at the highest level. Section 3.4.4 presents a list of possible functions that a DPC
420 implementation can address. We recommend that you use this information when communicating risk
421 throughout your organization.

422 ### 3.4.1 Threats

423 NIST Special Publication 800-63 provides a general identity framework by incorporating authenticators,
424 credentials, and assertions into a digital system [7]. Included in the publication are threat analyses in the
425 areas of authenticator and lifecycle threats. This section uses these threats as a basis for a discussion of
426 threats applicable to a Derived PIV Credentials system.

427 **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 certificates are not issued from untrusted CA or user does not possess private key corresponding to the certificate).
	Fraudulent use of another's identity	An applicant attempts to use a PIV card associated with a different individual to obtain a DPC.	Two-factor 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

Activity	Threat/ Attack	Example	Applicability to DPC
			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 7-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 attackers choosing.	A DPC subscriber's mobile device could contain malware that intercepts the PIN/password. 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 credentials for that subscriber.	An attacker could steal a one-time use code through a man-in-the-middle attack or other means. Use an EMM to authenticate the device requesting the DPC. Further, ensure an appropriate channel is used to distribute the onetime use code, and

Activity	Threat/ Attack	Example	Applicability to DPC
			ensure the onetime use code is resistant to attempts by an attacker to brute force attack (or use other means) to discover the value of the onetime code.
	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.

428 **Table 3-2 Authenticator Threats**

Authenticator Threats/ Attacks	Examples	Applicability to DPC
Theft	A hardware cryptographic device is stolen.	An external USB or microSD can be readily stolen. Two-factor authentication prevents unauthorized use of the private key.
	A cell phone is stolen.	A mobile device that stores the DPC in software or 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, two-factor authentication prevents unauthorized use of the private key.

Authenticator Threats/ Attacks	Examples	Applicability to DPC
Duplication	Software PKI authenticator (private key) 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 a mitigation.
Eavesdropping	Memorized secrets are obtained by watching keyboard entry.	An attacker could observe a PIN/password that protects the cryptographic token through shoulder surfing. Educate users to be mindful of surroundings when entering PIN/password. Note: This attack compromises only one factor of the two-factor 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 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 subject to offline cracking. Use PIN/password throttling, device encryption, and malware detection mechanisms as a 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 and/or PIN usage timeout/limits and adopt other countermeasures described in NIST SP 800-63-3b and PHY-5 [8].

Authenticator Threats/ Attacks	Examples	Applicability to DPC
	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 [8].
Endpoint compromise	A cryptographic authenticator connected to the endpoint is used to authenticate remote attackers (i.e., Malicious code on the endpoint proxies 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. Two-factor 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 proxies 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 subject to offline cracking. Use sandboxing, device encryption, and malware detection mechanisms as a mitigation.

3.4.1.1 Other Threats

Using mobile devices like those featured in our example solution are subject to the broader set of mobile ecosystem threats. From NISTIR 8144 [19]:

> 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 this practice guide in whole or part to consult NIST Mobile Threat Catalogue when assessing relevant threats to your own organization.

Because infrastructure threats are addressed by normal computer security controls (e.g., separation of duties, record keeping, independent audits), they are outside the scope of this practice guide. See NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, for appropriate security controls.

3.4.2 Vulnerabilities

Vulnerabilities are commonly associated with mobile applications, mobile operating systems, and network applications that are employed in the storage and use of a mobile credential. However, vulnerabilities can be exploited at all levels in the information stack. For up-to-date information regarding vulnerabilities, this guide recommends that security professionals leverage the National Vulnerability Database (NVD) [17]. The NVD is the U.S. government repository of standards-based vulnerability management data.

3.4.2.1 Mobile Device Vulnerabilities

Vulnerabilities discovered within mobile applications and operating systems are important to any deployment of Derived PIV Credentials. The DPC issuer must ensure strong protections on the use of the credential via a PIN or passphrase [6, Sec. 3], while also making sure that other applications on the device cannot access the credential. Sensitive cryptographic material can be stored in software at LOA-3, leaving the mobile device open to exploits that attack vulnerable code. To thwart these type of attacks, it is common for mobile applications to be sandboxed in some manner to prevent unexpected and unwanted interaction between the system, its applications, and those applications' respective data (including user data) [11]. However, a search of the National Vulnerability Database yields examples of software vulnerabilities [18] that might allow exploits to *break* sandboxing protections. A full discussion on these topics, including mitigations, can be found in NISTIR 8144 *Assessing Threats to Mobile Devices & Infrastructure* [19] and Special Publication 800-163 *Vetting the Security of Mobile Applications* [20].

Vulnerabilities are also introduced by downloading non-approved applications. We recommend that only vetted and approved applications be downloaded. NIST's AppVet is an example application vetting platform.

3.4.2.2 Network Vulnerabilities

Considering that Derived PIV Credential enrollment may happen remotely [6], issuing organizations will want to mitigate network vulnerabilities before deploying a DPC solution for your organization. For example, a DPC applicant may be required to enter a one-time password into the DPC mobile provisioning app to complete enrollment as described in NIST SP 800-157 (Section C.1, Appendix C). Your organization will want to maintain confidentiality and authenticity of the one-time password (OTP) as it traverses potentially untrustworthy networks.

This guide suggests two resources to assist network vulnerability analyses as input to a risk assessment. The Common Vulnerability Enumeration (CVE) database [21] lists more than 85,000 vulnerabilities that can affect web servers, Structured Query Language (SQL) servers, Domain Name System (DNS), firewalls, routers, and other network components. These vulnerabilities include denial of service, code execution, overflow, cross-site scripting, directory traversal, process bypass, unauthorized gaining of information, SQL injection, file inclusion, memory corruption, cross-site request forgery, and HTTP response splitting.

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

3.4.3 Risk

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

The NIST SP 800-63-3 series of documents retired the Level of Assurance concept and in its place introduced Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), and Federation Assurance Level components to assist in risk management decisions. At the time of this writing, NIST SP 800-157 refers to the older LOA for tokens/authenticators. However, we have mapped the cryptographic tokens/authenticators used in this project to AAL. IAL is not applicable in the context of DPC because deriving identity is accomplished by proving possession and successful authentication of an authenticator (i.e., The PIV Card) that is already bound to the original, proofed digital identity [7].

As an implementer of DPC, you should refer to the NIST SP 800-63-3 discussion of digital identity risk management and the corresponding risk assessment guidelines that supplement the Risk Management

Framework. Specifically, this section provides guidelines on the selection of the DPC vendor AAL based on risk.

