DISCLAIMER

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


FEEDBACK

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

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

Public comment period: September 29, 2017 through November 29, 2017

All comments are subject to release under the Freedom of Information Act (FOIA).
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Federal Information Processing Standards (FIPS) Publication 201-2, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” establishes a standard for a PIV system based on secure and reliable forms of identity credentials issued by the federal government to its employees and contractors. These credentials are intended to authenticate individuals who require access to federally controlled facilities, information systems, and applications. In 2005, when FIPS 201 was published, logical access was geared toward traditional computing devices (i.e., desktop and laptop computers) where the PIV card provides common multifactor authentication mechanisms through integrated smart card readers across the federal government. With the emergence of computing devices such as tablets, convertible...
computers, and in particular mobile devices, the use of PIV cards has proved challenging. Mobile devices lack the integrated smart card readers found in laptop and desktop computers and require separate card readers attached to devices to provide authentication services. To extend the value of PIV systems into mobile devices that do not have PIV Card readers, NIST developed technical guidelines on the implementation and lifecycle of identity credentials that are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV card. These NIST guidelines, published in 2014, describe Derived PIV Credentials (DPCs) which leverage identity proofing and vetting results of current and valid PIV credentials.

To demonstrate the DPCs guidelines, the National Cybersecurity Center of Excellence (NCCoE) at NIST built in its laboratory a security architecture using commercial technology to manage the lifecycle of DPCs demonstrating the process that enables a PIV Card holder to establish DPCs in a mobile device which then can be used to allow the PIV Card holder to access websites that require PIV authentication. This project resulted in a freely available NIST Cybersecurity Practice Guide which demonstrates how an organization can continue to provide two-factor authentication for users with a mobile device that leverages the strengths of the PIV standard. Although this project is primarily aimed at the Federal sector’s needs, it is also relevant to mobile device users with smart card based credentials in the private sector.

**KEYWORDS**

Cybersecurity; derived PIV credential (DPC); enterprise mobility management (EMM); identity; mobile device; mobile threat; (multifactor) authentication; network/software vulnerability; Personal Identity Verification (PIV); PIV card; smart card

**ACKNOWLEDGMENTS**

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Walter Holda</td>
<td>MobileIron</td>
</tr>
<tr>
<td>Loay Oweis</td>
<td>MobileIron</td>
</tr>
<tr>
<td>Sean Frazier</td>
<td>MobileIron</td>
</tr>
<tr>
<td>Dan Miller</td>
<td>Entrust Datacard</td>
</tr>
</tbody>
</table>
The technology vendors who participated in this build submitted their capabilities in response to a notice in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

<table>
<thead>
<tr>
<th>Technology Partner/Collaborator</th>
<th>Build Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entrust Datacard</td>
<td>Entrust IdentityGuard, Entrust Managed Services PKI</td>
</tr>
<tr>
<td>MobileIron</td>
<td>MobileIron Enterprise Mobility Management Platform</td>
</tr>
</tbody>
</table>

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

1 Introduction ........................................................................................................................................ 1
  1.1 Practice Guide Structure .............................................................................................................. 1
  1.2 Build Overview ............................................................................................................................ 2
  1.3 Typographical Conventions ......................................................................................................... 4

2 Product Installation Guides ............................................................................................................ 4
  2.1 Entrust Datacard IdentityGuard (IDG) ........................................................................................ 5
    2.1.1 Identity Management Profiles ............................................................................................... 6
  2.2 MobileIron Core .......................................................................................................................... 6
    2.2.1 Installation ............................................................................................................................. 6
    2.2.2 General MobileIron Core Set Up .......................................................................................... 7
    2.2.3 Configuration of MobileIron Core for DPC ......................................................................... 7
  2.3 DPC Lifecycle Workflows .......................................................................................................... 17
    2.3.1 DPC Initial Issuance .............................................................................................................. 17
    2.3.2 DPC Maintenance .................................................................................................................. 50
    2.3.3 DPC Termination ................................................................................................................... 50

