

Derived Personal Identity Verification (PIV) Credentials

Volume B:
Approach, Architecture, and Security Characteristics

William Newhouse

National Cybersecurity Center of Excellence
Information Technology Laboratory

Michael Bartock

Jeffrey Cichonski

Hildegard Ferraiolo

Murugiah Souppaya

National Institute of Standards and Technology
Information Technology Laboratory

Christopher Brown

Spike E. Dog

Susan Prince

Julian Sexton

The MITRE Corporation
McLean, Virginia

August 2019

This publication is available free of charge from <https://doi.org/10.6028/NIST.SP.1800-12>

Previous drafts of this publication are available free of charge from
<https://www.nccoe.nist.gov/library/derived-piv-credentials-nist-sp-1800-12-practice-guide>



DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither 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, 83 pages, (August 2019), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at piv-nccoe@nist.gov.

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

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 information technology security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

Acronyms used in figures can be found in the Acronyms appendix.

ABSTRACT

Federal Information Processing Standards (FIPS) Publication 201-2, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” establishes a standard for a PIV system based on secure and reliable forms of identity credentials issued by the federal government to its employees and contractors. These credentials are intended to authenticate individuals to federally controlled facilities, information systems, and applications as part of access management. In 2005, when FIPS 201 was published, authentication of individuals was geared toward traditional computing devices (i.e., desktop and laptop

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

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

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

KEYWORDS

cybersecurity; Derived PIV Credential (DPC); Enterprise Mobility Management (EMM); identity; mobile device; mobile threat; multifactor authentication; personal identity verification; PIV Card; smart card

ACKNOWLEDGMENTS

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

| Name | Organization |
|------------------|---|
| Judith Spencer | CertiPath Inc. |
| Cliff Mechalske | U.S. Department of Veterans Affairs |
| Matt Scholz | National Aeronautics and Space Administration |
| Brandon Frankens | National Aeronautics and Space Administration |

| Name | Organization |
|----------------------------|-------------------|
| Walter Holda | MobileIron |
| Loay Oweis | MobileIron |
| Sean Frazier | MobileIron |
| Dan Miller | Entrust Datacard |
| Bryan Rosensteel | Entrust Datacard |
| Carlton Ashley | Intel Corporation |
| Abhilasha Bhargav-Spantzel | Intel Corporation |
| Simy Cohen | Intel Corporation |
| Dror Shilo | Intel Corporation |
| Alfonso Villasenor | Intel Corporation |
| Won Jun | Intercede |
| Alan Parker | Intercede |
| Allen Storey | Intercede |
| Iain Wotherspoon | Intercede |
| Andre Varacka | Verizon |
| Russ Weiser | Verizon |

| Name | Organization |
|----------------------|-----------------------|
| Lorrayne Auld | The MITRE Corporation |
| Emmanuel Bello-Ogunu | The MITRE Corporation |
| Eileen Division | The MITRE Corporation |
| Sarah Kinling | The MITRE Corporation |
| Poornima Koka | The MITRE Corporation |
| Matthew Steele | The MITRE Corporation |

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

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

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 | Typographic Conventions | 5 |
| 3 | Approach..... | 6 |
| 3.1 | Audience..... | 7 |
| 3.2 | Scope | 7 |
| 3.3 | Relationship to NIST SP 800-63-3 | 8 |
| 3.4 | Assumptions | 8 |
| 3.4.1 | Modularity | 8 |
| 3.4.2 | Security | 8 |
| 3.4.3 | Existing Infrastructure..... | 9 |
| 3.4.4 | Architecture Components..... | 9 |
| 3.4.4.1 | Credential Management System | 10 |
| 3.4.4.2 | Public Key Infrastructure | 10 |
| 3.4.4.3 | Enterprise Mobility Management | 11 |
| 3.4.4.4 | Mobile Device | 11 |
| 3.4.4.5 | Authenticator..... | 11 |
| 3.5 | Risk Assessment | 12 |
| 3.5.1 | Threats | 13 |
| 3.5.1.1 | Other Threats..... | 17 |
| 3.5.2 | Vulnerabilities | 20 |

| | | |
|----------|--|-----------|
| 3.5.2.1 | Mobile Device Vulnerabilities..... | 20 |
| 3.5.2.2 | Network Vulnerabilities..... | 21 |
| 3.5.3 | Risk..... | 21 |
| 3.5.4 | Security Control Map..... | 22 |
| 3.6 | Technologies..... | 23 |
| 3.6.1 | Entrust Datacard..... | 23 |
| 3.6.2 | Intel Authenticate..... | 24 |
| 3.6.3 | Intercede..... | 24 |
| 3.6.4 | MobileIron..... | 25 |
| 3.6.5 | Verizon Shared Service Provider..... | 25 |
| 3.6.6 | Mobile Endpoints..... | 26 |
| 3.6.7 | Technology Mapping..... | 26 |
| 4 | Architecture | 28 |
| 4.1 | Architecture Description..... | 28 |
| 4.2 | Managed Architecture with EMM Integration..... | 29 |
| 4.3 | Hybrid Architecture for PIV and DPC Life-Cycle Management..... | 30 |
| 5 | Security Characteristics Analysis..... | 34 |
| 5.1 | Assumptions and Limitations..... | 35 |
| 5.2 | Build Testing..... | 35 |
| 5.2.1 | Managed Architecture Build Testing..... | 35 |
| 5.2.1.1 | Initial Issuance..... | 35 |
| 5.2.1.2 | Maintenance..... | 42 |
| 5.2.1.3 | Termination..... | 42 |
| 5.2.1.4 | Derived PIV Authentication Certificate Management..... | 43 |
| 5.2.2 | Hybrid Architecture Build Testing..... | 44 |

| | | |
|-------------------|--|-----------|
| 5.2.2.1 | Initial Issuance | 44 |
| 5.2.2.2 | Maintenance..... | 49 |
| 5.2.2.3 | Termination | 50 |
| 5.2.2.4 | Derived PIV Authentication Certificate Management..... | 50 |
| 5.3 | Scenarios and Findings | 50 |
| 5.3.1 | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes..... | 51 |
| 5.3.2 | PR.AC-3: Remote Access Is Managed | 51 |
| 5.3.3 | PR.AC-6: Identities Are Proofed and Bound to Credentials and Asserted in Interactions | 52 |
| 5.3.4 | PR.AC-7: Users, Devices, and Other Assets Are Authenticated (e.g., Single-Factor, Multifactor) Commensurate with the Risk of the Transaction (e.g., individuals' security and privacy risks and other organizational risks)..... | 52 |
| 5.3.5 | PR.DS-2: Data-in-Transit Is Protected | 52 |
| 5.3.6 | PR.DS-5: Protections Against Data Leaks Are Implemented..... | 53 |
| 5.3.7 | PR.IP-3: Configuration Change Control Processes Are in Place | 53 |
| 5.4 | Authenticator AAL Mapping..... | 54 |
| 6 | Future Build Considerations | 56 |
| Appendix A | List of Acronyms | 58 |
| Appendix B | Glossary | 61 |
| Appendix C | NIST IR 8055 [10] Requirements Enumeration and Implementation Mappings | 65 |
| Appendix D | References..... | 71 |

List of Figures

| | |
|---|----|
| Figure 3-1 Federal ICAM Enterprise Architecture..... | 10 |
| Figure 3-2 The Mobile Ecosystem | 20 |
| Figure 4-1 Federal ICAM Enterprise Architecture..... | 29 |
| Figure 4-2 PIV and DPC Cloud Service Life-Cycle Management with EMM Integration | 30 |
| Figure 4-3 Mobile Device Hybrid Architecture for Both PIV Card and DPC Life-Cycle Management..... | 33 |
| Figure 4-4 Intel-Based Hybrid Architecture for Both PIV Card and DPC Life-Cycle Management | 34 |
| Figure 5-1 PIV Authentication Certificate Selection for PKI-AUTH | 36 |
| Figure 5-2 Password-Based Subscriber Authentication via PIN..... | 37 |
| Figure 5-3 Entrust IdentityGuard DPC Activation Codes | 38 |
| Figure 5-4 MobileIron PIV-D Entrust App | 39 |
| Figure 5-5 Entrust DPC Activation | 40 |
| Figure 5-6 PIV-D Application | 41 |
| Figure 5-7 PIV-D Passcode Entry | 42 |
| Figure 5-8 DPC IdentityGuard Termination..... | 43 |
| Figure 5-9 Test PIV Card User..... | 44 |
| Figure 5-10 Kiosk Workflow..... | 45 |
| Figure 5-11 DPC in MyID Identity Agent | 46 |
| Figure 5-12 DPC Applicant Chooses Intel Credential Profile | 47 |
| Figure 5-13 Email Notification Message via Self-Service Kiosk..... | 47 |
| Figure 5-14 DPC Applicant Inputs the One-Time Code | 48 |
| Figure 5-15 Verizon SSP DPC Authentication Certificate..... | 49 |

List of Tables

Table 3-1 Enrollment and Identity Proofing Threats13

Table 3-2 Authenticator Threats to DPC15

Table 3-3 Mobile Threat Classes and Categories18

Table 3-4 Security Control Mappings22

Table 3-5 Mobile Endpoints26

Table 3-6 Products and Technologies26

Table 4-1 MyID CMS Component Descriptions32

Table 5-1 FIPS 140-2 Validation of Cryptographic Modules53

Table 5-2 AAL-2 Authenticator Requirements Mapping54

Table 5-3 AAL Technology Mappings.....55

1 Summary

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

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

The National Cybersecurity Center of Excellence (NCCoE) Cybersecurity Practice Guide *Derived Personal Identity Verification (PIV) Credentials* demonstrates how Derived PIV Credentials can be issued to PIV Cardholders' mobile devices by using commercial off-the-shelf products and by leveraging the PIV standard for remote authentication to information technology (IT) systems. The NCCoE's Derived PIV Credentials Project is aimed primarily at the federal sector. However, private-sector organizations can leverage these solutions to extend identity proofing and vetting of a primary identity credential to credentials for mobile device users in the commercial sector who use smart card-based credentials or other means of authenticating identity. To that end, the example implementations in this practice guide work from a simple scenario that forms the basis of an architecture tailored to the public and private sectors.

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

Identity Verification (PIV) of Federal Employees and Contractors [2]; Internet Engineering Task Force (IETF) Request for Comments (RFC) 4210; NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [8]; and NIST's *Mobile Threat Catalogue* [9].

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

Section 1: Summary presents the challenge addressed in this volume (Volume B: *Approach, Architecture, and Security Characteristics*). The example implementations address 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 business decision makers, program managers, IT professionals (e.g., systems administrators), and other stakeholders who will be responsible for procuring, designing, implementing, and managing deployments of DPCs 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, explains the risk assessment that informed platform development, and provides an overview of 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 Characteristic Analysis provides details about the tools and techniques we used to perform risk assessments pertaining to DPCs. 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 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 DPCs.

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

1.1 Challenge

Mobile phones and tablets that lack card readers are being increasingly deployed by federal agencies. Additionally, laptop personal computers without built-in card readers are increasingly being used by PIV users in mobile situations away from their desktop environments. These mobile devices are not able to

use the PIV Card directly to leverage the security and control characteristics of the FIPS 201-2 PIV system standard.

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

Additionally, the guidelines in NIST SP 800-157 for managing the Derived PIV Authentication certificate throughout its life cycle (issuance and maintenance) and its interactions with the PIV Card life cycle present challenges to the implementer such as managing integration efforts between DPC and PIV Card issuing systems. Further, the DPC implementers must acquire the Derived PIV Authentication certificates from approved public key infrastructure (PKI) service providers, necessitating integration with these service providers.

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

1.2 Solution

This NIST Cybersecurity Practice Guide demonstrates how commercially available technologies can meet an organization's need to issue multifactor credentials to mobile devices for authenticating to IT systems in operational environments.

We built an environment that resembles an enterprise network by using commonplace components such as identity repositories, supporting certificate authorities, and web servers. Next, products and capabilities were identified that, when linked together, provide two example implementations demonstrating life-cycle guidelines outlined in NIST SP 800-157 [\[6\]](#). These example implementations leverage cloud services where possible through a software as a service (SaaS) component. The federal government encourages the use of SaaS or shared service providers (SSPs) [\[11\]](#) that operate under federal policy, such as certificate authorities operating in accordance with policy developed by the Federal 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.

One of our example implementations includes integration of an EMM and a DPC solution. EMMs are useful in applying NIST SP 800-157 life-cycle guidelines by integrating an organization's mobile device

issuance process with DPC issuance. EMMs can also assist with terminating the DPC by remotely destroying the EMM's software container.

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

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

1.3 Benefits

For an organization that is planning and looking for solutions to issue DPCs to its workforce, the example implementations described in this guide will help the organization 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 life-cycle management
- demonstrating integration with an EMM solution

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrate standards-based reference designs and provides users with the information they need to replicate the DPC example implementations. These reference designs are modular and can be deployed in whole or in part.

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 solutions

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 following topics:

- challenges that enterprises face in issuing strong multifactor credentials to mobile devices

- the example solutions built at the NCCoE
- benefits of adopting the example solutions

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 3.5.3](#), Risk, provides a description of the risk analysis we performed
- [Section 3.5.4](#), Security Control Map, maps the security characteristics of the example solutions 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 DPC 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 builds created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solutions. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create the example solutions.