Table 3-3 AAL Vendor Mappings

NIST SP 800-157 LOA	NIST SP 800-63-3 AAL	Cryptographic Token FIPS 140-2 Validation	Cryptographic Token Type	Derived PIV Authentication Certificate Policy	Enrollment Method
LOA-3	AAL-2	Level 1	MobileIron Container Software Token	Id-fpki-common-pivAuth-derived	Remote

3.4.4 Security Control Map

Your organization may benefit from examples in NISTIR 8170 [16]. For instance, the framework's Example 1—*Integrate Enterprise and Cybersecurity Risk Management*—recommends using five cybersecurity functions (identify, protect, detect, respond, and recover) to organize cybersecurity risk management activities at the highest level. Table 3-4 presents a list of possible functions that a DPC implementation can address. In addition, for each CSF subcategory a mapping was made to the NIST National Initiative for Cybersecurity Education (NICE) Framework Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [22] to show what types of work roles are needed to implement and maintain a DPC solution. We recommend that you use this information when communicating risk throughout your organization.

Table 3-4 Security Control Mappings

Cybersecurity Framework Function	Cybersecurity Framework Category	Cybersecurity Framework Subcategory	NIST SP 800-53 rev4	NIST SP 800-181 Work Role
Protect	Access Control	**PR.AC-1**: Identities and credentials are managed for authorized devices and users.	IA-2, IA-4, IA-5, AC-19, SC-12, SC-13, SC-17	Software Developer SP-DEV-001), Product Support Manager (OV-PMA-003)
Protect	Access Control	**PR.AC-3**: Remote access is managed.	AC-7, AC-19	Information Systems Security Developer (SP-SYS-001), System Administrator (OM-ADM-001)
Protect	Data Security	**PR.DS-2:** Data-in-transit is protected.	SC-8, SC-13, SC-17	Data Analyst (OM-DTA-002), Cyber Defense Analyst (PR-CDA-001)

Cybersecurity Framework Function	Cybersecurity Framework Category	Cybersecurity Framework Subcategory	NIST SP 800-53 rev4	NIST SP 800-181 Work Role
Protect	Data Security	**PR.DS-4:** Protections against data leaks are implemented.	AC-2	Research and Development Specialist (SP-TRD-001), Cyber Defense Analyst (PR-CDA-001)
Protect	Information Protection	**PR.IP-3:** Configuration change control processes are in place.	CM-3	Software Developer (SP-DEV-001), Systems Security Analyst (OM-ANA-001)

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

4 Architecture

In this section, we first identify and define the key components used in our DPC example solution followed by descriptions of how those components, as implemented by our partner technologies (see Section 4.2, Technologies), were integrated to produce the final architecture (Section 4.3). Note that this architecture was based on time and product capability constraints and is focused on supporting DPC lifecycle activities. In future phases of the project, architectures may be expanded to include a managed PIV Card component, broader application of DPCs to mobile apps, and other enhancements. Refer to Section 6 for further details.

4.1 Architecture Components

4.1.1 Credential Management System

A Credential Management System is central to executing the lifecycle operations, typically issuance, maintenance, and termination of authentication credentials. In our architecture, we depict two types of CMSs – PIV and Derived PIV. The PIV Credential Management System is responsible for enforcing lifecycle activities in accordance with FIPS 201-2 and the Derived PIV Credential Management System enforces the lifecycle activities in accordance with NIST SP 800-157. Readers will need to be familiar with the PIV standard [2] and associated guidelines before implementing a Derived PIV Credential solution.

4.1.2 PKI Managed Service

A second component, the PKI, issues, maintains, and revokes digital certificates issued to PIV Cards and Derived PIV Credentials. PKI components are also offered as managed services. PIV CMS service providers partner with PKI service providers for issuing the digital certificates that are provisioned to the PIV Card and DPCs.

4.1.3 Enterprise Mobility Management

An EMM is typically used by organizations to provide security services commonly needed for security management of mobile devices such as remote wiping of a device, device encryption enforcement, and application restrictions. An EMM within the DPC context enhances application white listing security 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. 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 lifecycle tasks of the DPC. For instance, if a mobile device is lost by the DPC subscriber, an EMM administrator can destroy the software container that stores the DPC.

4.2 Technologies

We built the example solution using products from vendors who signed CRADAs with NCCoE for the DPC project. Products for the supporting infrastructure components are from vendors who are National Cybersecurity Excellence Partnership (NCEP) 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 your own requirements and integrate well with your existing IT system infrastructure.

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

4.2.1 Entrust Datacard

Entrust Datacard is a federal government provider that offers solutions for PKI and for PIV Card lifecycle management activities. 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 lifecycle 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, 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.

4.2.2 MobileIron

Many of the vendors who provide products and solutions to manage mobile devices enter into partnerships with identity and credentials management product vendors to deliver integrated solutions. MobileIron, one such vendor, is partnering with Entrust Datacard and offering an integrated solution for the lifecycle management of DPCs 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 backend IT platforms and can be deployed on-premises or in the cloud.

MobileIron Sentry functions as an in-line gateway to manage and secure the traffic between mobile devices and backend 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.

Table 4-1 lists all the technologies that we incorporated into the example solution and maps the generic application term (component) to the specific product we used, and the Cybersecurity Framework subcategories the product addresses. Note: some of our components are marked as not applicable in the version column. This is due to the use of SaaS [24] cloud services.

Table 4-1 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

Component	Product	Version	Function	Cybersecurity Framework Subcategories
Derived PIV Credential Management System	Entrust Datacard IdentityGuard	Not applicable	Entity that implements Derived PIV lifecycle 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 lifecycle 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 [12].	PR.AC-1, PR.AC-3
Cryptographic Token	Entrust PIV-D	1.3.0.4	Software component that stores the Derived PIV Authentication private key.	PR.DS-2, PR.DS-5

4.2.3 Mobile Devices

Table 4-2 lists the devices used to complete our example solution. Operating system (OS) versions are current as of the writing of this document. Readers should consult vendor documentation for the latest compatibility requirements.