List of Figures

82 Figure 1-1 Lab Network Diagram ...................................................................................................... 3
83 Figure 2-1 Build 1 Architecture ....................................................................................................... 5
84 Figure 2-2 MobileIron Registration Confirmation Page .................................................................. 23
85 Figure 2-3 Derived Mobile Smart Credential QR Code Activation Page ......................................... 47
1 Introduction

The following guides show IT professionals and security engineers how we implemented this example solution. We cover all of the products employed in this reference design. We do not recreate the product manufacturers’ documentation, which is presumed to be widely available. Rather, these guides show how we incorporated the products together in our environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

1.1 Practice Guide Structure

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate Derived Personal Identity Verification (PIV) Credential (DPC) lifecycle solution. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-12a: Executive Summary
- NIST SP 1800-12c: How-To Guides – instructions for building the example solution (you are here)

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

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

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

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

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

You might share the Executive Summary, NIST SP 1800-12a, with your leadership team members to help them understand the importance of adopting a standards-based Derived PIV Credential lifecycle solution.
IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, *NIST SP 1800-12c*, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers’ documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

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

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

### 1.2 Build Overview

Unlike desktop computers and laptops that have built-in readers to facilitate the use of PIV Cards, mobile devices pose usability and portability issues because of the lack of a smart card reader.

NIST sought to address this issue with the introduction of the general concept of Derived PIV Credentials in SP 800-63-2, which leverages identity proofing and vetting results of current and valid credentials. Published in 2014, SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* defined requirements for initial issuance and maintenance of Derived PIV Credentials. NIST’s Applied Cybersecurity Division then created a NCCoE project to provide an example solution for federal agencies and private entities that follows the requirements in SP 800-157.

In the NCCoE lab, the team built an environment that resembles an enterprise network using commonplace components such as identity repositories, supporting certificate authorities (CA), and web servers. In addition, products and capabilities were identified that, when linked together, provide an example solution that demonstrate lifecycle functions outlined in SP 800-157. Figure 1-1 depicts the final lab environment.
Figure 1-1 Lab Network Diagram
1.3 Typographical Conventions

The following table presents typographic conventions used in this volume.

<table>
<thead>
<tr>
<th>Typeface/ Symbol</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Italics</em></td>
<td>filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders</td>
<td>For detailed definitions of terms, see the NCCoE Glossary.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>names of menus, options, command buttons and fields</td>
<td>Choose File &gt; Edit.</td>
</tr>
<tr>
<td>Monospace</td>
<td>command-line input, on-screen computer output, sample code examples, status codes</td>
<td>mkdir</td>
</tr>
<tr>
<td>Monospace Bold</td>
<td>command-line user input contrasted with computer output</td>
<td>service sshd start</td>
</tr>
<tr>
<td>blue text</td>
<td>link to other parts of the document, a web URL, or an email address</td>
<td>All publications from NIST’s National Cybersecurity Center of Excellence are available at <a href="http://nccoe.nist.gov">http://nccoe.nist.gov</a></td>
</tr>
</tbody>
</table>

2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring of key products used for the depicted architecture illustrated below, as well as demonstration of the DPC lifecycle management activities of initial issuance and termination.

In our lab environment, the example solution was logically separated by a Virtual Local Area Network (VLAN) wherein each VLAN represented a mock enterprise environment. The network topology consists of an edge router connected to a Demilitarized Zone (DMZ). An internal firewall separates the DMZ from internal systems that support the enterprise. All routers and firewalls used in the example solution were virtual pfSense appliances.