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 either 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 the DPC 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 that you will seek products that are congruent with applicable standards and best practices. [Section 3.6](#), Technologies, lists the products we used and maps them to the cybersecurity controls provided by the reference solutions.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

3 Approach

To develop our example solutions, the Derived PIV Credentials 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) [12]. In response to the FRN, several vendors expressed interest in helping the NCCoE build example solutions. Technology companies with relevant products then signed a Cooperative Research and Development Agreement (CRADA) with the NCCoE for the project. After the CRADAs were signed, the NCCoE sponsored a kickoff meeting for the project team, collaborating vendors, and other members of the Derived PIV Credentials Community of Interest (COI).

During the kickoff, we gathered requirements and lessons learned from project stakeholders; this helped establish objectives for our example implementations. 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 implementations. This assessment included risk factors to both the functions of the system (e.g., DPC issuance or revocation) and to its parts, such as the mobile devices into which a DPC would be provisioned.

The Derived PIV Credentials Project used a phased approach that took direct advantage of previous work by NIST in this area. NIST Internal Report 8055 [10], *Derived Personal Identity Verification (PIV)*

Credentials (DPC) Proof of Concept Research, presents a scheme for provisioning a DPC to an organization-managed mobile device. This project applied these technologies as a starting point, then sought to expand on the DPC ecosystem to provide greater diversity across mobile device models, platforms, [authenticators](#), [Derived PIV Credential Management Systems \(DCMSes\)](#), and EMM products.

3.1 Audience

This guide is intended for IT and security managers and for system administrators responsible for deploying secure solutions to support the evolving mobile ecosystem of an 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 when using these devices. As mentioned previously, DPC 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 Personal Identity Verification (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 on only a portion of NIST SP 800-157—the life-cycle activities. Specifically, we evaluated the example solutions against the requirements related to initial issuance, maintenance, and termination of DPCs.

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

Only Derived PIV Authentication certificates that support remote issuance are addressed in this practice guide. To support a higher level of assurance, we would need to address additional in-person life-cycle requirements that were deemed out of scope for this project. [Section 6](#) offers some future build considerations.

This project integrates an EMM component into one of our documented example implementations. EMMs are essential to securing mobile end points; however, this project defers to the [Mobile Device Security: Corporate-Owned Personally-Enabled](#) Project at the NCCoE for specific security control recommendations. [Section 3.5](#), Risk Assessment, includes threats specific to DPCs issued to

[authenticators](#) contained within mobile devices. For privacy considerations as they pertain to risk, readers of this publication are encouraged to review the NIST [SP 800-63-3 discussion on privacy](#).

[PIV Card life-cycle management](#) is not within the scope of the project. However, tests were conducted on test PIV credentials prior to issuing DPCs and to validate that a DCMS performs all required checks of a DPC subscriber's PIV Card and associated PIV Authentication certificate per NIST SP 800-157.

3.3 Relationship to NIST SP 800-63-3

The NIST SP 800-63-3 series of documents published in June 2017 retired the level of assurance (LOA) 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, FIPS 201-2 [\[2\]](#) and NIST SP 800-157 refer to the earlier LOA terminology for electronic authentications. We have mapped the authenticators used in this project to an AAL in [Section 5.4](#). IAL is not applicable in the context of DPC because deriving identity is accomplished by proving possession and successful authentication of an authenticator (on the PIV Card) that is already bound to the original, proofed digital identity [\[7\]](#).

3.4 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 implementations presented have the following assumptions:

- An implementer who works for a U.S. federal agency will be complying with FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors* [\[2\]](#).
- The mobile devices in an organization's DPC solution are organization-provided [\[13\]](#), and the organization centrally manages them with security policies and controls.

3.4.1 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 life-cycle management solution into a diverse set of existing deployments.

3.4.2 Security

A second assumption is that adopters of our example implementations 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 SP 800-63-3. Further, we assume that the security features of each product integrated into our example implementations will perform as described by the respective product vendor.

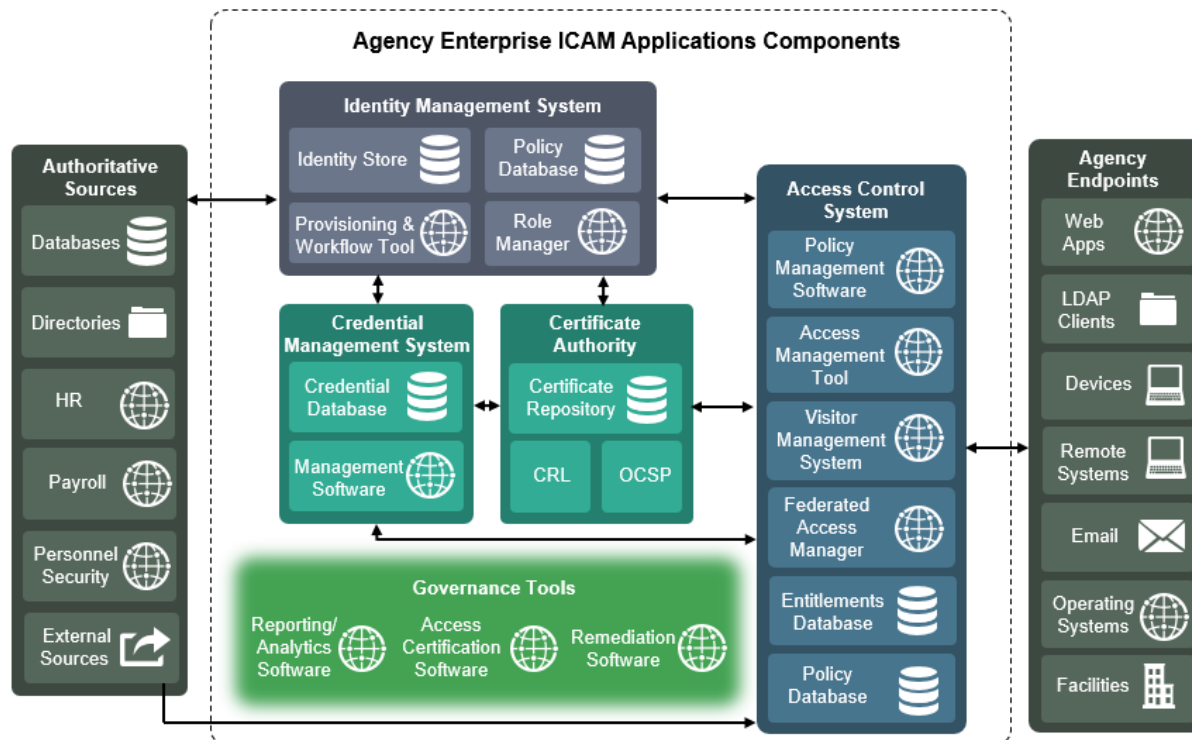
3.4.3 Existing Infrastructure

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

3.4.4 Architecture Components

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

Figure 3-1 [Federal ICAM Enterprise Architecture](#)



3.4.4.1 Credential Management System

A [CMS](#) contains management software and is central to executing the life-cycle operations, typically sponsorship, registration, issuance, maintenance, and termination of authentication credentials. Usually, information related to the life-cycle operations is stored within a database. In our architecture, we depict two types of CMSes: PIV and Derived PIV. The PIV CMS is responsible for enforcing life-cycle activities in accordance with FIPS 201-2, and the DCMS enforces the life-cycle 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 DPC solution.

3.4.4.2 Public Key Infrastructure

The PKI (also referred to as the certificate authority or certification authority [CA]) issues, maintains, and revokes digital certificates. References to PKI in this document will focus only on digital certificates stored on PIV Cards and mobile devices. The PKI can be operated as part of an on-premises infrastructure and is also offered as a managed service. PIV CMS service providers partner with PKI service providers for issuing the digital certificates that are provisioned to the PIV Card and the mobile

device. Typically, certificate status services such as a certificate revocation list (CRL) repository and online certificate status protocol (OCSP) services are also offered by PKIs.

3.4.4.3 Enterprise Mobility Management

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

3.4.4.4 Mobile Device

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

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

In this publication, we use only mobile devices as the “devices” shown in Figure 3-1. In one scenario, we use a hybrid device, a laptop that does not have a built-in smart card reader but that can leverage PIV Card capabilities in a hardware-enhanced container.

3.4.4.5 Authenticator

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

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

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

3.5 Risk Assessment

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

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of [NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*](#) [4]—material that is available to the public. The [Risk Management Framework \(RMF\)](#) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the builds, and this guide.

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

Allowing users access to services from a mobile device leads to a more efficient and effective workforce. There are risks, however, and the security objectives [13] of confidentiality, integrity, and availability need to be maintained on the mobile end point. The threats to weak single-factor authentication mechanisms, such as passwords, are well documented by industry [14] and government [9]. Further, the 2017 Department of Homeland Security (DHS) *Study on Mobile Device Security* [15] found the failure to use strong multifactor authentication mechanisms to protect critical cloud services to be a gap in the defense of current mobile devices. This finding is underscored by the move of organizations to cloud services that provide critical services such as email and calendaring. The DHS study recommends enhancing mobile Federal Information Security Modernization Act 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 Special Publication 800-123, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, recommends. The publication further recommends that organizations design and acquire one or more solutions that collectively mitigate current workforce mobile device security risk. For an in-depth discussion on digital identity risk management, we encourage review of [Section 3.5.1](#), which presents a list of possible identity risks and how they are addressed by DPCs, based on NIST SP 800-63-3 guidelines related to digital identity risk. An

organization can apply the guidelines while executing all relevant Cybersecurity Framework and RMF life-cycle phases [\[7\]](#).

Federal cybersecurity risk management has taken on increased emphasis with release of the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [\[16\]](#). 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.”

In response, NIST released NIST Internal Report 8170, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies* [\[17\]](#). This NIST Internal Report guides agencies on how the Cybersecurity Framework can be used to augment current NIST security and privacy risk management publications. We recommend that organizations, especially federal agencies that implement a DCMS, follow the recommendations presented in NIST Internal Report 8170. For instance, the framework’s Example 1—Integrate Enterprise and Cybersecurity Risk Management—recommends using the five cybersecurity Functions (Identify, Protect, Detect, Respond, and Recover) to organize cybersecurity risk management activities at the highest level. [Section 3.5.4](#) presents a list of possible functions that a DPC implementation can address. We recommend that this information be used when communicating risk throughout an organization.

3.5.1 Threats

NIST SP 800-63-3 provides a general identity framework by incorporating authenticators, credentials, and assertions into a digital system [\[7\]](#). Included in the publication are threat analyses in the areas of authenticator and life-cycle threats. Table 3-1 and Table 3-2 use these threats as a basis for a discussion of threats applicable to a DPC system.

Table 3-1 Enrollment and Issuance Threats

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

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

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

Table 3-2 Authenticator Threats to DPC

| Authenticator Threats/Attacks | Examples | Applicability to DPC |
|-------------------------------|---|---|
| Theft | A hardware cryptographic device is stolen. | An external USB drive or microSD card can be readily stolen. Multifactor authentication prevents unauthorized use of the private key. |
| | A cell phone is stolen. | A mobile device that stores the DPC in software or in an embedded cryptographic token can be readily stolen. Use mobile locking mechanisms, remote wipe, and other mobile device security best practices to mitigate risk of a stolen device. Furthermore, multifactor authentication prevents unauthorized use of the private key. |
| Duplication | A software PKI authenticator (private key) is copied. | A DPC stored in a software-based container on a mobile device could be copied from the device. Use device sandboxing mechanisms, cryptographic techniques, and malware detection mechanisms as mitigation. |

| Authenticator Threats/Attacks | Examples | Applicability to DPC |
|-------------------------------|---|---|
| Eavesdropping | Memorized secrets are obtained by watching keyboard entry. | Through shoulder surfing, an attacker could observe a PIN/password that protects the cryptographic token. Educate users to be mindful of surroundings when entering PINs/passwords. Use authentication end points that employ trusted input and trusted display capabilities. Note: This attack compromises only one factor of the multifactor authentication mechanisms provided by DPC. |
| | Memorized secrets or authenticator outputs are intercepted by key-stroke-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 end point. Also, native cryptographic token storage on some devices can leverage trusted paths for PIN/password entry. |
| Offline cracking | A software PKI authenticator is subjected to a dictionary attack to identify the correct password or PIN to use to decrypt the private key. | A DPC stored in a software-based container on a mobile device could be copied from the device and would be subject to offline cracking. Use PIN/password throttling, device encryption, and malware detection mechanisms as mitigation. |
| Side-channel attack | A key is extracted by differential power analysis on a hardware cryptographic authenticator. | A mobile device is susceptible to side-channel attacks only if the PIN/password has been successfully entered. Use key and/or PIN usage time-out/limits and adopt other countermeasures described in NIST SP 800-63-3B and PHY-5 [9] . |
| | A cryptographic authenticator secret is extracted by analysis of the response time of the authenticator over many attempts. | A mobile device is susceptible to side-channel attacks only if the PIN/password has been successfully entered. Use key and/or PIN usage time-out/limits and adopt other |

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

3.5.1.1 Other Threats

Mobile devices like those featured in our example implementations are subject to the broader set of mobile ecosystem threats. From NIST Internal Report 8144 [\[18\]](#):

Mobile devices pose a unique set of threats to enterprises. Typical enterprise protections, such as isolated enterprise sandboxes and the ability to remote wipe a device, may fail to fully mitigate the security challenges associated with these complex mobile information systems. With this in mind, a set of security controls and countermeasures that address mobile threats in a holistic manner must be identified, necessitating a broader view of the entire mobile security

ecosystem. This view must go beyond devices to include, as an example, the cellular networks and cloud infrastructure used to support mobile applications and native mobile services.