Table 4-2 Mobile Devices

Manufacturer	Model	OS/Version
Apple	iPhone	iOS 10.3.2
Apple	iPad Mini	iOS 10.2.1
Samsung	Galaxy S6	Android 6.0.1

4.3 Managed Architecture with EMM Integration

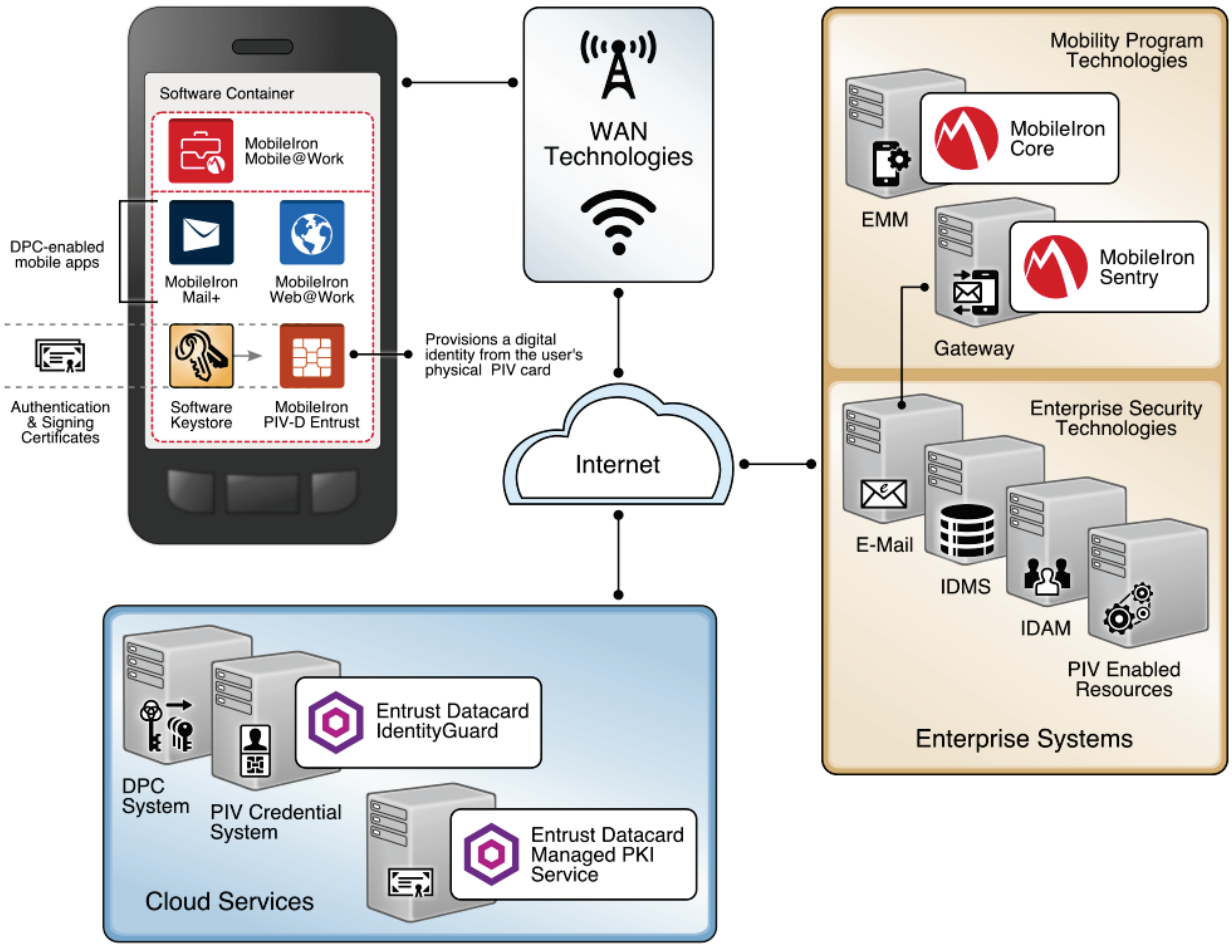
Many federal agencies have opted to use a managed shared solution for issuing PIV Cards for their employees rather than deploy and operate their own PKI infrastructure. The General Services Administration's (GSA) Managed Service Office established the USAccess program to offer federal agencies a managed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

With the assumption that many agencies use a managed service for their PIV Card issuance and a shared service provider for the PKI services, we took into consideration a few of the different deployment architectures while planning our example solution. Managing mobile devices with EMM products is an integral part of the mobile ecosystem for most organizations. Therefore, we considered architectures for DPC provisioning solutions both independent of and integrated with an EMM product.

Figure 4-1 depicts the final architecture for this example solution. In this type of deployment architecture, an organization chose to use cloud services to manage the PIV and DPC lifecycle activities. It also introduces an EMM into the workflow, recognizing the need for organizations to apply a consistent set of security policies on the device. In this scenario, the same vendor operates the PIV and DPC management services to simplify the lifecycle linkage requirements between the DPC and PIV so that integration efforts across two solutions are not necessary. This simplification also allows for the recovery of the PIV user's key management key onto the mobile device with relatively little difficulty, again, because of the single vendor solution. This type of scenario, however, may not be sufficient if an organization prefers a more modular architecture.

The backend EMM components, MobileIron Core and MobileIron Sentry, were deployed on-premises in the Demilitarized Zone of a simulated enterprise network. MobileIron Core allows administration of users and devices by applying policies and configurations to them based on their assigned labels. MobileIron Sentry provides a VPN endpoint, which creates an authenticated protected channel between managed devices and on-premises resources, such as internal email. Sentry was included in this architecture to explore DPC usage scenarios as discussed in Section 6, Future Build Considerations. However, as Sentry is not required for any lifecycle management activities of DPCs, it is not further documented by this guide. The enterprise network also includes an Active Directory (AD) and Exchange server. The instance of AD was used to store the identities of the test users in this scenario. The EMM used AD as its trusted repository of authorized mobile device owners.

625 **Figure 4-1 PIV and DPC Cloud Service Lifecycle Management with EMM Integration**



626

627 # 5 Security Characteristics Analysis

628 The purpose of the security characteristic evaluation is to understand the extent to which the project
629 meets its objective of demonstrating the lifecycle of Derived PIV Credentials requirements specified in
630 NIST SP 800-157. In addition, it seeks to understand the security benefits and drawbacks of the example
631 solution. Readers may also find Section 3.4, Risk Assessment, helpful when evaluating DPC security
632 characteristics for your own organization.

5.1 Assumptions and Limitations

The security characteristic evaluation has the following limitations:

- It is neither a comprehensive test of all security components nor a red team exercise.
- It cannot identify all weaknesses.
- It does not include lab infrastructure. It assumes that devices and infrastructure are hardened.

5.2 Build Testing

This project uses Table 5: Requirements Definition and Implementation Mappings from NISTIR 8055 [9] as a basis for testing the example solution. Using the table as a foundation (see Appendix C), we created a test plan that specifies test cases with traceability to DPC requirements. We collected artifacts from each test case execution, such as screen captures and network packet traces, and documented the results. In cases where a requirement could not be tested from our lab environment, we collaborated with our build partners to document how a requirement could be fulfilled in a production environment.