As a basis, the enterprise network had an instance of Active Directory (AD) to serve as a repository for identities to support DPC vendors.
2.1 Entrust Datacard IdentityGuard (IDG)

Entrust Datacard contributed test instances of their managed Public Key Infrastructure (PKI) service and IdentityGuard products, the latter of which directly integrates with MobileIron to support the use of Derived PIV Credentials with MobileIron Mobile@Work apps. Contact Entrust Datacard ([https://www.entrust.com/contact/](https://www.entrust.com/contact/)) to establish service instances in support of a Derived PIV Credentials with MobileIron ([https://www.mobileiron.com/](https://www.mobileiron.com/)).
2.1.1 Identity Management Profiles

To configure services and issue certificates for Derived PIV Credentials that will work with your organization's user identity profiles, Entrust Datacard will need information on how identities are structured and which users will use PKI services. For this lab instance, Entrust Datacard issued PIV Authentication, Digital Signature, and Encryption certificates for PIV Cards and Derived PIV Credentials for two test identities, as represented below.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Email Address</th>
<th>User Principal Name (UPN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patel, Asha</td>
<td><a href="mailto:asha@entrust.dpc.nccoe.org">asha@entrust.dpc.nccoe.org</a></td>
<td><a href="mailto:asha@entrust.dpc.nccoe.org">asha@entrust.dpc.nccoe.org</a></td>
</tr>
<tr>
<td>Tucker, Matteo</td>
<td><a href="mailto:matteo@entrust.dpc.nccoe.org">matteo@entrust.dpc.nccoe.org</a></td>
<td><a href="mailto:matteo@entrust.dpc.nccoe.org">matteo@entrust.dpc.nccoe.org</a></td>
</tr>
</tbody>
</table>

2.2 MobileIron Core

MobileIron Core is the central product in the MobileIron suite. The following sections describe the steps for installation, configuration, and integration with Active Directory and the Entrust Datacard IdentityGuard cloud service. Key configuration files used in this build are listed below and are available from the NCCoE DPC project website.

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>core.dpc.nccoe.org-Default AppConnect Global Policy-2017-08-14 16-48-36.json</td>
<td>Configures policies such as password strength for the container</td>
</tr>
<tr>
<td>core.dpc.nccoe.org-Default Privacy Policy-2017-08-14 16-52-33.json</td>
<td>Configures privacy settings for each enrolled device</td>
</tr>
<tr>
<td>core.dpc.nccoe.org-DPC Security Policy-2017-08-14 16-51-07.json</td>
<td>Configures device level security management settings</td>
</tr>
<tr>
<td>shared_mdm_profile.mobileconfig</td>
<td>iOS MDM profile used when issuing DPCs to devices</td>
</tr>
</tbody>
</table>

2.2.1 Installation

Follow the steps below to install MobileIron Core:


2. Follow the MobileIron Core pre-deployment and installation steps in Chapter 1 of the *On-Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector* for the version of MobileIron being deployed in your environment. In our lab implementation, we deployed MobileIron Core 9.2.0.0 as a Virtual Core running on VMware 6.0.
2.2.2 General MobileIron Core Set Up

The following steps are necessary for mobile device administrators or users to register devices with MobileIron, which is a prerequisite to issuing Derived PIV Credentials.


2. Complete all instructions provided in Chapter 1, Setup Tasks.

2.2.3 Configuration of MobileIron Core for DPC

The following steps will reproduce this configuration of MobileIron Core.

2.2.3.1 Integration with Active Directory

In our implementation, we chose to integrate MobileIron Core with Active Directory using LDAP. This is optional. General instructions for this process are covered in the Configuring LDAP Servers section in Chapter 2 of On-Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector. The configuration details used during our completion of selected steps (retaining original numbering) from that guide are given below:

1. From Step 4 in the MobileIron guide, in the New LDAP Server dialog:

   a. Directory Connection:

   ![New LDAP Setting](image)
b. Directory Configuration - OUs:

New LDAP Setting - OUs

- OU Base DN: `dc=entrust,dc=dpc,dc=local`
- OU Search Filter: `((objectClass=organizationalUnit)(objectClass=container))`

210

c. Directory Configuration - Users:

New LDAP Setting - Users

- User Base DN: `dc=entrust,dc=dpc,dc=local`
- Search Filter: `(&(objectClass=user)(objectClass=person))`
- Search Scope: All Levels
- First Name: `givenName`
- Last Name: `sn`
- User ID: `sAMAccountName`
- Email: `mail`
- Display Name: `displayName`
- Distinguished Name: `distinguishedName`
- User Principal Name: `userPrincipalName`
- Locale: `c`