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

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

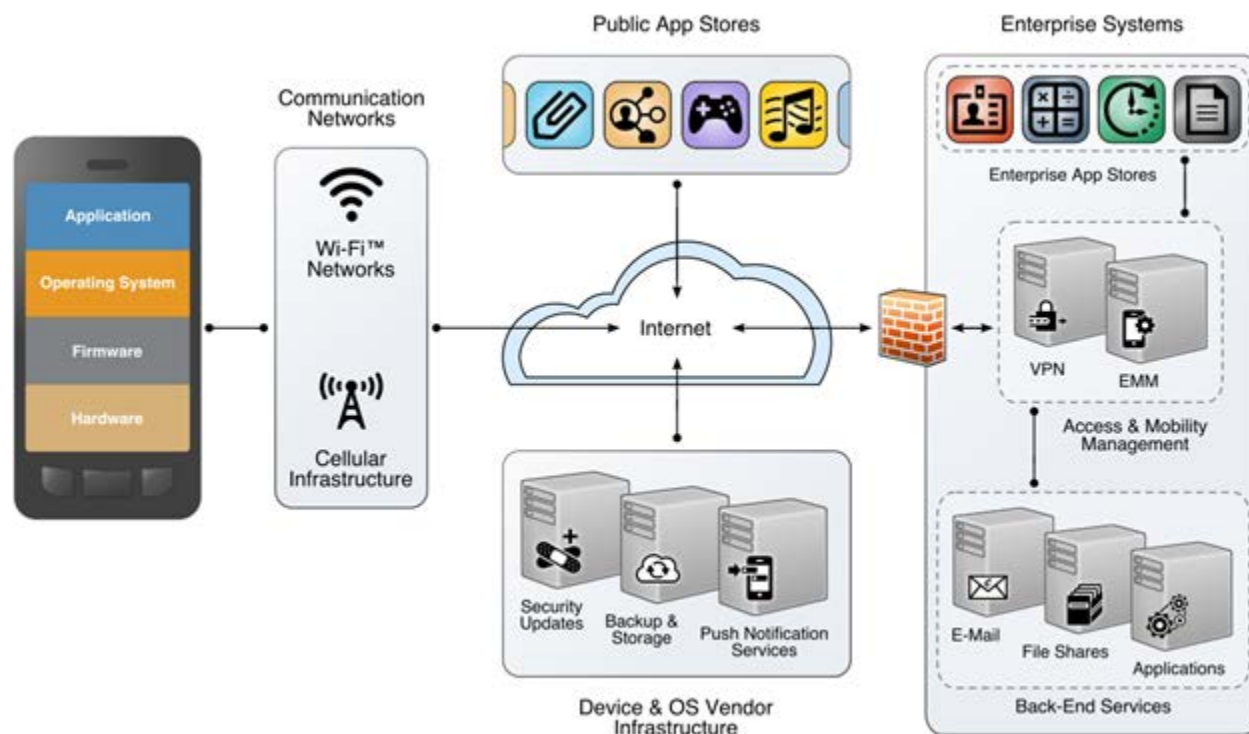
Table 3-3 Mobile Threat Classes and Categories

| Threat Class | Threat Category | Threat Class | Threat Category |
|-----------------------|--|---|---|
| Application | Malicious or Privacy-Invasive Application | Local Area Network and Personal Area Network | Network Threats: Bluetooth |
| | Vulnerable Applications | | Network Threats: Near-Field Communication (NFC) |
| Authentication | Authentication: User or Device to Network | | Network Threats: Wi-Fi |
| | Authentication: User or Device to Remote Service | Payment | Application-Based |
| | Authentication: User to Device | | In-Application Purchases |
| Cellular | Carrier Infrastructure | | NFC-Based |
| | Carrier Interoperability | Physical Access | Physical Access |
| | Cellular Air Interface | Privacy | Behavior Tracking |
| | Consumer-Grade Femtocell | Supply Chain | Supply Chain |
| | Short Messaging Service/Multi-media Messaging Service/Rich Communications Services | Stack | Baseband Subsystem |
| | Unstructured Supplementary Service Data | | Boot Firmware |
| | Voice over Long-Term Evolution | | Device Drivers |

| | | | |
|--|--|--|---|
| Ecosystem | Mobile Application Store | | Isolated Execution Environments |
| | Mobile Operating System (OS) and Vendor Infrastructure | | Mobile Operating System |
| EMM | Enterprise Mobility | | SD Card |
| Global Positioning System (GPS) | GPS | | Universal Subscriber Identity Module/Subscriber Identity Module/Universal Integrated Circuit Card (UICC) Security |

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

Figure 3-2 The Mobile Ecosystem



Because threats to organizationally controlled infrastructure 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 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [5], for appropriate security controls.

3.5.2 Vulnerabilities

Vulnerabilities can exist within mobile applications, mobile and desktop operating systems, and network applications that are employed in the storage and use of a mobile credential. 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) [19]. The NVD is the U.S. government repository of standards-based vulnerability management data.

3.5.2.1 Mobile Device Vulnerabilities

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

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

3.5.2.2 Network Vulnerabilities

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

This guide suggests two resources to assist network vulnerability analyses as input to a risk assessment. The CVE database [22] lists more than 100,000 vulnerabilities that can affect web servers, Structured Query Language (SQL) servers, domain name system (DNS) servers, 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 hypertext transfer protocol (http) response splitting.

Many of these vulnerabilities are operating system- or application-based. Others are protocol-based (e.g., vulnerabilities inherent in internet protocol Version 6, 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 the NVD so it remains a viable source of vulnerabilities that affect network servers.

3.5.3 Risk

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

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

3.5.4 Security Control Map

An organization may benefit from examples in NIST Interagency Report 8170 [\[17\]](#). For instance, the framework's Example 1—Integrate Enterprise and Cybersecurity Risk Management—recommends using the 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 Cybersecurity Framework Subcategory, a mapping was made to NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [\[8\]](#), to show what types of work roles are needed to implement and maintain a DPC solution. We recommend that this information be used when communicating risk throughout an organization.

Table 3-4 Security Control Mappings

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

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

Example 3 documented in Draft NIST Interagency Report 8170—Integrate and Align Cybersecurity and Acquisition Processes—may help in acquiring and integrating a DCMS into an organization’s environment. As the framework notes, an organization could ask a vendor to include its Cybersecurity Framework Profile in response to a request for information for a DPC solution. Receiving this data allows an objective comparison of solutions.

3.6 Technologies

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

3.6.1 Entrust Datacard

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

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

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

3.6.2 Intel Authenticate

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

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

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

3.6.3 Intercede

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

3.6.4 MobileIron

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

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

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

3.6.5 Verizon Shared Service Provider

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

The SSP solution is built as a scalable architecture that may be complemented (at the Agency’s option) with Card Management Services, Lightweight Directory Access Protocol (LDAP)-based Directory services, and Simple Certificate Validation Protocol Validation Services. The core Verizon SSP offering provides all the digital certificate profiles required to be implemented on FIPS-201 approved smart cards.

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

3.6.6 Mobile End Points

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

Table 3-5 Mobile End Points

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

3.6.7 Technology Mapping

Table 3-6 lists all of the technologies used in this project, and provides a mapping among the generic application term, the specific product used, and the security control(s) that the product provides. Refer to Table 3-4 for an explanation of the NIST Cybersecurity Framework Subcategory codes. Note: Some of our components are marked in the version column as not applicable. This is due to the use of SaaS [\[24\]](#) cloud services.

Table 3-6 Products and Technologies

| Component | Product | Version | Function | Cybersecurity Framework Subcategories |
|---------------------------|-------------------------------|----------------|---|---------------------------------------|
| PKI Certificate Authority | Entrust Data-card 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 |
|--|---------------------------------|----------------|---|---|
| PKI Certificate Authority | Verizon Shared Service Provider | Not applicable | Entity that issues an authentication certificate, which is an X.509 public key certificate that has been issued in accordance with the requirements of NIST SP 800-157 and the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [25] | PR.AC-1 |
| Derived PIV Credential Management System | Entrust Data-card IdentityGuard | Not applicable | Entity that implements Derived PIV life-cycle activities in accordance with NIST SP 800-157 | PR.AC-1, PR.IP-3 |
| Derived PIV Credential Management System | Intercede MyID | 10.8 | Entity that implements Derived PIV life-cycle activities in accordance with NIST SP 800-157 | PR.AC-1, PR.IP-3 |
| PIV Credential Management System | Entrust Data-card IdentityGuard | Not applicable | Entity that implements PIV life-cycle activities in accordance with FIPS 201-2 | PR.AC-1, PR.IP-3 |
| PIV Credential Management System | Intercede MyID | 10.8 | Entity that implements PIV life-cycle activities in accordance with FIPS 201-2 | PR.AC-1, PR.IP-3 |
| Enterprise Mobility Management System | MobileIron Core | 9.3 | Entity that provides security services commonly needed for security management of mobile devices [13] | PR.AC-1, PR.AC-3 |
| Authenticator | Entrust PIV-D | 1.3.0.4 | Software component that stores the private key associated with the Derived PIV Authentication certificate | PR.DS-2, PR.DS-5 |
| Authenticator | Intercede Identity Agent | 3.14 | Software component that stores the private key associated with the Derived PIV Authentication certificate | PR.DS-2, PR.DS-5 |

| Component | Product | Version | Function | Cybersecurity Framework Subcategories |
|---------------|--------------------|----------------|---|--|
| Authenticator | Intel Authenticate | Not applicable | Hybrid component that stores the private key associated with the Derived PIV Authentication certificate | PR.DS-2 , PR.DS-5 |

4 Architecture

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

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

4.1 Architecture Description

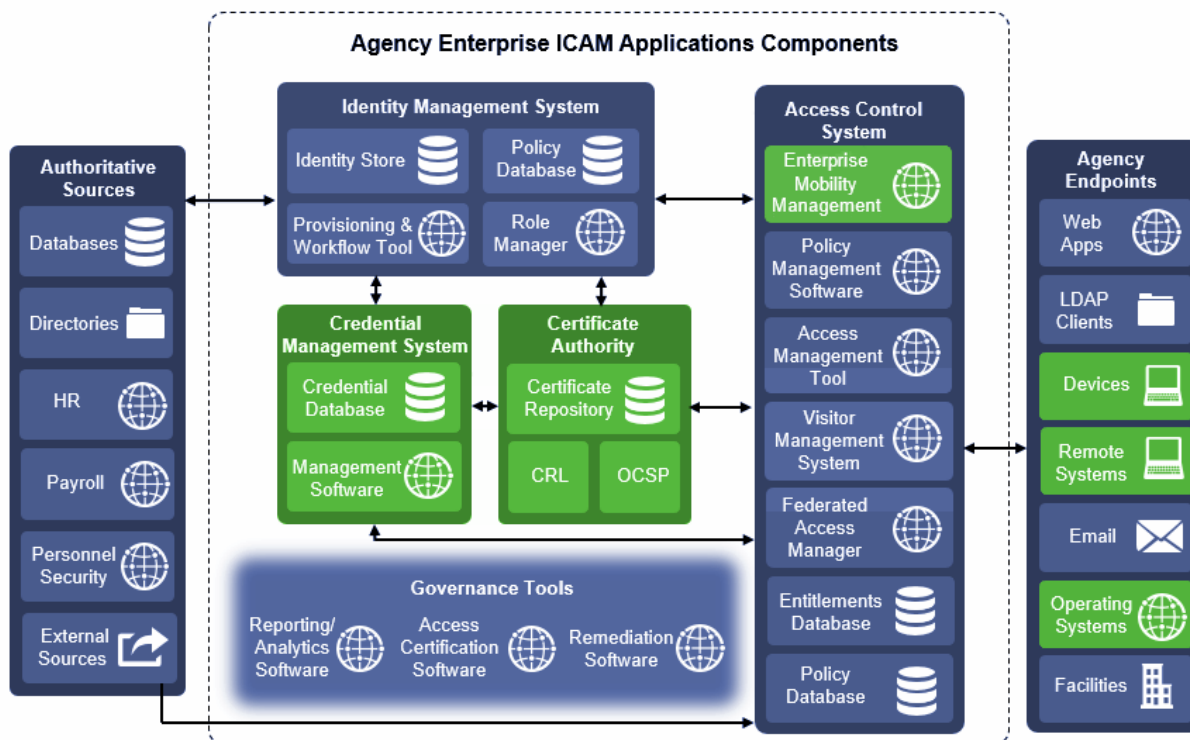
Many federal agencies have opted to use a managed shared solution for issuing PIV Cards for their employees rather than deploy and operate their own PKI. GSA's Managed Service Office established the USAccess program to offer federal agencies a managed shared service solution for PIV Card issuance to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

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

As a result, this practice guide documents two reference architectures that are described in the following sections. To assist readers in putting our architectures in the context of the Federal ICAM Enterprise Architecture, as discussed in [Section 3.4.4](#), below we have highlighted (in green) the components that are used within each architecture. Note that Figure 4-1 is slightly modified from the original FICAM architecture to allow an EMM component to be included within the access control

system. An EMM can execute the access processes from policy stored within an access management database.