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

5.2.1 Example Solution Initial Issuance

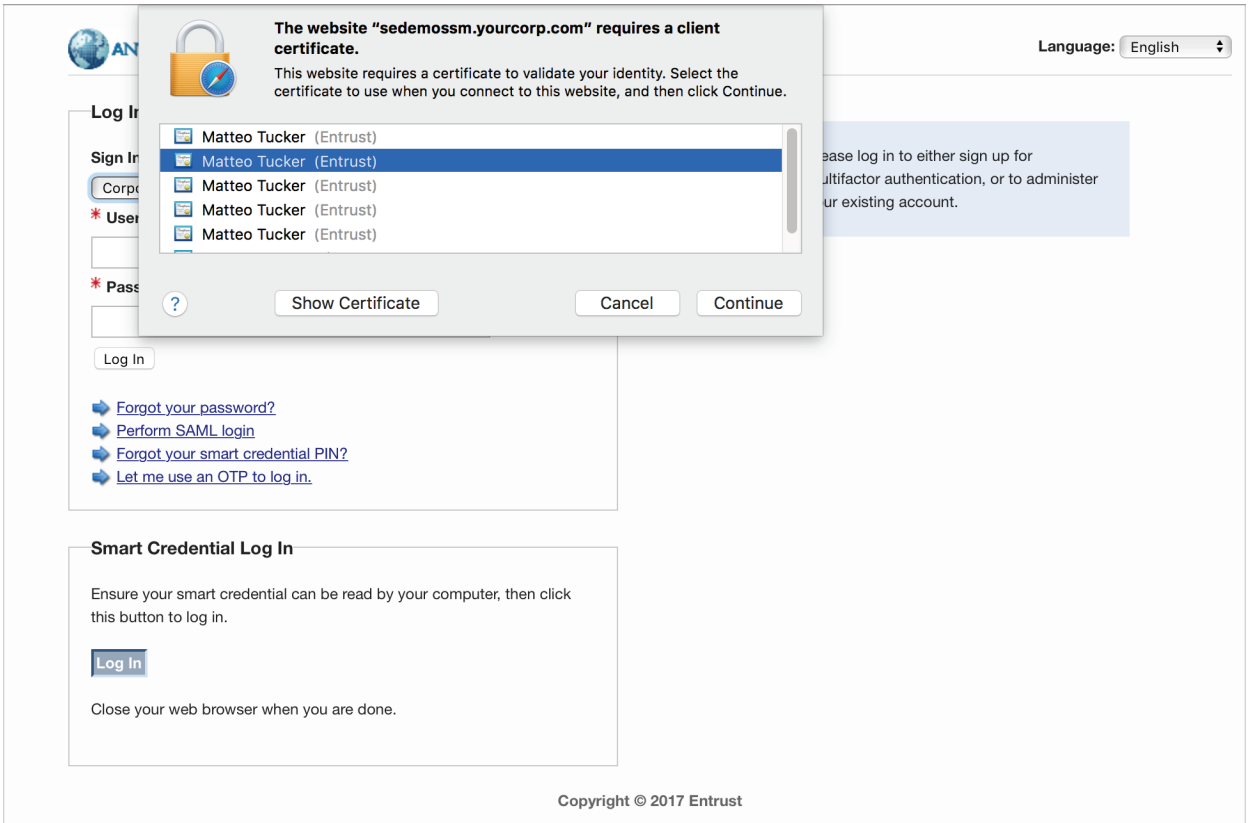
With our Entrust Datacard example solution, the mobile device connects to the IdentityGuard system, and the IdentityGuard connects to the Certificate Authority (CA), thereby handling the delivery of the public certificate to the mobile device, which follows the same process for issuing a PIV Card. In this case, the Derived PIV Credential key pairs are generated on the mobile device and the user's public key certificate is securely passed to the CA for certificate issuance by means of IdentityGuard.

To test this architecture, Entrust Datacard gave us access to a development instance of their IdentityGuard service and populated it with identities of users who were issued test PIV Cards. These users were also granted pre-approval to request a DPC. We observed that the prescribed initial issuance workflow, summarized below, adhered to the requirements in NIST SP 800-157 [6].

660 As a prerequisite to issuance we added our test DPC applicant's user account to an Active Directory
661 group associated with users authorized to use DPC. Users of this group are managed by a MobileIron
662 AppConnect policy configured to achieve compliance with NIST SP 800-157. The policy enforces multiple
663 issuance requirements, such as the need for a DPC applicant to create a 6- to 8-digit password to protect
664 access to the private key associated with the DPC's PIV authentication certificate. Additionally, the test
665 applicant has a mobile device enrolled into management by MobileIron Core. Two MobileIron apps are
666 employed: PIV-D Entrust, which is used in the DPC issuance workflow, and Mobile@Work, which
667 maintains the target software token where the DPC will be stored.