212

d. Directory Configuration - Groups:

New LDAP Setting - Groups

- User Group Base DN: `dc=entrust,dc=dpc,dc=local`
- Search Filter: `(objectClass=group)`
- Search Scope: All Levels
- User Group Name: `cn`
- Membership Attribute: `member`
- Member Of Attribute: `memberOf`
- Custom Attribute 1: 
- Custom Attribute 2: 
- Custom Attribute 3: 
- Custom Attribute 4: 
e. LDAP Groups:

i. As a prerequisite step, we used Active Directory Users and Computers to create a new security group for DPC-authorized users on the Domain Controller for the entrust.dpc.local domain. In our example, this group is named **DPC Users**.

ii. In the search bar, enter the name of the LDAP group for DPC-authorized users and click the **magnifying glass** button; the group name should be added to the **Available** list.

iii. In the **Available** list, select **DPC Users** and click the **right-arrow** button to move it to the **Selected** list.

iv. In the **Selected** list, select the default **Users** group and click the **left-arrow** button to move it to the **Available** list.

f. Custom Settings: custom settings were not specified.

g. Advanced Options:
Note: In our lab environment, we did not enable stronger Quality of Protection or enable the Use of
Client TLS Certificate or Request Mutual Authentication features. However, we recommend
implementers consider using those additional security mechanisms to secure communication with the
LDAP server.

2. From Steps 19-21 from the MobileIron guide, we tested that MobileIron can successfully query
LDAP for DPC Users.
   a. In the New LDAP Setting dialog, click the Test button to open the LDAP Test dialog.
   b. In the LDAP Test dialog, enter a User ID for a member of the DPC Users group then click
      the Submit button. A member of the DPC Users group in our environment is Matteo.
c. The **LDAP Test** dialog indicates the query was successful:
2.2.3.2 Create a DPC Users Label

MobileIron uses labels to link policies and device configurations with users and mobile devices. Creating a unique label for DPC users allows mobile device administrators to apply controls applicable to mobile devices provisioned with a derived credential specifically to those devices. We recommend applying DPC-specific policies and configurations to this label, in addition to any others appropriate to your organization's mobile device security policy.

1. In the **MobileIron Core Admin Portal**, navigate to Devices & Users > Devices.
2. Select **Advanced Search** (far right).

3. In the **Advanced Search** pane:
   a. In the blank rule:
      i. In the Field drop-down menu, select User > LDAP > Groups > Name.
      ii. In the Value drop-down menu, select the Active Directory group created to support DPC-specific MobileIron policies (named **DPC User** in this example).
   b. Select the **plus sign icon** to add a blank rule.
   c. In the newly created blank rule:
      i. In the Field drop-down menu, select Common > Platform.
      ii. In the Value drop-down menu, select iOS.
   d. Optionally, select **Search** to view matching devices.
   e. Select **Save to Label**.
f. In the Save to Label dialog:

i. In the Name field, enter a descriptive name for this label (DPC Users in this example).

ii. In the Description field, provide additional information to convey the purpose of this label.

iii. Click Save.
Navigate to Devices & Users > Labels to confirm the label was successfully created. It can be applied to Derived PIV Credential-specific MobileIron policies and configurations in future steps.

### 2.2.3.3 Implement MobileIron Guidance

The following provides the sections from the *MobileIron Derived Credentials with Entrust Guide* that were used in configuring this instance of MobileIron Derived PIV Credentials. Sections for which there may be configuration items tailored to a given instance (e.g., local system hostnames), this configuration is provided only as a reference. We noted any sections in which the steps performed to configure our systems varies from those in the *MobileIron Derived Credentials with Entrust Guide*.
Complete these sections in Chapter 2 of the *MobileIron Derived Credentials with Entrust Guide*:

1. Before beginning:
   a. Configuring certificate authentication to the user portal.  
      \textit{Note}: The root CA certificate or trust chain file can be obtained from Entrust Datacard.
      \textit{Note}: The URL will be specific to your organization’s instance of the IDG service and can be obtained from Entrust Datacard.