Figure 4-1 Federal ICAM Enterprise Architecture



4.2 Managed Architecture with EMM Integration

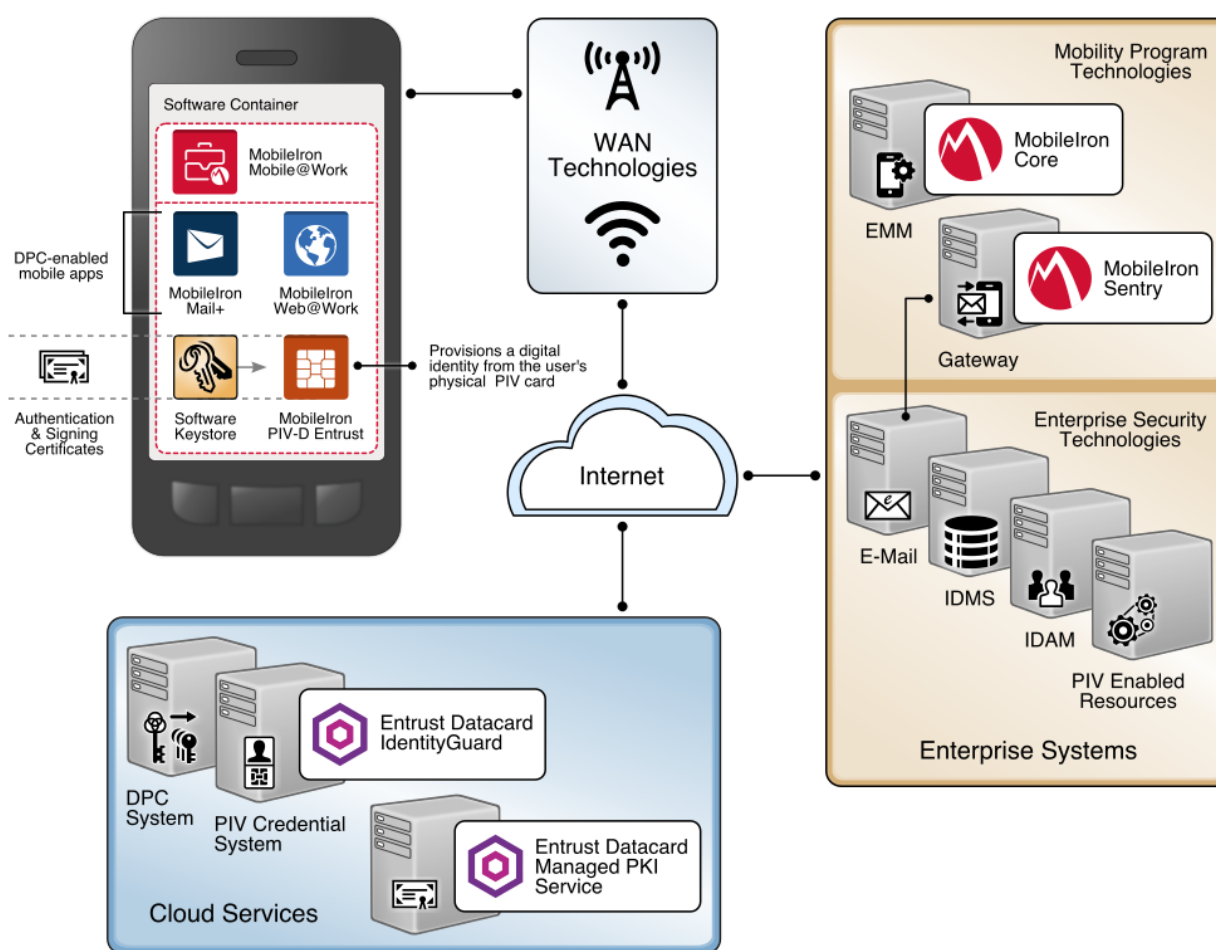
[Figure 4-2](#) depicts the final example implementation for this reference architecture, in which cloud services are used to manage the PIV and DPC life-cycle activities. It also introduces an EMM into the workflow, recognizing the need for organizations to apply a consistent set of security policies on the device. In this scenario, the same vendor operates the PIV and DPC management services to simplify the life-cycle linkage requirements between the DPC and PIV so that integration efforts across two solutions are not necessary. This simplification also allows 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 suitable if an organization prefers a more modular architecture.

The back-end EMM components, MobileIron Core and MobileIron Sentry, were deployed on premises in the demilitarized zone (DMZ) 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 virtual private network (VPN) end point, which creates an authenticated

and 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](#). However, as Sentry is not required for any life-cycle management activities of DPCs, it is not further documented by this guide.

The enterprise network also includes Active Directory (AD) and an 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.

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



4.3 Hybrid Architecture for PIV and DPC Life-Cycle Management

This architecture is described as *hybrid*, in that it utilizes resources that are located both on premises and in the cloud. Organizations have chosen this architectural path to leverage previous investments in

enterprise systems, such as identity management solutions, while simultaneously gaining efficiencies and agility from cloud services. In this scenario, the PIV Card and Derived PIV Credential Management Systems are deployed within a simulated internal enterprise network. A self-service kiosk, which serves as the enrollment station for DPC initial issuance, is also deployed on the internal network. The cloud-based managed PKI service is integrated with the on-premises CMS through a toolkit available for the CMS software.

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

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

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

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

This architecture supports options for mobile and Intel-based devices, which use software- and hardware-backed authenticators, respectively. The DPC applicant experience for initial issuance differs slightly, depending on the authenticator type. When requesting a DPC for a mobile device, the applicant is prompted to scan a quick response (QR) code by using the enrollment application once the back-end system has validated the PIV Authentication certificate. In Intel-based hybrid devices, however, the applicant is sent an OTP through an out-of-band notification scheme, which in this example implementation uses email. Knowledge of the OTP verifies that the user attempting to collect the DPC is the same user who requested it. More details of this process can be found in [Section 5.2.2.1](#).

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

Table 4-1 MyID CMS Component Descriptions

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

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

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

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

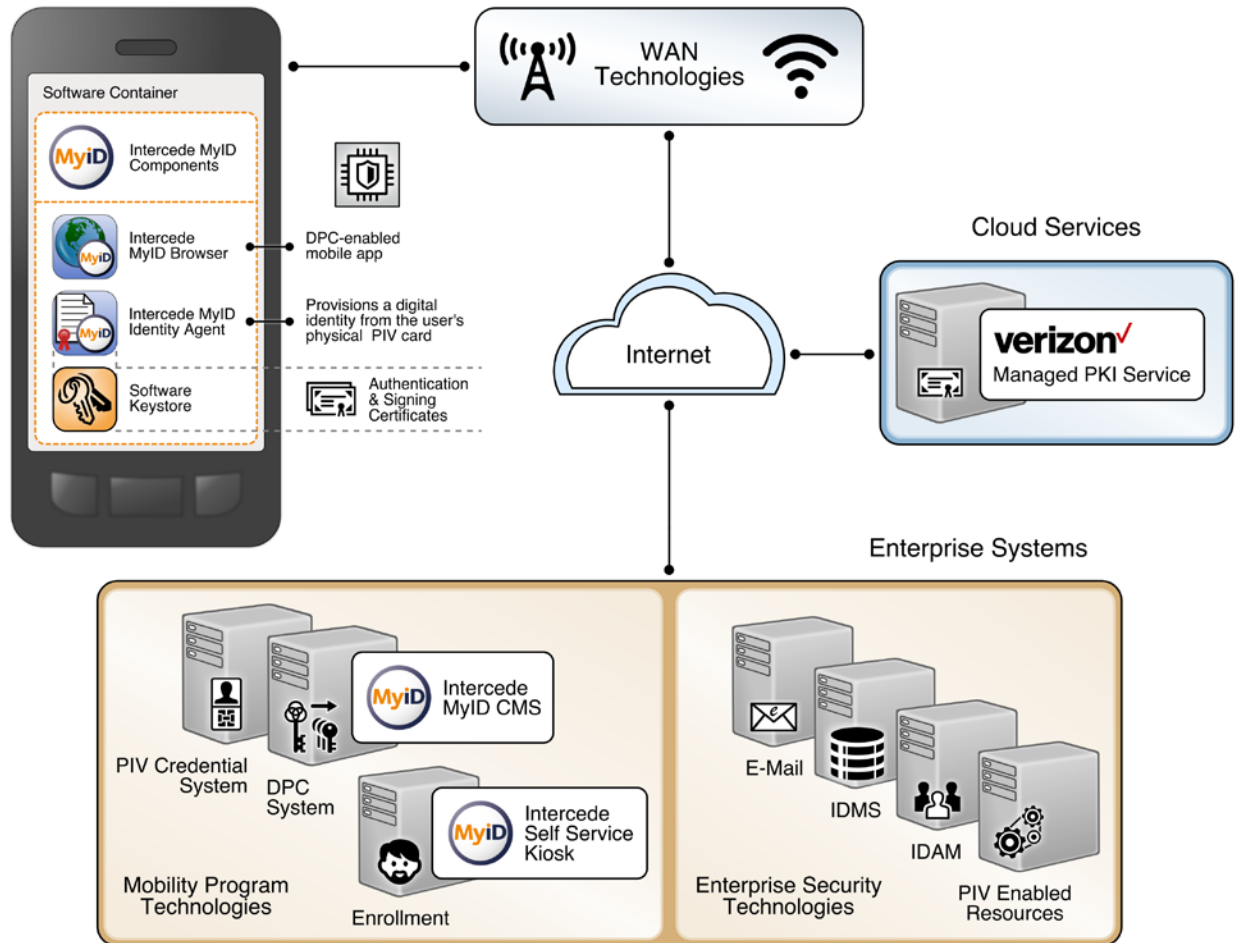
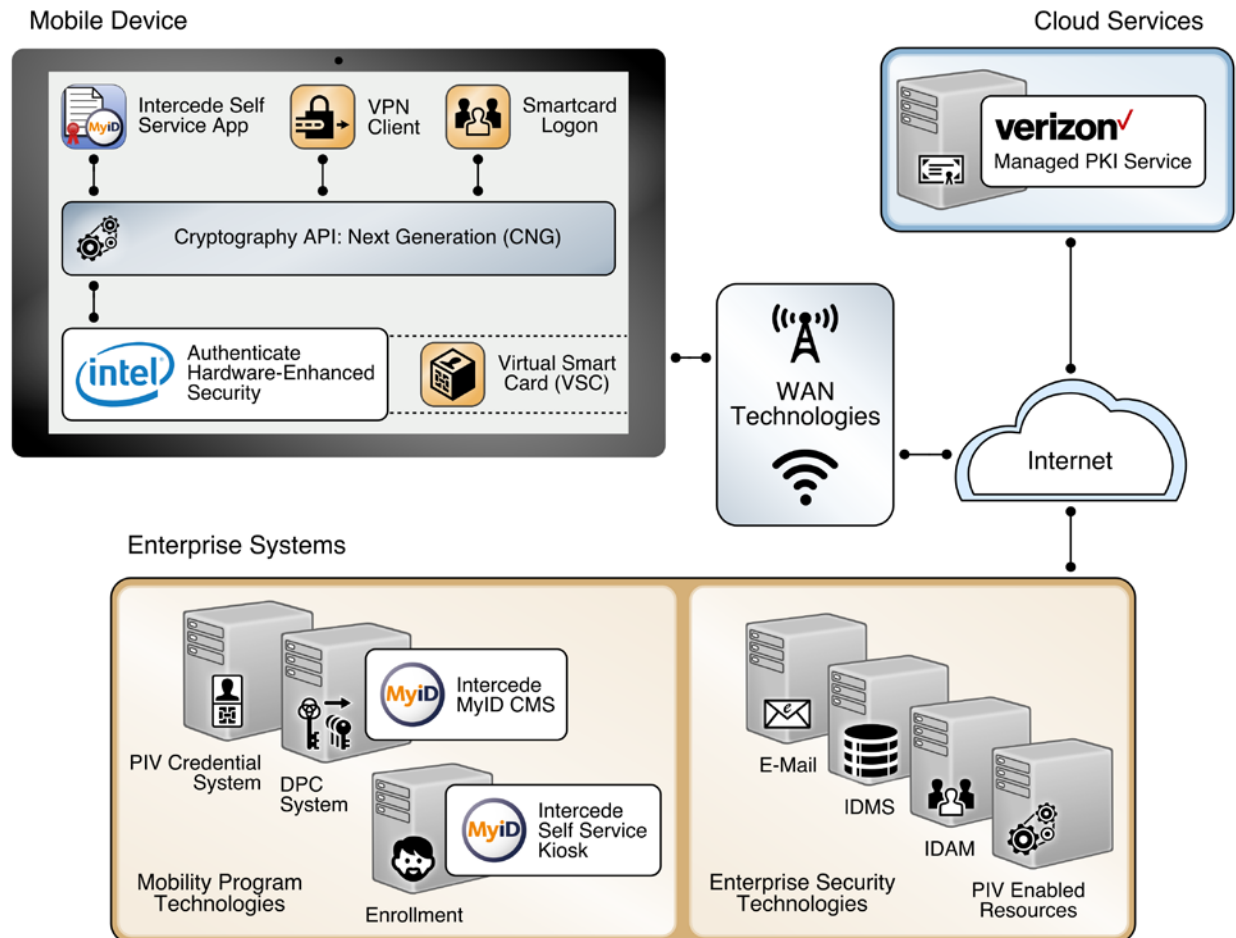


Figure 4-4 Intel-Based Hybrid Architecture for Both PIV Card and DPC Life-Cycle Management



5 Security Characteristic Analysis

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of demonstrating the life cycle of DPC requirements specified in NIST SP 800-157. In addition, it seeks to understand the security benefits and drawbacks of the example solutions. Readers may also find [Section 3.5](#) helpful when evaluating DPC security characteristics for their own organization.