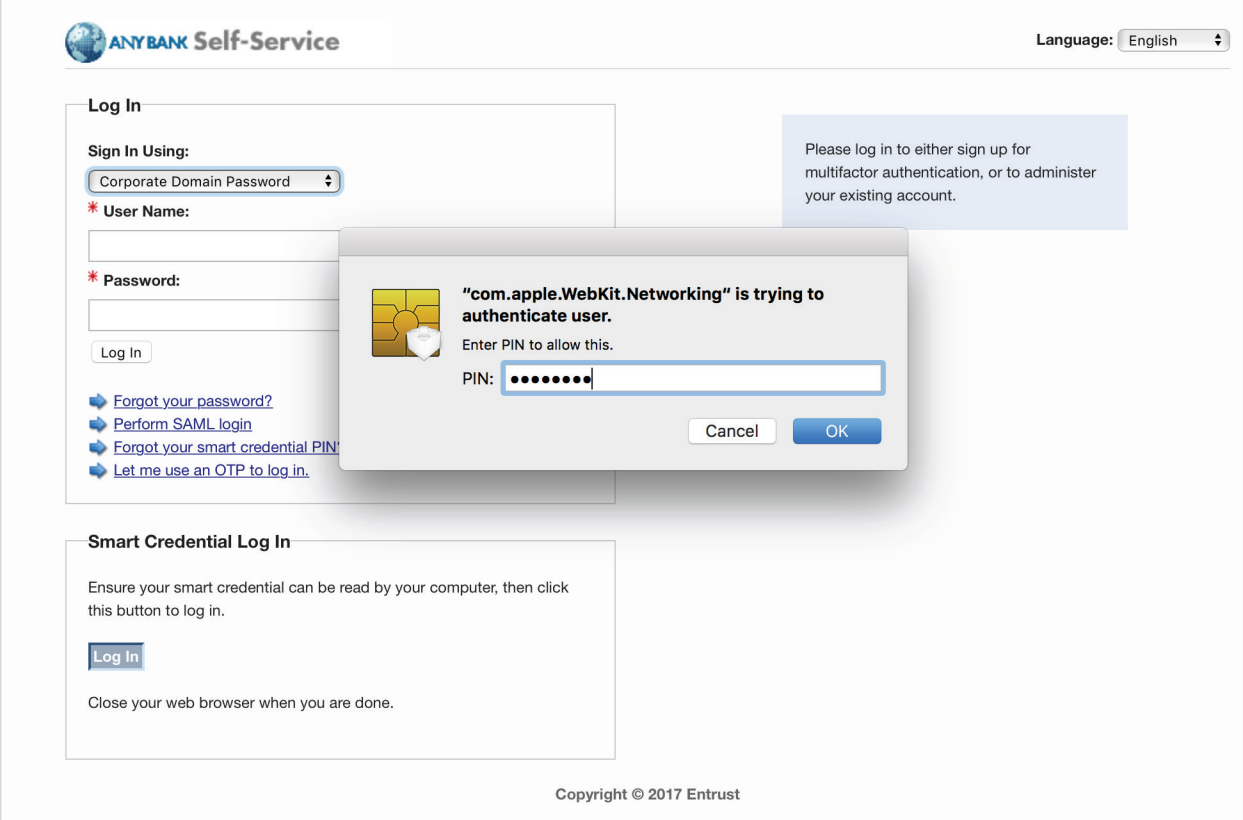
668 Issuance begins with the test DPC applicant (Matteo) authenticating to the Entrust IdentityGuard self-
669 service portal via PKI-AUTH two-factor authentication using a computer and the applicant's valid PIV
670 Card. The applicant then makes appropriate selections within the portal to request issuance of a new
671 DPC.

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



673

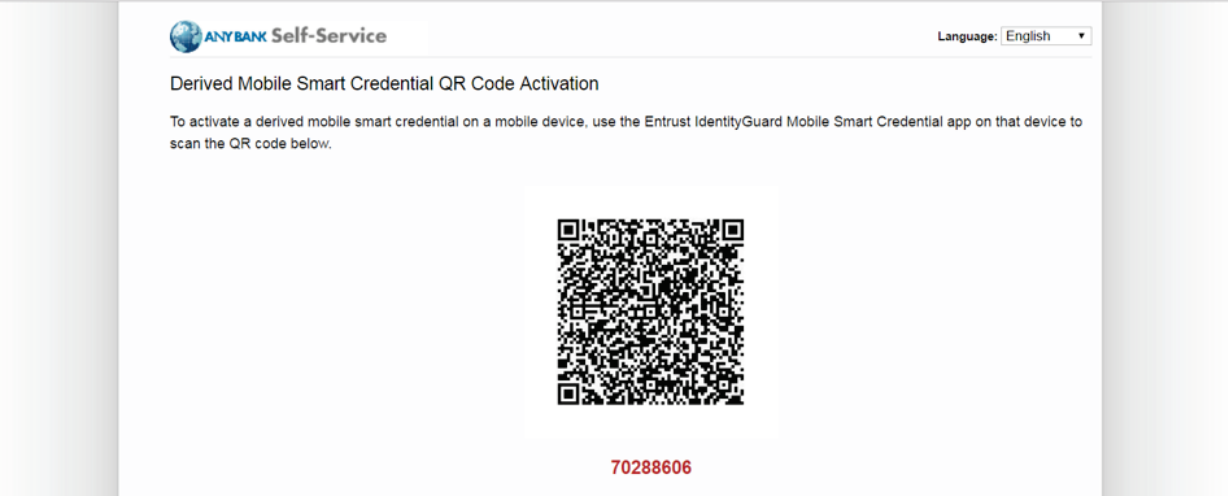
674 **Figure 5-2 Password-Based Subscriber Authentication via PIN**



675

676 Entrust IdentityGuard presents a QR code (see Figure 5-3) containing the IdentityGuard Uniform
677 Resource Locator(URL) and a numeric OTP code. This time-limited shared secret links Matteo's (the DPC
678 applicant) session from a computer to the Entrust IdentityGuard self-service portal to the subsequent
679 session between his target mobile device and Entrust IdentityGuard.

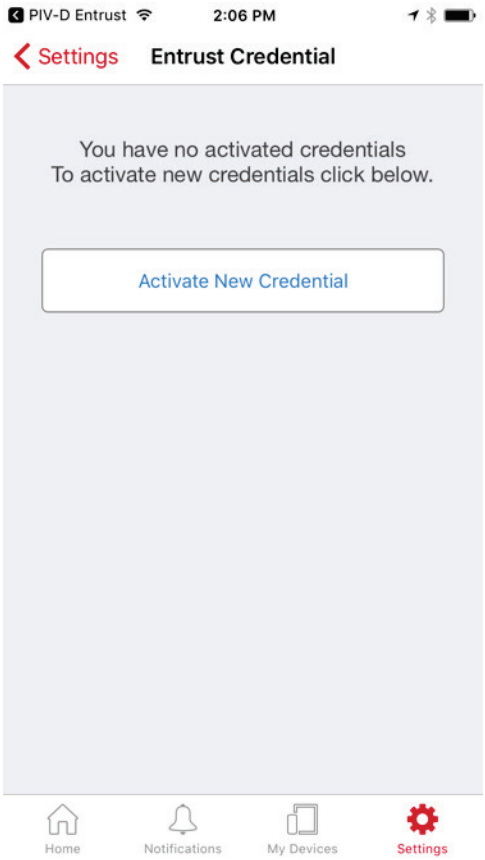
680 **Figure 5-3 Entrust IdentityGuard DPC Activation Codes**



681

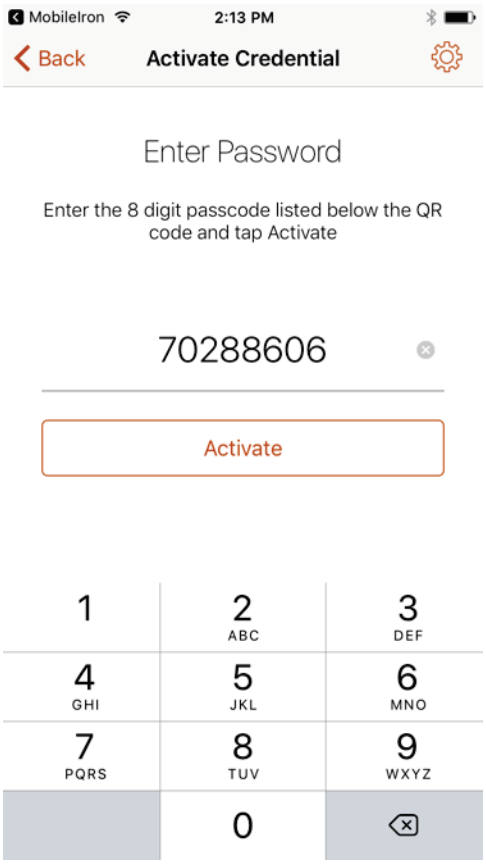
682 The applicant launches the MobileIron PIV-D Entrust app on the mobile device and uses it to scan the QR
683 code and enter the OTP. See Figure 5-4 and Figure 5-5.