2. Configuring PIN-based registration.

3. Configuring user portal roles.

4. Adding the PIV-D Entrust app to the App Catalog.
   a. Adding Web@Work for iOS.

5. Configuring Apps@Work.
   a. Setting authentication options.
   b. Sending the Apps@Work web clip to devices.

   a. Configuring AppConnect licenses.
   b. Configuring the AppConnect global policy. The \textbf{AppConnect Passcode} policy settings for our implementation are presented below.
Note that based on our testing, a Passcode Strength of 61/100 or higher prevents easily guessable derived credential passcode combinations (e.g., abc123) from being set by a DPC Applicant.
7. Configuring the PIV-D Entrust app.

8. Configuring client-provided certificate enrollment settings. Note that the configuration items created by completing this section will be used in the following section. Replace Step 2 in this section of the MobileIron Derived Credentials with Entrust Guide with the following:

   a. Select Add New > Certificate Enrollment > SCEP.

9. Configuring Web@Work to use Derived PIV Credentials.

   a. Require a device password.

   b. Configure a Web@Work setting. The Custom Configurations key-value pairs set for our instance in Step 4 are presented below.

   Note: The value for idCertificate_1 is the descriptive name we applied to the Simple Certificate Enrollment Protocol (SCEP) certificate enrollment configuration for derived credential authentication created in the MobileIron Derived Credentials with Entrust Guide section referenced in Step 8.

<table>
<thead>
<tr>
<th>KEY</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>idCertificate_1_host</td>
<td>*</td>
</tr>
<tr>
<td>idCertificate_1</td>
<td>DC Authentication</td>
</tr>
</tbody>
</table>

2.3 DPC Lifecycle Workflows

The following sections describe how to perform the DPC lifecycle activities of issuance, maintenance, and termination.

2.3.1 DPC Initial Issuance

The following sections provide the steps necessary to issue a Derived PIV Credential onto a target mobile device.

2.3.1.1 Register Target Device with MobileIron

The following steps will register the target mobile device with MobileIron, which will create the secure Mobile@Work container into which a Derived PIV Credential is later provisioned.

1. Insert your valid PIV Card into the card reader attached to, or integrated into, your laptop or computer workstation.

2. Using a web browser, visit the MobileIron Self-Service Portal URL provided by your administrator.
3. In the MobileIron Self-Service Portal, click **Sign in with certificate**.

4. In the certificate selection dialog:
   a. If necessary, identify your PIV Authentication certificate:
      i. Highlight a certificate.
      ii. Select **Show Certificate**.
   iii. Navigate to the **Details** tab.
iv. The PIV Authentication certificate contains a **Field** named **Certificate Policies** with a **Value** that contains **Policy Identifier=2.16.840.1.101.3.2.1.3.13**.

v. Repeat **Steps** i-iii above as necessary.
b. Select your PIV Authentication certificate in the list of available certificates.

c. Click OK.

5. In the authentication dialog:

a. In the PIN field, enter your PIV Card PIN.

b. Click OK.
6. In the right-hand sidebar of the device summary screen, click Request Registration PIN.

7. In the Request Registration PIN page:
   a. Select iOS from the Platform drop-down menu.
   b. If your device does not have a phone number, check My device has no phone number.
   c. If your device has a phone number, enter it in the Phone Number field.
d. Click **Request PIN**.
The Confirmation page, shown in Figure 2-2 displays a unique device Registration PIN. Leave this page open while additional registration steps are performed on the target mobile device.

Note: This page may also facilitate the workflow for initial DPC issuance, covered in Section 2.3.1.2.

Figure 2-2 MobileIron Registration Confirmation Page
8. Using the target mobile device, launch the MobileIron **Mobile@Work** app.