5.1 Assumptions and Limitations

The security characteristic analysis 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 the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting these reference architectures.

5.2 Build Testing

This project uses Table 5, Requirements Definition and Implementation Mappings, from NIST Internal Report 8055 [10] as a basis for testing the example implementations. 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 life-cycle stages: initial issuance, maintenance, and termination. Screenshots of certain operations aid the narrative. Detailed workflow steps for these example implementations are 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 Managed Architecture Build Testing

5.2.1.1 Initial Issuance

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

To test this example implementation, Entrust Datacard gave us access to a development instance of its IdentityGuard service and populated it with identities of users who were issued test PIV Cards. These users were also granted preapproval to request a DPC. We observed that the prescribed DPC initial issuance workflow, summarized below, adhered to the requirements in NIST SP 800-157 [6]. Note that the figures below are screenshots from a shared IdentityGuard test infrastructure and feature an

AnyBank Self-Service logo. This image is configurable and is not intended to exclude federal agencies from using this service.

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

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

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

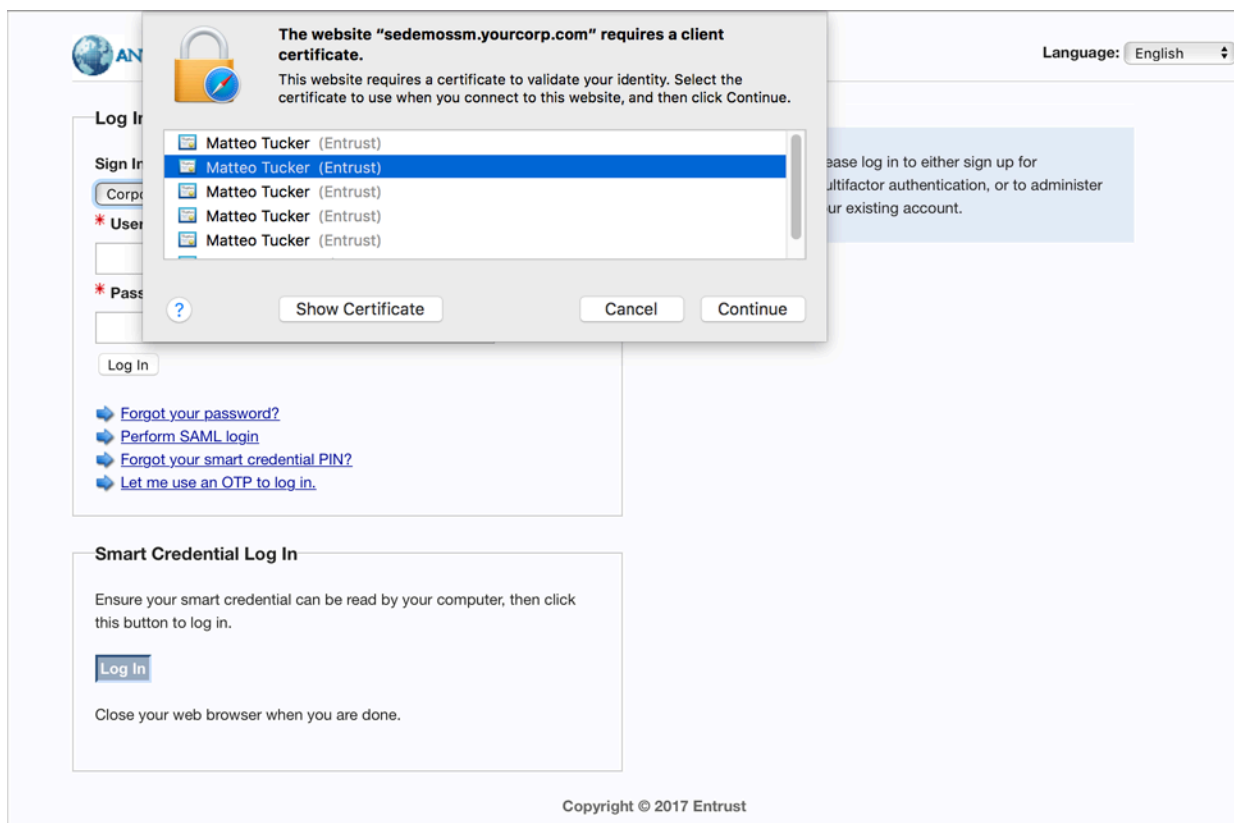
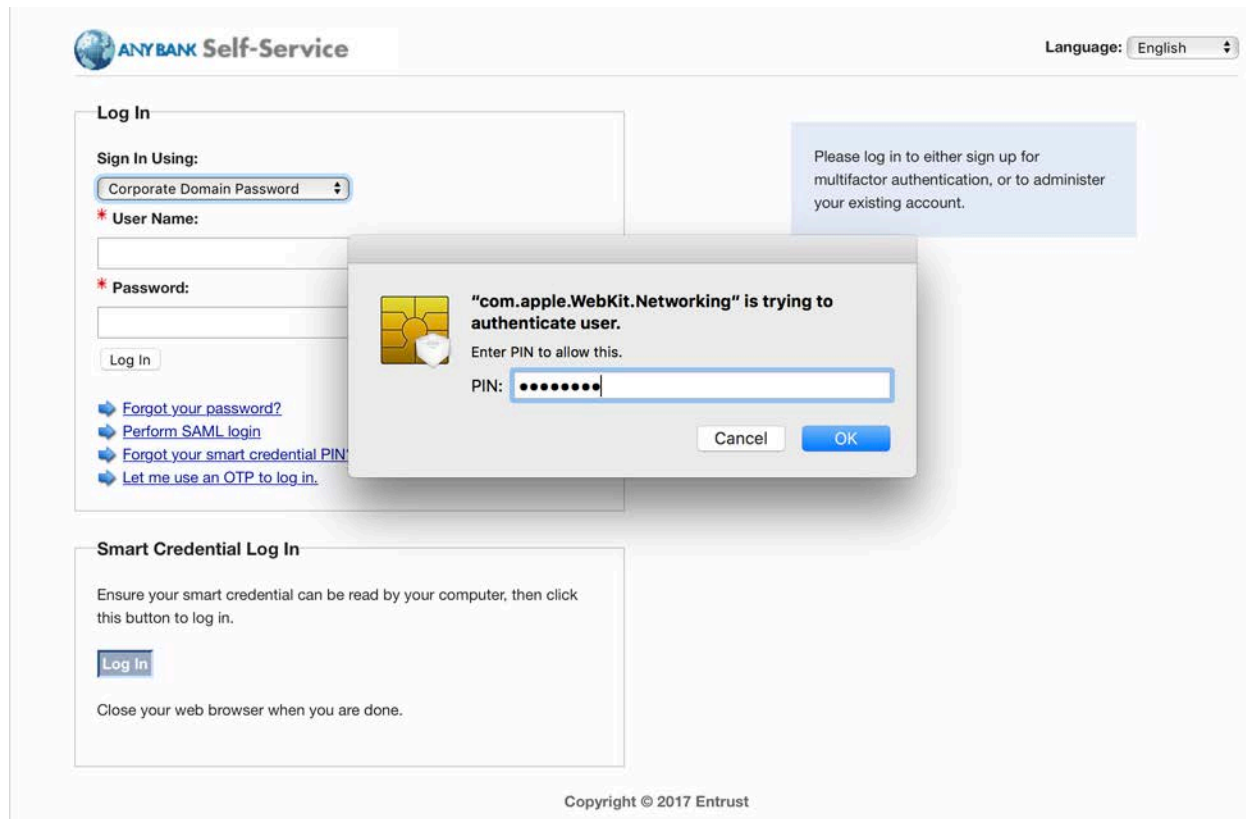
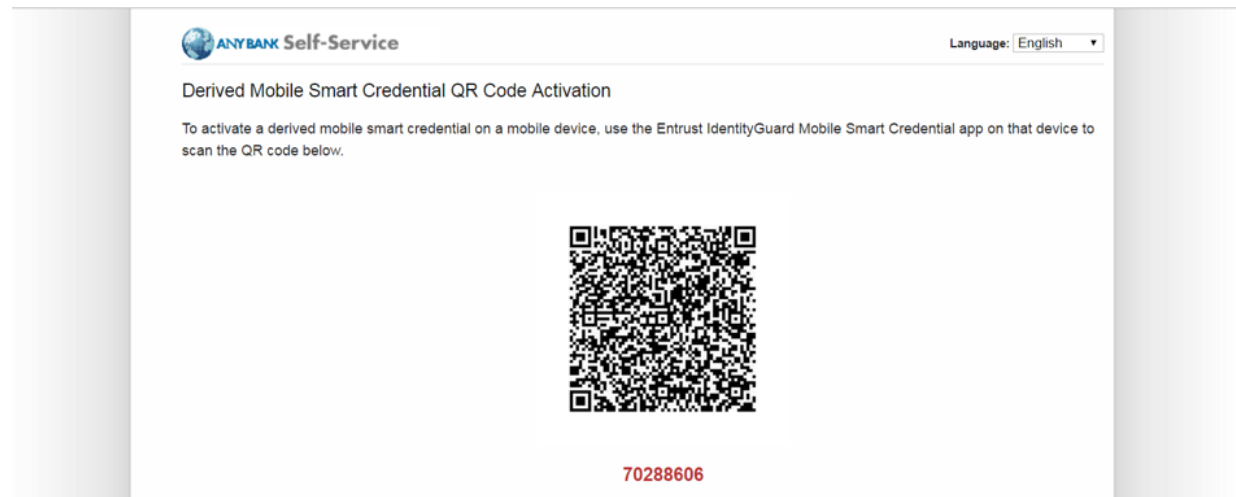


Figure 5-2 Password-Based Subscriber Authentication via PIN



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

Figure 5-3 Entrust IdentityGuard DPC Activation Codes



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

Figure 5-4 MobileIron PIV-D Entrust Application

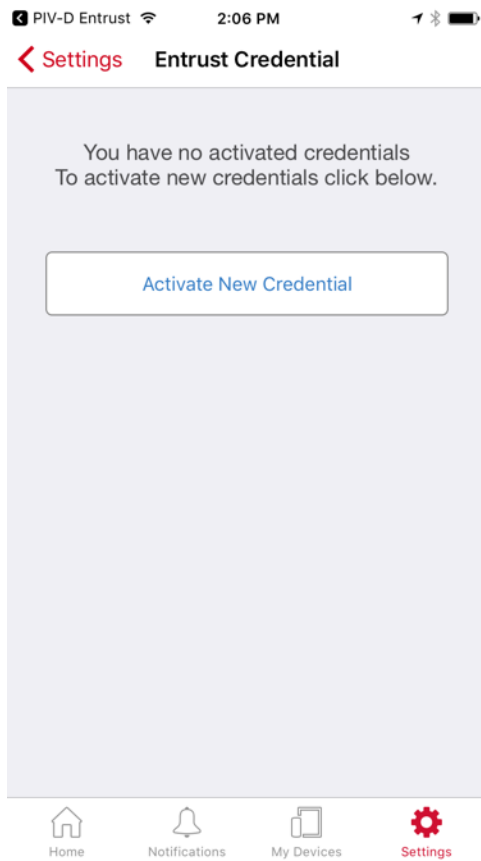


Figure 5-5 Entrust DPC Activation

MobileIron 2:13 PM

Back Activate Credential

Enter Password

Enter the 8 digit passcode listed below the QR code and tap Activate

70288606

Activate

| | | |
|-----------|----------|-----------|
| 1 | 2 ABC | 3 DEF |
| 4 GHI | 5 JKL | 6 MNO |
| 7 PQRS | 8 TUV | 9 WXYZ |
| | 0 | X |