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



685

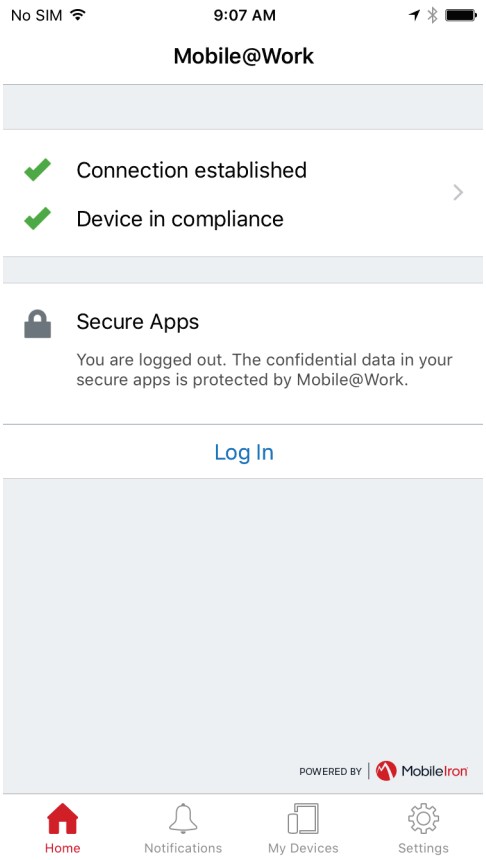
686 **Figure 5-5 Entrust DPC Activation**



687

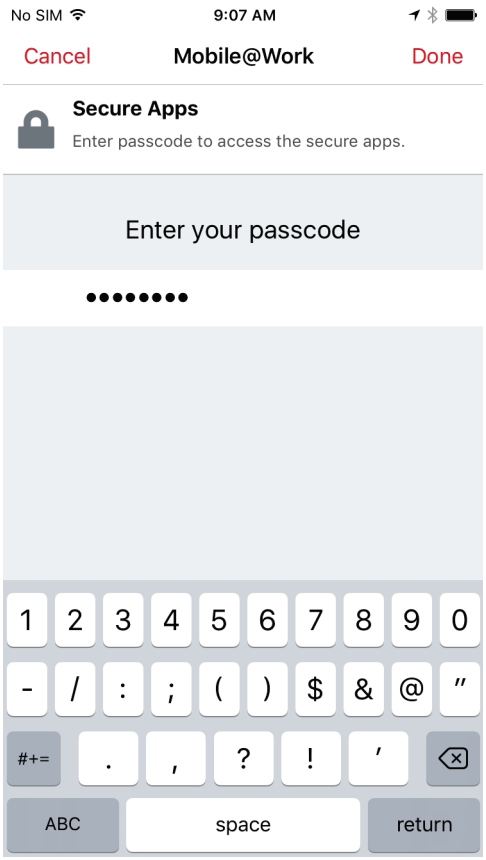
688 The app then creates a TLS 1.2-secured session with Entrust IdentityGuard and authenticates with the
689 OTP. Once authenticated, the app generates asymmetric key pairs for derived PIV authentication and
690 digital signing certificates and transmits the certificate requests to Entrust IdentityGuard. The
691 IdentityGuard service verifies that the requested certificates match information on file for the PIV
692 subscriber for whom the OTP was generated (i.e., Matteo). Once verified, it forwards the certificate
693 requests to the Entrust CA, receives the DPC certificates, then relays them to the MobileIron PIV-D
694 Entrust app, where they are stored in the software token. The DPC subscriber must authenticate to the
695 MobileIron PIV-D Entrust container using the created password before DPC certificates or their
696 associated private keys can be used by any application integrated with MobileIron. See Figure 5-6 and
697 Figure 5-7.

698 **Figure 5-6 PIV-D App**



699

700 **Figure 5-7 PIV-D Passcode Entry**



701

702 5.2.2 Example Solution Maintenance

703 Maintenance activities for a DPC issued within this architecture are managed in two ways. Operations
704 that require generating a new PIV Authentication certificate (certificate modification or rekey) require
705 the DPC subscriber to repeat the initial issuance process as described in Section 5.2.1, Example Solution
706 Initial Issuance.

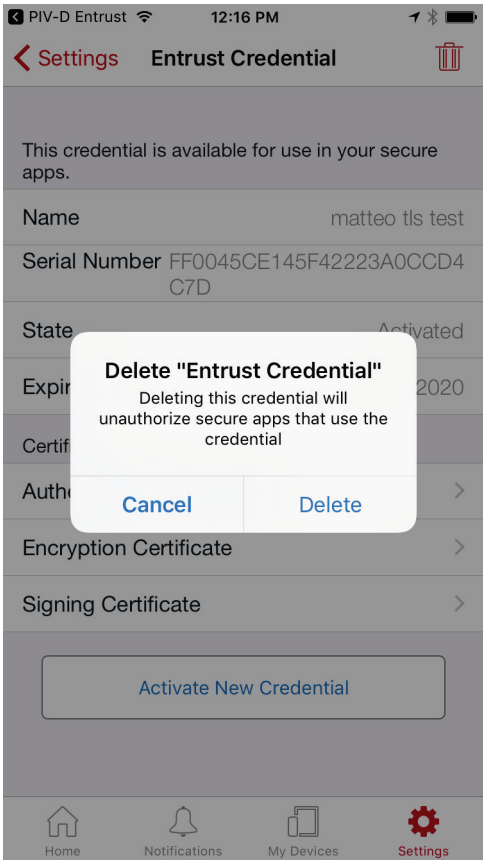
707 Linkage requirements between the status of the subscriber's PIV Card and DPC are covered by both the
708 CA and IDMS being under the control of Entrust Datacard. These systems exchange Identity
709 Management System data and any necessary changes to the status of the subscriber's DPC will occur
710 automatically.