9. In the request to grant MobileIron permission to receive push notifications, tap **Allow**.

10. In **Mobile@Work**:
    
    a. In the **User Name** field, enter your LDAP or MobileIron user ID.
    
    b. Tap **Next**.
c. In the **Server** field, enter the URL for your organization's instance of MobileIron Core as provided by a MobileIron Core administrator.

d. Tap **Next**.
e. In the PIN field, enter the Registration PIN displayed in the Confirmation page (see Figure 2-2) of the MobileIron Self-Service Portal at the completion of Step 7e.

f. Tap Go on keyboard or Register in Mobile@Work.
g. In the Privacy screen, tap **Continue**.
11. In the **Updating Configuration** dialog, tap **OK**; this will launch the built-in iOS **Settings** app.
12. In the **Settings** app, in the **Install Profile** dialog:

   a. In the **Signed By** field, confirm the originating server identity shows as **Verified**.

   **Note:** If verification of the originating server fails, contact your MobileIron administrator before resuming registration.

   b. Tap **Install**.
13. In the Enter **Passcode** dialog:

a. Enter your device unlock code.

b. Tap **Done**.
14. In the **Install Profile** dialog, tap **Install**.
15. In the **Warning** dialog, tap **Install**.
16. In the **Remote Management** dialog, tap **Trust**.
17. In the **Profile Installed** dialog, tap **Done**.

18. In the **App Management Change** dialog, tap **Manage**.
19. If additional Mobile@Work apps (e.g., Email+) are installed as part of the MobileIron management profile (based on your organization's use case), an **App Installation** dialog will appear for each app. To confirm, tap **Install**.
20. In the **Profile Installed** dialog, tap **Done**.
21. The **Mobile@Work > Home** screen should now display checkmarks for both status indicators of **Connection established** (with MobileIron Core) and **Device in compliance** (with the MobileIron policies that apply to your device).
2.3.1.2 DPC Initial Issuance

The following steps demonstrate how a DPC is issued to an applicant’s mobile device. It assumes the target mobile device is registered with MobileIron (see Register Target Device with MobileIron) and the MobileIron PIV-D Entrust app is installed (see Implement MobileIron Guidance). These steps are completed by the mobile device user who is receiving a DPC.

1. Launch the MobileIron PIV-D Entrust app on the target mobile device.

2. If a Mobile@Work Secure Apps passcode has not been set, you will be prompted to create one.
   In the Mobile@Work Secure Apps screen:
   a. In the Enter your new passcode field, enter a password consistent with your organization’s DPC password policy. This password will be used to activate your DPC (password-based Subscriber authentication) for use by Mobile@Work secure apps.

Note: NIST SP 800-63-3 increased the minimum DPC password length to eight characters.
b. In the **Re-Enter your new passcode** field, re-enter the password you entered in **Step 2b**.

c. Tap **Done**.
3. Following registration with MobileIron Core and when no Derived PIV Credential is associated with Mobile@Work, **PIV-D Entrust** displays a screen for managing your DPC. You will return to this app in a later step.
4. Insert your valid PIV Card into the reader attached to your laptop or computer workstation.
5. To request a Derived PIV Credential during the same session as registration with MobileIron:
   a. In the MobileIron Self-Service Portal **Confirmation** page (see Figure 2-2), click **Request Derived Credential**.

   ![MobileIron Self-Service Portal](image)

   b. In the certificate selection dialog:
      i. Select your PIV Authentication certificate from the list of available certificates. See **Step 4** of **Section 2.3.1.1** for additional steps to identify this certificate, as necessary.
      ii. Click OK.
      iii. Continue with **Step 7**.
6. To request a Derived PIV Credential in a new session:
   a. Using a web browser, visit the Entrust IDG Self-Service Portal URL provided by an administrator.
   b. In the Entrust IDG Self-Service portal, under **Smart Credential Log In**, click **Log In**.

   **Note:** The portal used in our test environment is branded as a fictitious company, AnyBank Self-Service.
c. In the **Select a certificate** dialog:
   
   i. Select your PIV Authentication certificate from the list of available certificates. See *Step 4* of *Section 2.1.3.1* for additional steps to identify this certificate, as necessary.
   
   ii. Click **OK**.
In the authentication dialog:

i. In the **PIN** field, enter the password to activate your PIV Card.

ii. Click **OK**.