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

Figure 5-6 PIV-D Application

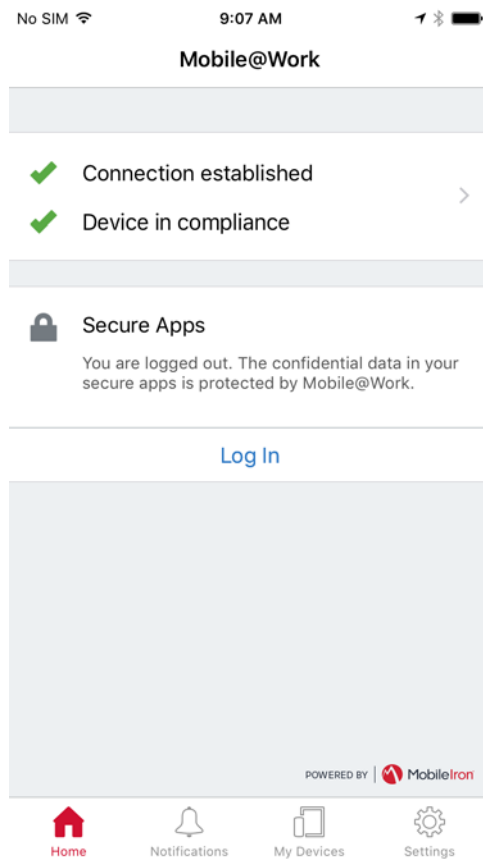
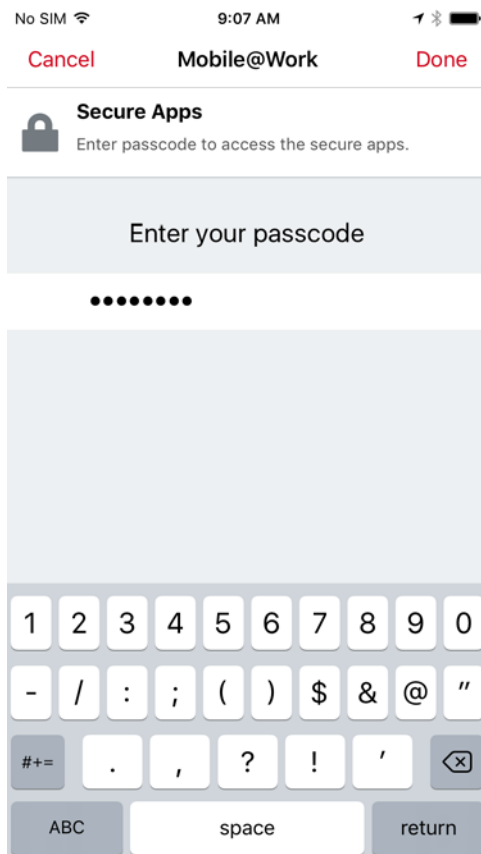


Figure 5-7 PIV-D Passcode Entry



5.2.1.2 Maintenance

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

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

5.2.1.3 Termination

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

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

Figure 5-8 DPC IdentityGuard Termination

The screenshot displays the Entrust IdentityGuard Administration web interface. At the top, the logo 'Entrust IdentityGuard Administration' is visible. Below it, a navigation bar shows the user 'Administrator: NCCoEadmin' and menu items: Home, User Accounts, Smart Credentials, and Policies. A breadcrumb trail indicates the current path: Go To Account > Find Accounts > Search Options > Search Results > View Account > Unapprove Smart Credential. The main content area is titled 'Unapprove a user's smart credential'. It contains a text block explaining the process: 'To unapprove the smart credential details for User Name asha in Group NCCoE Derived Credential Project with Smart Credential ID ET9925845, enter a reason for unapproving this smart credential in the comments field.' Below this is a 'Comments:' label and a large text input field containing the text 'Lost device.' At the bottom of the form are two buttons: 'Unapprove Smart Credential' and 'Cancel'.

5.2.1.4 Derived PIV Authentication Certificate Management

PKI management instructions between the Entrust IdentityGuard service and the Entrust Datacard Managed CA use a combination of the Public Key Infrastructure X.509—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 IETF, which standardizes many network-based protocols, in RFC 4210. 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 (PKCS) #10 format over PKIX-CMP. The Entrust Datacard Managed CA returns the signed DPC certificate to the Entrust IdentityGuard service.

5.2.2 Hybrid Architecture Build Testing

5.2.2.1 Initial Issuance

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

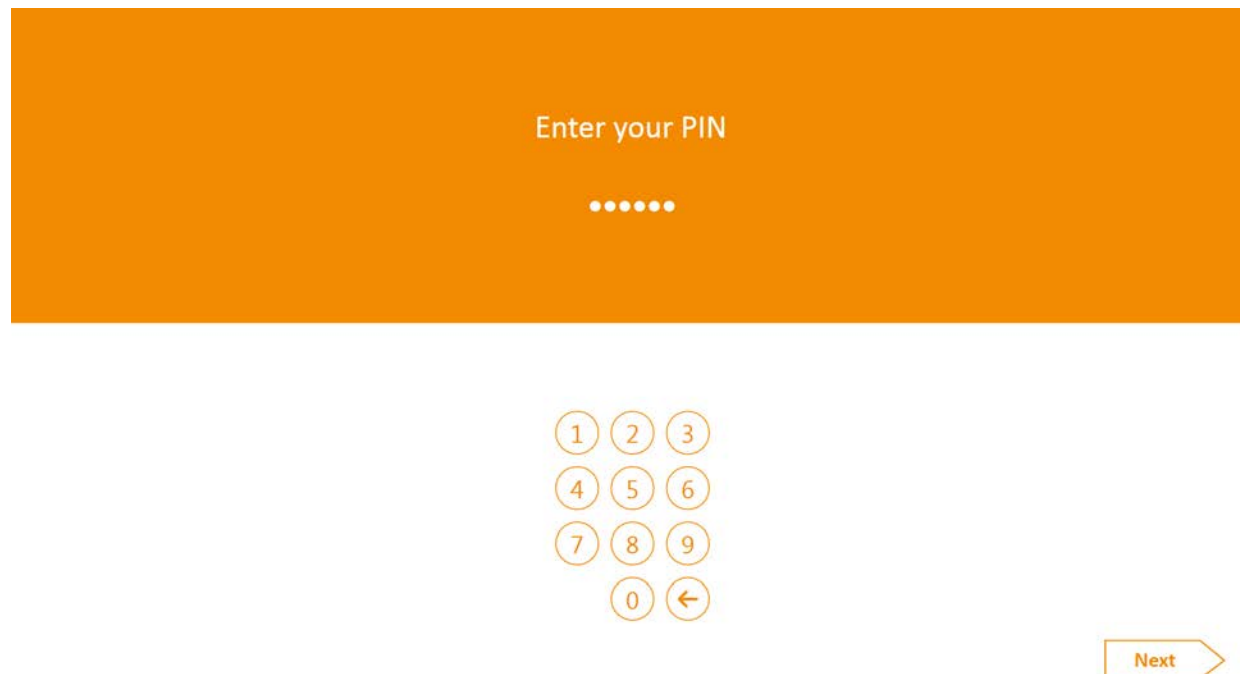
Figure 5-9 Test PIV Card User

Edit PIV Applicant

| Personal | Position | Biometrics | Application |
|---------------------------------------|------------------------------|-----------------------|--|
| Title: Mr | First Name: Matt | Middle Name: | Last Name: Steele |
| Nickname: | Suffix: | D. O. B.: 23 Feb 1976 | |
| Logon: 7654321 | Security: 7654321 | Enabled: Yes | Roles: Applicant, Derived Credential O |
| Group: Human Resources | Phone: 202-523-4567 | Fax: 202-623-4567 | |
| Email: demo@derivedpivcredentials.com | Cell: 0412345678 | | |
| Address 1: 28A Park Road | Address 2: Sunnydale Heights | | |
| City: Washington | State + Zip: DC 20223 | | |
| Card Issuance | | | |
| NACI Status: Waiting for Response | | | |
| User Data Approved: Yes | | | |

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

Figure 5-10 Kiosk Workflow

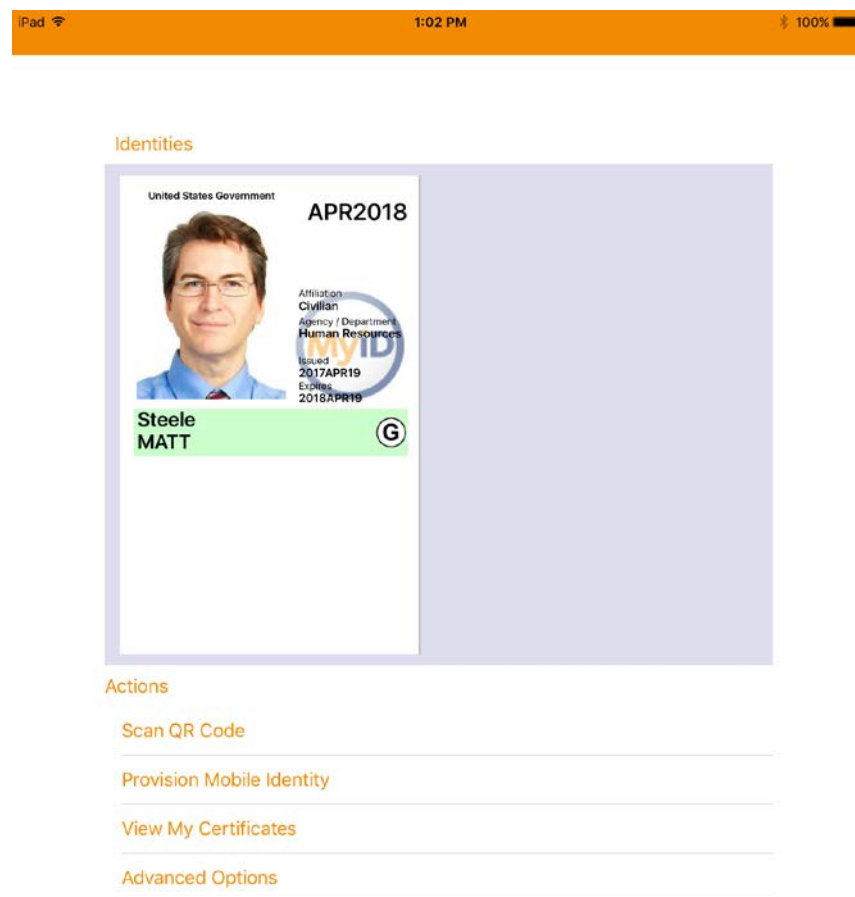


The DPC issuance process requires the use of the Identity Agent mobile application or the self-service application to complete the workflow. In the case of an iOS or Android-based mobile device, the applicant launches the Identity Agent application and scans a QR code presented by the self-service kiosk.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

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

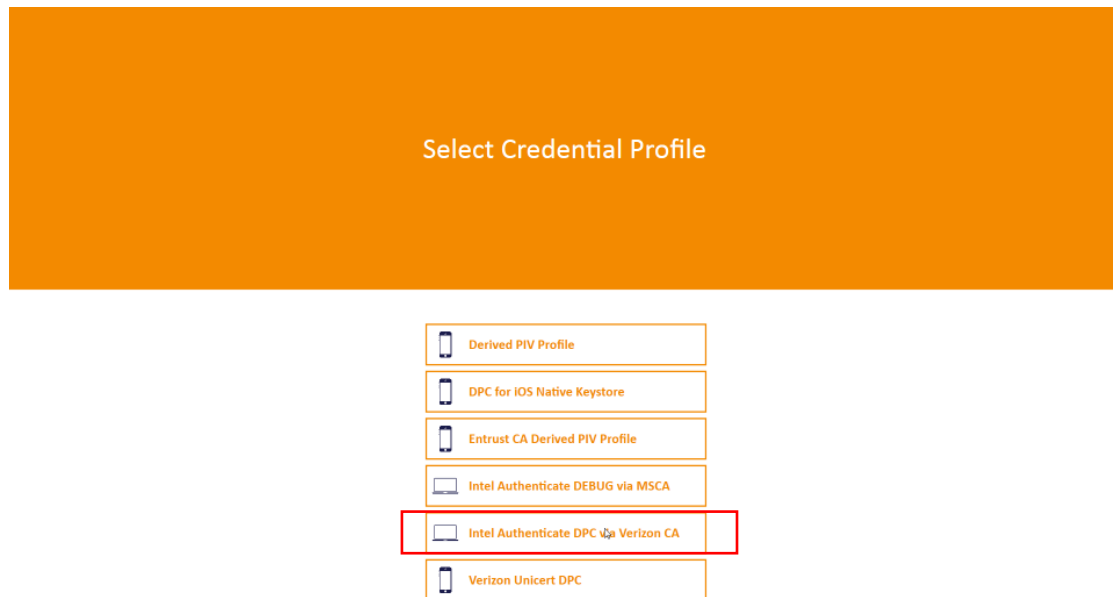
The DPC stored within the software container was protected with a PIN that can be configured to more complex schemes within the MyID Desktop console. A PIN is required before the certificate is delivered to the end point. The MyID Identity Agent mobile application displays a virtual image of the associated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

Figure 5-11 DPC in MyID Identity Agent



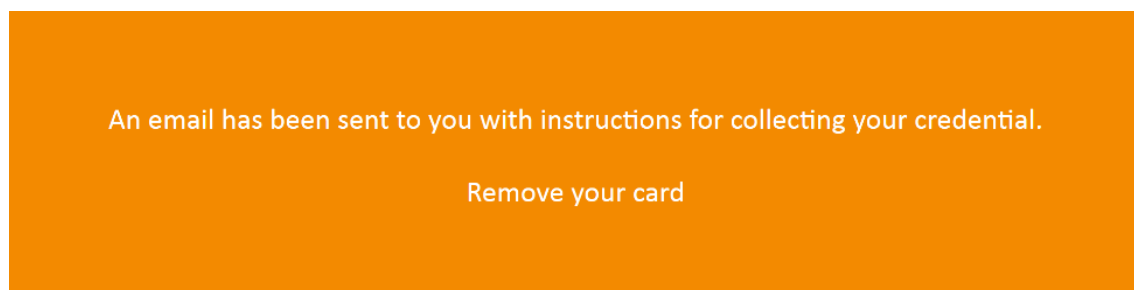
For Windows-based devices, the initial issuance process starts with the self-service kiosk, the same as for mobile devices. Figure 5-12 shows an example.