711 5.2.3 Example Solution Termination

712 Should the mobile device with a software token be lost or compromised, a DPC sponsor-initiated
713 workflow will specifically destroy the DPC by triggering the Retire Device operation available through the
714 MobileIron administrative console. This process removes the MobileIron and all Web@Work apps and

cryptographically wipes the MobileIron PIV-D Entrust software token containing the DPC. Triggering a remote wipe of all data on the device will also achieve this result. Further, the DPC authentication certificate can be directly revoked from the Entrust Identity Guard interface.

Figure 5-8 PIV-D App Termination



5.2.4 DPC Certificate Issuance

Public Key Infrastructure management instructions between the Entrust IdentityGuard service and the Entrust Datacard Managed CA use a combination of the X.509 Public Key Cryptography Standards - Certificate Management Protocol (PKIX-CMP) and the XML Administration Protocol (XAP). PKIX-CMP [26] provides online interactions between PKI components, including an exchange between a CA and a client system–in this case the Entrust IdentityGuard service. PKIX-CMP is defined as a standard by the Internet Engineering Task Force (IETF) in Request for Comments 4210. The IETF standardizes many of the protocols that underpin network-based communication. The XAP protocol was developed by Entrust Datacard and is used for administration tasks within the Entrust Datacard Managed CA.

The Entrust IdentityGuard service uses an XAP credential to securely communicate with the XAP subsystem on the Entrust Datacard Managed CA. The Entrust IdentityGuard service uses XAP to obtain an activation code, which is then used to create a PKIX-CMP General Message. The DPC certificate request is then forwarded to the Entrust Datacard Managed CA in the Public Key Cryptography Standards #10 format over PKIX-CMP. The Entrust Datacard Managed CA returns the signed DPC certificate to the Entrust IdentityGuard service.

5.3 Scenarios and Findings

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

Our example solution primarily focuses on the *Protect* function areas of the Cybersecurity Framework. We discuss the associated subcategories in the following subsections.

5.3.1 PR.AC-1: Identities and Credentials Are Managed for Authorized Devices and Users

To address the *Protect* function of the Cybersecurity Framework, users of the Derived PIV Credential Management System are managed through group and role membership. In our example solution 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 our example solution, we worked with Entrust Datacard engineers to populate sample PIV information within IdentityGuard. These sample PIV user data linked to local user data in an Active Directory repository that was also leveraged by the MobileIron Core user management system.

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* [27] as a resource.

5.3.2 PR.AC-3: Remote Access is Managed

To address the Cybersecurity Framework *Protect* function, the organizationally owned mobile devices of DPC subscribers are, or should be, managed through an EMM. While we used a basic set of security policies in our project, such as requiring device encryption before DPC issuance, holistic mobile device

762 security is out of scope. Please refer to the Mobile Device Security for Enterprises project at the NCCoE
763 for guidance that will enable you to tailor the work in this practice guide your organization's needs.

764 5.3.3 PR.DS-2: Data-in-Transit Is Protected

765 To address the Cybersecurity Framework *Protect* function, we used the DPC to protect data-in-transit by
766 ensuring the integrity and confidentiality through client/server mutually authenticated internet
767 protocols. To test integrity and confidentiality we set up a PIV-enabled example website through which
768 we emulated a remote service offered to federal employees. The Derived PIV authentication certificate
769 was then used in a client-authenticated session, during which the private key was used to digitally sign a
770 portion of the handshake message. The resulting session was protected.

771 5.3.4 PR.DS-5: Protections Against Data Leaks Are Implemented

772 To address the *Protect* function, we used the client/server mutually authenticated internet protocols in
773 the previous scenario to also identify the source party (i.e. the DPC subscriber) when remote systems
774 are accessed. Because client authentication is enforced by the relying application, the server in our
775 example solution validates the X.509 public certificate and its private key associated with the DPC. This
776 step, combined with the PIN requirement to unlock the cryptographic token that stores the DPC,
777 provides strong two-factor authentication of the subscriber and reduces the likelihood of data leaks to
778 unauthorized parties.

779 5.3.5 PR.IP-3: Configuration Change Control Processes Are in Place

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

784 6 Future Build Considerations

785 Mobile technologies such as Derived PIV Credentials are constantly evolving. This project seeks to keep
786 reasonable pace with the changing mobile landscape while sustaining an attainable scope. As such, we
787 will consider additional challenges for future projects, including:

788 - **Key Management Key Recovery** – Mobile users should be able to recover key management keys
789 from escrow. Unlike a signature key, the same key management key that is stored on the PIV
790 Card is necessary to decrypt encrypted email stored on the device, for example. While this
791 project did not have key management key recovery as a requirement, we observed this feature
792 in practice while testing the Entrust Datacard cloud services.
793 - **Level of Assurance** – This project specifically targeted LOA-3/AAL-2 cryptographic tokens as an
794 initial requirement due to its broad applicability. However, specific use cases where LOA-4/AAL-
795 3 cryptographic tokens are useful to implementers are likely too. Our anticipated project can

leverage *Go-Trust,* using their *Encryptor MicroSD* cryptographic modules in future architectures to demonstrate LOA-4/AAL-3 lifecycle functions. Also, the use of other cryptographic tokens such as Intel Authenticate can be demonstrated in future projects.

- **Shared Service Providers** – As mentioned previously in this practice guide, shared services are an integral part of modern organizations. A potential future requirement could be to integrate other PIV and Certificate Authority management services, such as GSA's managed USAccess service, to enable exchanging PIV credential lifecycle information with Derived PIV service providers. The NCCoE has begun to broker the discussion among USAccess and our collaborators so that USAccess can eventually support Derived PIV Credentials. Future output might include updates to the USAccess service Application Programming Interface and support within collaborator products and services.
- **Application Enablement** – To leverage DPC, an organization needs to enable applications on its mobile devices and from the relying party perspective. Mobile device application development is complicated by the various operating systems, cryptographic token options, and third-party software development kits provided by software containers. Further, modifying the source code of third-party closed mobile applications can be difficult or impossible. Relying parties face similar challenges with legacy systems that can be difficult to make ready for DPC. Future work might focus on adopting native embedded cryptographic tokens provided by hardware manufacturers and using federations for relying parties.