7. On the **Self-Administration Actions** page, follow the **I'd like to enroll for a derived mobile smart credential** link (displayed below as the last item; this may vary based on which self-administration actions your Entrust IDG administrator enabled).
8. On the Smart Credential enabled Application page, select Option 2: I've successfully downloaded and installed the Smart Credential enabled application.

9. On the Derived Mobile Smart Credential page:
   a. In the Identity Name field, enter your LDAP or MobileIron user ID.
   b. Click OK.
10. The **Derived Mobile Smart Credential QR Code Activation** page displays information used in future steps; keep this page displayed. The workflow resumes using the MobileIron PIV-D Entrust app open on the target mobile device.

**Note:** Steps 11-13 must be completed using the target mobile device within approximately three minutes or Steps 7-10 must be repeated to generate new activation codes.

![Figure 2-3 Derived Mobile Smart Credential QR Code Activation Page](image)

11. In the **PIV-D Entrust** app running on the target mobile device, tap **Activate New Credential**.
12. Use the device camera to capture the QR code displayed on the Derived Mobile Smart Credential QR Code Activation page as represented in Figure 2-3.
13. On the **Activate Credential** screen:

   a. Enter the **password** below the QR code displayed on the **Derived Mobile Smart Credential QR Code Activation** page (displayed by the same device used to perform Steps 4-10) as represented in Figure 2-3.

   b. Tap **Activate**.

14. If issuance was successful, the PIV-D Entrust app should automatically launch MobileIron. Go to **Mobile@Work > Settings > Entrust Credential** to view its details.
2.3.2 DPC Maintenance

Changes to a DPC Subscriber’s PIV Card that result in a re-key or reissuance (e.g., official name change) require the subscriber to repeat the initial issuance workflow as described in the previous section. The issued DPC will replace any existing DPC in the MobileIron Apps@Work container.

2.3.3 DPC Termination

Termination of a DPC can be initiated from the MobileIron Admin Console. Upon completion of this workflow, the DPC stored in the MobileIron Apps@Work container will be cryptographically wiped (destroyed). These steps are performed by a MobileIron Core administrator.

1. In the MobileIron Admin Console, navigate to Devices & Users > Devices.
2. Select the checkbox in the row identifying the mobile device to be retired.

3. Select Actions > Retire.
4. In the **Retire** dialog that appears:
   a. In the **Note** textbox, enter the reason(s) the device is being retired from MobileIron.
   b. Select **Retire**.

5. The **Devices** tab no longer displays the retired mobile device in the list of the devices.

The MobileIron PIV-D Entrust app now no longer reflects management by MobileIron. As a result, the Derived PIV Credential has been cryptographically wiped (destroyed) and its recovery is computationally infeasible.
## Appendix A  List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CAPI</td>
<td>Cryptographic Application Programming Interface</td>
</tr>
<tr>
<td>CMS</td>
<td>Credential Management System</td>
</tr>
<tr>
<td>CRADA</td>
<td>Cooperative Research and Development Agreement</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>DN</td>
<td>Distinguished Name</td>
</tr>
<tr>
<td>DPC</td>
<td>Derived PIV Credential</td>
</tr>
<tr>
<td>EEM</td>
<td>Enterprise Mobility Management</td>
</tr>
<tr>
<td>FASC-N</td>
<td>Federal Agency Smart Card Number</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>IDG</td>
<td>Identity Guard</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>JCE</td>
<td>Java Cryptography Extension</td>
</tr>
<tr>
<td>JTK</td>
<td>Java Tool Kit</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>NCCoE</td>
<td>National Cybersecurity Center of Excellence</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit</td>
</tr>
<tr>
<td>PFX</td>
<td>Personal Exchange Format</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identity Verification</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>QR</td>
<td>Quick Response [code]</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest-Shamir-Adleman</td>
</tr>
<tr>
<td>SCEP</td>
<td>Simple Certificate Enrollment Protocol</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSM</td>
<td>Self-Service Module</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>UPN</td>
<td>User Principal Name</td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator</td>
</tr>
<tr>
<td>UUID</td>
<td>Universal Unique Identifier</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
</tbody>
</table>