Figure 5-12 DPC Applicant Chooses Intel Credential Profile



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

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



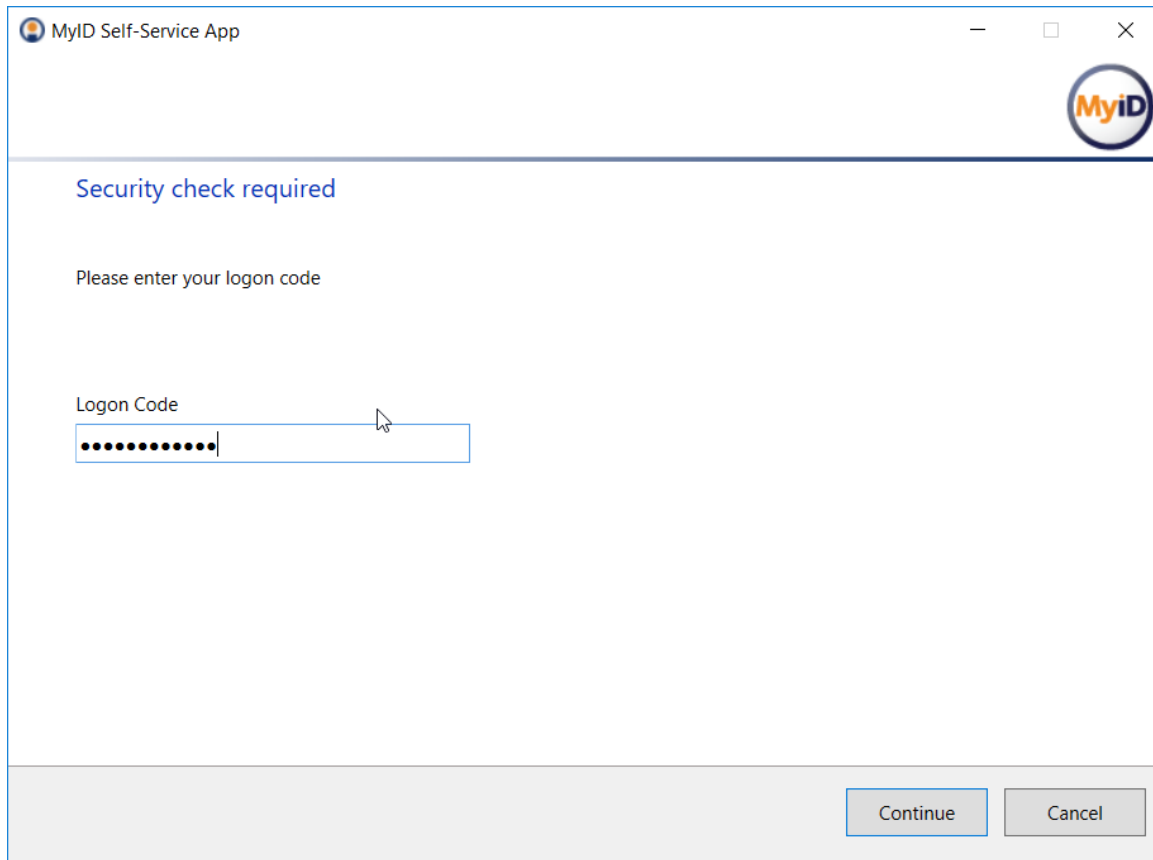
www.intercede.com



intercede

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

Figure 5-14 DPC Applicant Inputs the Onetime Code

The image shows a screenshot of a web application window titled "MyID Self-Service App". In the top right corner, there is a "MyiD" logo. The main content area has a heading "Security check required" in blue. Below this, it says "Please enter your logon code". There is a text input field labeled "Logon Code" which contains ten black dots, indicating a masked PIN. A mouse cursor is positioned over the input field. At the bottom right of the window, there are two buttons: "Continue" and "Cancel".

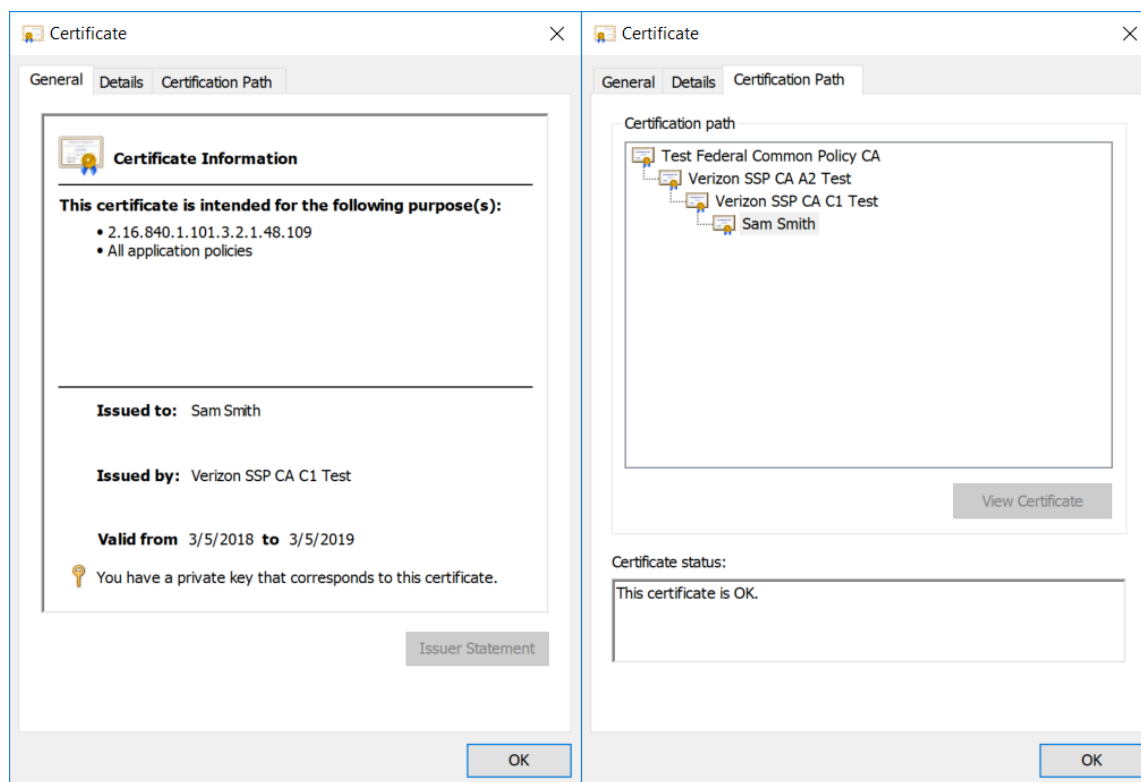
Once the DPC is issued to the Intel Authenticate token, it can be activated only by using a PIN set by the DPC applicant through the Intel Authenticate client (see Part C for details). The client allows the user to choose one or more additional *factors* to protect PKI-based keys; however, the PIN-based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

- Software-based screen scraping or malware attacks that attempt to perform a screen capture of the keypad cannot view the actual layout of the numbers. Instead, the entire keypad is blacked out.
- Each time the keypad window is presented, the numeric keypad is randomized. This means the locations used to enter the PIN change every time. An attacker that captures the PIN entry pattern for successful authenticator activation cannot use it for subsequent PIN entries.

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

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

Figure 5-15 Verizon SSP Derived PIV Authentication Certificate



5.2.2.2 Maintenance

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

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

5.2.2.3 Termination

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

5.2.2.4 Derived PIV Authentication Certificate Management

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

5.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference architectures address the security characteristics that they were intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to a Subcategory. The cited sections provide validation points that the example solutions would be expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference designs support the intended security characteristics.

Our reference architectures primarily support the Function known as Protect (PR) of the Cybersecurity Framework, which features Identity Management and Access Control (AC) as an outcome Subcategory. We discuss the associated Subcategories in the following subsections.

5.3.1 PR.AC-1: Identities and Credentials Are Issued, Managed, Verified, Revoked, and Audited for Authorized Devices, Users, and Processes

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

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

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

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

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

5.3.2 PR.AC-3: Remote Access Is Managed

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

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

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

5.3.4 PR.AC-7: Users, Devices, and Other Assets Are Authenticated (e.g., Single-Factor, Multifactor) Commensurate with the Risk of the Transaction (e.g., Individuals' Security and Privacy Risks and Other Organizational Risks)

To address the Function known as Protect, the [managed architecture with EMM integration](#) example implementation allows an organization to create a policy to lock and/or wipe the device after an organization-set number of unsuccessful authenticator unlock attempts. This results in the DPC becoming unusable until an administrator acts to either unlock the device or force reenrollment for the DPC.

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

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

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

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

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

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

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

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

5.4 Authenticator AAL Mapping

Based on NIST's [Digital Identity Guidelines](#), the strength of an authentication transaction is measured by the AAL. A higher AAL authenticator requires more resources and capabilities by attackers to subvert the authentication process. This DPC Project meets the requirements for the AAL-2 [software multifactor authenticator](#). Table 5-2 lists the authenticator requirements at AAL-2, which provide high confidence that the claimant controls the authenticator(s) bound to the subscriber's account and maps it to the corresponding requirement in NIST SP 800-157.

Table 5-2 AAL-2 Authenticator Requirements Mapping

| Requirement Identifier | NIST SP 800-63-3 Authenticator Requirement | NIST SP 800-157 Guideline |
|------------------------|--|--|
| 1 | Multifactor software cryptographic authenticators encapsulate one or more secret keys that are unique to the authenticator and are accessible only through the input of an additional factor—either a memorized secret or a biometric. | Use of the Derived PIV Authentication private key, or access to the plain text or wrapped private key, shall be blocked prior to password-based subscriber authentication. ... The required password length shall be at least six characters. |
| 2 | The key SHOULD be stored in suitably secure storage available to the authenticator application (e.g., key chain storage, Trusted Platform Module, Trusted Execution Environment). | Many mobile devices on the market provide a hybrid approach where the key is stored in hardware, but a software cryptographic module uses the key during an authentication operation. ... Therefore, the hybrid approach is recommended when supported by mobile devices and applications. |
| 3 | The key SHALL be strongly protected against unauthorized disclosure by access controls that limit access to the key to only those software components on the device requiring access. | No mapping exists. |
| 4 | Multifactor cryptographic software authenticators SHOULD discourage and SHALL NOT facilitate cloning of the secret key onto multiple devices. | For Derived PIV Authentication certificates issued under id-fpki-common-pivAuth-derived (LOA-3), the Derived PIV Authentication key pair shall be generated within a cryptographic module that has been validated to [FIPS 140] Level 1 or higher. |

| Requirement Identifier | NIST SP 800-63-3 Authenticator Requirement | NIST SP 800-157 Guideline |
|------------------------|--|---|
| 5 | Any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric value at least six decimal digits in length or other memorized secret meeting the requirements of Section 5.1.1.2 (Memorized Secret Verifiers). | Use of the Derived PIV Authentication private key or access to the plain text or wrapped private key shall be blocked prior to password-based subscriber authentication. ... The required password length shall be at least six characters. |
| 6 | Any memorized secret used by the authenticator for activation SHALL be rate limited as specified in Section 5.2.2 . | Throttling mechanisms may be used to limit the number of attempts that may be performed over a given period. |
| 7 | A biometric activation factor SHALL meet the requirements of Section 5.2.3 , including limits on the number of consecutive authentication failures. | Biometric activation is outside the bounds of NIST SP 800-157. |
| 8 | The unencrypted key and activation secret or biometric sample, and any biometric data derived from the biometric sample such as a probe produced through signal processing, SHALL be zeroized immediately after an authentication transaction has taken place. | No mapping exists. Biometric sample not collected for activation of the authenticator |

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

Table 5-3 AAL Technology Mappings for Authenticators Used

| Requirement Identifier | Authenticator | | |
|------------------------|---|--|---|
| | MobileIron Container Software Token | Intercede Container Software Token | Intel Authenticate |
| 1 | PIN required to activate token | PIN required to activate token | PIN required to activate token |
| 2 | Encrypted software container | Encrypted software container | Hardware/firmware protection |
| 3 | Authentication key available only to other MobileIron | Authentication key available only to other Intercede | Authentication key available for domain log-on and VPN with PIN |

| Requirement Identifier | Authenticator | | |
|------------------------|--|--|--|
| | MobileIron Container Software Token | Intercede Container Software Token | Intel Authenticate |
| | secure container applications with PIN | secure container applications with PIN | |
| 4 | No export mechanism available, and device encryption discourages cloning | No export mechanism available, and device encryption discourages cloning | Authentication key binds to unique hardware key |
| 5 | Configurable PIN length and complexity rules | Configurable PIN length and complexity rules | Configurable PIN length and complexity rules |
| 6 | Configurable PIN lock after failed attempts | Configurable PIN lock after failed attempts | Protected PIN input has built-in throttling mechanism. |
| 7 | Biometric activation is outside the bounds of NIST SP 800-157. | Biometric activation is outside the bounds of NIST SP 800-157. | Biometric activation is outside the bounds of NIST SP 800-157. |

6 Future Build Considerations

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

- **Application Enablement**—To leverage DPCs, 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 DPCs. Future work might focus on adopting native embedded cryptographic tokens provided by hardware manufacturers and on using federations for relying parties such as cloud service providers.
- **Architecture Expansion**—Integrate with an identity management system (IDMS), which [retains identity data that is retrieved from authoritative sources](#), to provide DPC subscriber PIV eligibility status information. NIST SP 800-157 recommends that the issuer of the DPC prevent further use of the DPC when the subscriber is no longer eligible for a PIV Card. Integration with an IDMS would store the eligibility of the DPC subscriber to help determine when DPC should be revoked, and it allows for DPC status to remain independent of the PIV Card status. This is

helpful in the case of lost or stolen cards to allow a DPC subscriber to keep working without a PIV Card.