Appendix A List of Acronyms

AAL	Authenticator Assurance Level
AD	Active Directory
CA	Certificate Authority
CMS	Credential Management System
COI	Community of Interest
COTS	Commercial Off the Shelf
CRADA	Cooperative Research and Development Agreement
CSF	Cybersecurity Framework
CSP	Credential Service Provider
CVE	Common Vulnerability Enumeration
DCMS	Derived PIV Credential Management System
DNS	Domain Name System
DPC	Derived PIV Credential
EMM	Enterprise Mobility Management
FIPS	Federal Information Processing Standard
FRN	Federal Register Notice
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive-12
IAL	Identity Assurance Level
IETF	Internet Engineering Task Force
IT	Information Technology
LOA	Level of Assurance
NCCoE	The National Cybersecurity Center of Excellence
NCEP	National Cybersecurity Excellence Partnership
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal/Interagency Report
NVD	National Vulnerability Database
OS	Operating system
OTP	One-time Password
PIN	Personal Identification Numbers
PIV	Personal Identity Verification

PKI	Public Key Infrastructure
PKIX-CMP	Public Key Cryptography Standards - Certificate Management Protocol
RMF	Risk Management Framework
SaaS	Software as Service
SP	Special Publication
SQL	Structured Query Language
SSM	Self -Service Module
SSP	Shared Service Providers
TLS	Transport Layer Security
URL	Uniform Resource Locator
VSC	Virtual Smart Card
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 Derived PIV Credentials 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 card management system that manages the lifecycle 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 Credential	A trusted entity that issues and revokes public key certificates. 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.
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 OMB0404 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 manages 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 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	Office of Management and Budget 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, 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.
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 that 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 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 NISTIR 8055 [9] 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: SD card with cryptographic module: on-board 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: 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 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
	RC1.24	2.3.5.3.2.5	Embedded cryptographic tokens: Other keys stored in the same cryptographic module

Regulatory Requirement	Req. Number	Req. Section Number	Requirement Name
	RC1.25	2.3.5.4.6	Embedded cryptographic tokens: authentication mechanism implemented by hardware or software mechanism outside of 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 DPCs
RC3 - PKI	RC3.1	2.3.1.3	PKI-based DPCs 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 as a result 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
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

Regulatory Requirement	Req. Number	Req. Section Number	Requirement Name
	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 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 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	Re-key of and expired or compromised DPC
	RC4.11	2.3.3.4	Re-key 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
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

Regulatory Requirement	Req. Number	Req. Section Number	Requirement Name
	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 Backend 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 8/11/17].

[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. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf [accessed 8/11/17].

[3] *Cybersecurity Framework*, National Institute of Standards and Technology [Website], http://www.nist.gov/cyberframework/ [accessed 8/11/17].

[4] Joint Task Force Transformation Initiative, *Guide for Applying the Risk Management Framework to Federal Information Systems*. NIST Special Publication (SP) 800-37 Revision 1, National Institute of Standards and Technology, Gaithersburg, Md., February 2010, http://dx.doi.org/10.6028/NIST.SP.800-37r1.

[5] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organization*. NIST Special Publication (SP) 800-53 Rev 4, National Institute of Standards and Technology, Gaithersburg, Md., April 2013, http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[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, Md., December 2014, http://dx.doi.org/10.6028/NIST.SP.800-157.

[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, Md., June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

[8] *Mobile Threat Catalogue*, National Institute of Standards and Technology [Website], https://pages.nist.gov/mobile-threat-catalogue/ [accessed 8/11/17].

[9] *Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research.* NIST Internal Report (NISTIR) 8055, National Institutes of Standards and Technology, Gaithersburg, Md., January 2016, http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8055.pdf.

[10] *GSA Identity Services*, IDManagement.gov [Website], https://www.idmanagement.gov/trust-services/#gov-identity-credentials [accessed 8/11/17].

[11] National Cybersecurity Center of Excellence, *Derived Personal Identity Verification Credentials Building Block*, 80 FR 48823, https://www.federalregister.gov/documents/2015/08/14/2015-20039/national-cybersecurity-center-of-excellence-derived-personal-identity-verification-credentials [accessed 8/13/15].

[12] 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, Md., June 2013. http://dx.doi.org/10.6028/NIST.SP.800-124r1.

[13] Top 10 2014-I2 Insufficient Authentication/Authorization, OWASP [Website], https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization [accessed 8/11/17].

[14] 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 8/11/17].

[15] Executive Order no. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 FR 32172, July 12, 2017. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

[16] M. Barrett, J. Marron et al., *The Cybersecurity Framework Implementation Guidance for Federal Agencies.* NIST Internal Report (NISTIR) 8170, National Institute of Standards and Technology, Gaithersburg, Md., May 2017, http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf.

[17] Computer Security Resource Center, National Vulnerability Database [Website], https://nvd.nist.gov/ [accessed 8/11/17].

[18] CVE-2016-6716 Detail, National Vulnerability Database [Website], https://nvd.nist.gov/vuln/detail/CVE-2016-6716 [accessed 8/11/17].

[19] *Assessing Threats to 2 Mobile Devices & Infrastructure 3: The Mobile Threat Catalogue.* Draft NIST Internal Report (NISTIR) 8144, National Institutes of Standards and Technology, Gaithersburg, Md., September 2016, https://nccoe.nist.gov/sites/default/files/library/mtc-nistir-8144-draft.pdf.

[20] 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, Md., January 2015, http://dx.doi.org/10.6028/NIST.SP.800-163.

[21] Common Vulnerabilities and Exposures, CVE [Website], https://cve.mitre.org/ [accessed 8/11/17].

[22] 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, Md., August 2017, https://doi.org/10.6028/NIST.SP.800-181.

[23] U.S. General Services Administration, *Authorization to Operate Letter*, November 2016, https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/entrust-ato.pdf [accessed 9/28/17].

[24] E. Simmon, DRAFT - Evaluation of Cloud Computing Services Based on NIST 800-145, NIST Draft Special Publication 500-322, National Institute of Standards and Technology, Gaithersburg, Md., 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 8/11/17].

[25] Federal Public Key Infrastructure Policy Authority, *X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework*, May 2015, https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/Common-Policy-Framework.pdf [accessed 8/11/17].

[26] C. Adams, S. Farrell et al., *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*, Internet Engineering Task Force Network Working Group Request for Comments 4210, September 2005 https://tools.ietf.org/html/rfc4210 [accessed 8/11/17].

[27] *Computer Security Division, Applied Cybersecurity Division*, Best Practices for Privileged User PIV Authentication, NIST Cybersecurity White Paper, National Institute of Standards and Technology, Gaithersburg, Md., April 2016, http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf [accessed 8/11/17].