- **Key Management (Encryption) Key Recovery**—Mobile users should be able to recover key management keys from escrow. Unlike a signature key, the same key management key that is stored on the PIV Card is necessary to decrypt encrypted email stored on the device, for example.

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

Appendix A List of Acronyms

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

| | |
|-----------------|---|
| LDAP | Lightweight Directory Access Protocol |
| LOA | Level of Assurance |
| microSD | Micro Secure Digital |
| MTC | Mobile Threat Catalogue |
| NCCoE | National Cybersecurity Center of Excellence |
| NFC | Near-Field Communication |
| NICE | National Initiative for Cybersecurity Education |
| NIST | National Institute of Standards and Technology |
| NVD | National Vulnerability Database |
| OCSP | Online Certificate Status Protocol |
| OS | Operating System |
| OTP | Onetime Password |
| PIN | Personal Identification Number |
| PIV | Personal Identity Verification |
| PKCS | Public Key Certificate Standard |
| PKI | Public Key Infrastructure |
| PKIX-CMP | Public Key Infrastructure X.509—Certificate Management Protocol |
| QR | Quick Response |
| RFC | Request for Comments |
| RMF | Risk Management Framework |
| SaaS | Software as a Service |
| SD | Secure Digital |
| SP | Special Publication |
| SQL | Structured Query Language |
| SSM | Self-Service Module |
| SSP | Shared Service Provider |
| TLS | Transport Layer Security |
| UICC | Universal Integrated Circuit Card |
| URL | Uniform Resource Locator |
| U.S. | United States |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |

| | |
|------------|-----------------------------|
| WAN | Wide Area Network |
| XAP | XML Administration Protocol |

Appendix B Glossary

All significant technical terms used within this document are defined in other key documents, including National Institute of Standards and Technology (NIST) Special Publication (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 DPCs are in this glossary.

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

| | |
|---|---|
| demilitarized zone | Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's information assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. |
| Derived PIV Application | A standardized application residing on a removable hardware cryptographic token that hosts a Derived PIV Credential and associated mandatory and optional elements |
| Derived PIV Credential | An X.509 Derived PIV Authentication certificate with associated public and private key that is issued in accordance with the requirements specified in this document where the PIV Authentication certificate on the applicant's PIV Card serves as the original credential. The Derived PIV Credential (DPC) is an additional common identity credential under Homeland Security Presidential Directive-12 and Federal Information Processing Standards (FIPS) 201 that is issued by a federal department or agency and is used with mobile devices. |
| e-authentication assurance level | <p>A measure of trust or confidence in an authentication mechanism defined in publications Office of Management and Budget (OMB)-04-04 and NIST SP 800-63 in terms of four levels:</p> <ul style="list-style-type: none"> ▪ 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 standard in FIPS covers a specific topic in information technology to achieve a common level of quality or some level of interoperability. |
| identity | The set of physical and behavioral characteristics by which an individual is uniquely recognizable |
| identity management system | One or more systems or applications that manage the identity verification, validation, and issuance process |
| identity proofing | The process of providing sufficient information (e.g., identity history, credentials, documents) to establish an identity |

| | |
|--|--|
| identity verification | The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those credentials previously proven and stored in the PIV Card or system and associated with the identity being claimed |
| issuer | The organization that is issuing the PIV Card (or DPC) to an applicant. Typically, this is an organization for which the applicant is working. |
| level of assurance | OMB Memorandum M-04-04 describes four levels of identity assurance and references NIST technical standards and guidelines, which are developed for agencies to use in identifying the appropriate authentication technologies that meet their requirements. |
| mobile device | A portable computing device that (1) has a small form factor so it can easily be carried by a single individual; (2) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (3) possesses local, nonremovable or removable data storage; and (4) includes a self-contained power source. Mobile devices may also include voice communication capabilities, onboard sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples are smartphones, tablets, and e-readers. |
| multifactor authentication | Authentication using two or more factors to achieve authentication. Factors are (i) something you know (e.g., password/personal identification number); (ii) something you have (e.g., cryptographic identification device, token); and (iii) something you are (e.g., biometric). |
| personal identification number | A secret number that a cardholder memorizes and uses to authenticate his or her identity as part of multifactor authentication |
| personal identity verification (card) | A physical artifact (e.g., identity card, “smart” card) issued to an individual, which contains a PIV Card application that stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human-readable and -verifiable) or an automated process (computer-readable and -verifiable) |
| PKI-PIV Authentication key (PKI-AUTH) | A PIV Authentication mechanism that is implemented by an asymmetric key challenge/response protocol by using the PIV Authentication key of the PIV Card and a contact reader or a contactless card reader that supports the virtual contact interface |

| | |
|----------------------------------|---|
| private key | The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data |
| public key | The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. |
| public key infrastructure | A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of enterprise data |
| sponsor | Submits a Derived PIV Credential request on behalf of the applicant |
| subscriber | The individual who is the subject named or identified in a Derived PIV Authentication certificate and who holds the token that contains the private key that corresponds to the public key in the certificate |

Appendix C National Institute of Standards and Technology (NIST) Internal Report 8055 [\[10\]](#) Requirements Enumeration and Implementation Mappings

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

| Regulatory Requirement | Req. Number | Req. Section Number | Requirement Name |
|------------------------|-------------|---------------------|---|
| | 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 |
| | RC1.14 | 2.3.5.3.1.6.1 | Removable hardware cryptographic tokens: Universal Integrated Circuit Card (UICC): separate security domain for Derived PIV Application |
| | RC1.15 | 2.3.5.3.1.6.2 | Removable hardware cryptographic tokens: UICC: NIST SP 800-157 Appendix B application protocol data unit (APDU) command interface |
| | RC1.16 | 2.3.5.3.1.6.3 | Removable hardware cryptographic tokens: UICC: <i>Global Platform Card Secure Element Configuration v1.0</i> |
| | RC1.17 | 2.3.5.3.1.7.1 | Removable hardware cryptographic tokens: Universal Serial Bus (USB) token with cryptographic module: integrated secure element with <i>Smart Card Integrated Circuit Card Devices Specification for USB Integrated Circuit Card Devices</i> |
| | 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 level of assurance (LOA)-3 |

| Regulatory Requirement | Req. Number | Req. Section Number | Requirement Name |
|-------------------------------------|-------------|---------------------|---|
| | 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 |
| | RC1.25 | 2.3.5.4.6 | Embedded cryptographic tokens: authentication mechanism implemented by hardware or software mechanism outside cryptographic boundary at LOA-3 |
| | RC1.26 | 2.3.5.4.7 | Implementation and enforcement of authentication mechanism by cryptographic module at LOA-4 |
| | RC1.27 | 2.3.5.4.10 | Support password reset per Appendix B of NIST SP 800-157 for removable token and new issuance of certificate for LOA-3 |
| RC2—PIV Card | RC2.1 | 2.3.1.4 | Identity proofing |
| | RC2.2 | 2.3.1.5 | Proof of possession of a valid PIV Card |
| | RC2.3 | 2.3.2.1 | Verification of applicant's PIV Authentication for issuance |
| | RC2.4 | 2.3.2.2 | Revocation status of PIV Authentication certificate checked after seven days of issuance |
| | RC2.5 | 2.3.2.10 | Issuance of multiple DPCs |
| RC3—Public Key Infrastructure (PKI) | RC3.1 | 2.3.1.3 | PKI-based DPC at LOA-3 and LOA-4 |
| | RC3.2 | 2.3.1.6 | X.509 public key certificate |
| | RC3.3 | 2.3.3.6 | Issuance of Derived PIV Authentication certificate because of subscriber name change |
| | RC3.4 | 2.3.5.1.2 | Worksheet 10: Derived PIV Authentication certificate profile found in <i>X.509 Certificate and Certificate Revocation List Profile for the Shared Service Providers Program</i> |

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

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

| Regulatory Requirement | Req. Number | Req. Section Number | Requirement Name |
|------------------------|-------------|---------------------|--|
| | 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 |
| | 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] Department of Homeland Security. *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*. [Online]. Available: <https://www.dhs.gov/homeland-security-presidential-directive-12>.
- [2] U.S. Department of Commerce, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Federal Information Processing Standards (FIPS) Publication 201-2, Aug. 2013. Available: <https://doi.org/10.6028/NIST.FIPS.201-2>.
- [3] National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. [Online]. Available: <https://www.nist.gov/cyberframework>.
- [4] Joint Task Force Transformation Initiative, *Risk Management Framework for Information Systems and Organizations*, NIST Special Publication (SP) 800-37 Revision 2, Gaithersburg, Md., Dec. 2018. Available: <https://doi.org/10.6028/NIST.SP.800-37r1>.
- [5] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 4, Gaithersburg, Md., Apr. 2013. Available: <https://doi.org/10.6028/NIST.SP.800-53r4>.
- [6] H. Ferraiolo et al., *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, NIST SP 800-157, Gaithersburg, Md., Dec. 2014. Available: <https://doi.org/10.6028/NIST.SP.800-157>.
- [7] P. Grassi et al., *Digital Identity Guidelines*, NIST SP 800-63-3, Gaithersburg, Md., June 2017. Available: <https://doi.org/10.6028/NIST.SP.800-63-3>.
- [8] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, NIST SP 800-181, Gaithersburg, Md., Aug. 2017. Available: <https://doi.org/10.6028/NIST.SP.800-181>.
- [9] NIST. *Mobile Threat Catalogue*. [Online]. Available: <https://pages.nist.gov/mobile-threat-catalogue/>.
- [10] M. Bartock et al., *Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research*, NIST Internal Report 8055, Gaithersburg, Md., Jan. 2016. Available: <https://doi.org/10.6028/NIST.IR.8055>.
- [11] IDManagement.gov. *Government Identity and Credentials*. [Online]. Available: <https://www.idmanagement.gov/trust-services/#gov-identity-credentials>.

- [12] “Derived Personal Identity Verification Credentials Building Block,” 80 *Federal Register* 157, Aug. 14, 2015. Available: <https://www.federalregister.gov/documents/2015/08/14/2015-20039/national-cybersecurity-center-of-excellence-derived-personal-identity-verification-credentials>.
- [13] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST SP 800-124 Revision 1, Gaithersburg, Md., June 2013. Available: <https://doi.org/10.6028/NIST.SP.800-124r1>.
- [14] OWASP. *Top 10 2014-I2 Insufficient Authentication/Authorization*. [Online]. Available: https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization.
- [15] Department of Homeland Security, *Study on Mobile Device Security*, Apr. 2017. Available: <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>.
- [16] Executive Order no. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017. Available: <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>.
- [17] M. Barrett et al., *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*, Draft, NIST Interagency Report 8170, Gaithersburg, Md., May 2017. Available: <https://csrc.nist.gov/publications/detail/nistir/8170/draft>.
- [18] C. Brown et al., *Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue*, Draft, NIST Interagency Report 8144, Gaithersburg, Md., Sept. 2016. Available: <https://csrc.nist.gov/publications/detail/nistir/8144/draft>.
- [19] NIST. National Vulnerability Database. [Online]. Available: <https://nvd.nist.gov/>.
- [20] NIST. CVE-2016-6716 Detail, National Vulnerability Database. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2016-6716>.
- [21] S. Quirolgico et al., *Vetting the Security of Mobile Applications*, NIST SP 800-163, Gaithersburg, Md., Jan. 2015. Available: <https://doi.org/10.6028/NIST.SP.800-163>.
- [22] The MITRE Corporation. Common Vulnerabilities and Exposures (CVE). [Online]. Available: <https://cve.mitre.org/>.
- [23] U.S. General Services Administration, *Decision for Standard Assessment & Authorization, Authorization to Operate Letter*, Nov. 3, 2016. Available: <https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/entrust-ato.pdf>.

- [24] E. Simmon, DRAFT—*Evaluation of Cloud Computing Services Based on NIST 800-145*, NIST SP 500-322, Gaithersburg, Md., Apr. 2017. Available:
https://www.nist.gov/sites/default/files/documents/2017/05/31/evaluation_of_cloud_computing_services_based_on_nist_800-145_20170427clean.pdf.
- [25] Federal Public Key Infrastructure Policy Authority, *X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework*, Version 1.24, May 7, 2015. Available:
<https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/Common-Policy-Framework.pdf>.
- [26] C. Adams et al., *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*, Internet Engineering Task Force Request for Comments 4210, Sept. 2005. Available:
<https://tools.ietf.org/html/rfc4210>.
- [27] T. Polk et al., *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, NIST SP 800-52 Revision 1, Gaithersburg, Md., Apr. 2014. Available:
<https://doi.org/10.6028/NIST.SP.800-52r1>.
- [28] Computer Security Division and Applied Cybersecurity Division, *Best Practices for Privileged User PIV Authentication*, NIST Cybersecurity White Paper, Gaithersburg, Md., Apr. 21, 2016. Available:
<https://doi.org/10.6028/NIST.CSWP.04212016>.