DISCLAIMER

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


FEEDBACK

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

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

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

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

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

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

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

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

**KEYWORDS**

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

**ACKNOWLEDGMENTS**

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

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:

<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 Public Key Infrastructure (PKI)</td>
</tr>
<tr>
<td>Intel Corporation</td>
<td>Intel Authenticate Solution</td>
</tr>
<tr>
<td>Intercede</td>
<td>MyID Credential Management System</td>
</tr>
<tr>
<td>MobileIron</td>
<td>MobileIron Enterprise Mobility Management (EMM) Platform</td>
</tr>
<tr>
<td>Verizon</td>
<td>Verizon Shared Service Provider (SSP) PKI</td>
</tr>
</tbody>
</table>
## Table of 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 Managed Service Architecture with Enterprise Mobility Management (EMM)
      Integration ............................................................................................................................... 5
      2.1.1 Entrust Datacard IdentityGuard (IDG) ........................................................................ 5
      2.1.2 MobileIron Core ......................................................................................................... 6
      2.1.3 DPC Lifecycle Workflows ......................................................................................... 17
   2.2 Hybrid Architecture for PIV and DPC Life-Cycle Management ........................................... 52
      2.2.1 Intercede MyID CMS ................................................................................................. 53
      2.2.2 Intercede MyID Identity Agent .................................................................................. 63
      2.2.3 Intercede Desktop Client ......................................................................................... 63
      2.2.4 Intercede Self-Service Kiosk .................................................................................... 64
      2.2.5 Windows Client Installation for MyID and Intel Authenticate ..................................... 66
      2.2.6 Intel Authenticate GPO ............................................................................................ 82
      2.2.7 Intel VSC Configuration ......................................................................................... 119
      2.2.8 DPC Lifecycle Workflows ....................................................................................... 131

3. **Appendix A** List of Acronyms ............................................................................................. 143
List of Figures

22 Figure 1-1 Lab Network Diagram ........................................................................................................3
24 Figure 2-1 Architecture.........................................................................................................................5
25 Figure 2-2 MobileIron Registration Confirmation Page ......................................................................23
26 Figure 2-3 Derived Mobile Smart Credential QR Code Activation Page ...............................................46
27 Figure 2-4 Mobile Device Hybrid Architecture for PIV Card and DPC Lifecycle Management (Software Keystore) .........................................................................................................................................52
29 Figure 2-5 Mobile Device Hybrid Architecture for PIV Card and DPC Lifecycle Management (Intel Authenticate) ..................................................................................................................................................................................53
31 Figure 2-6 Certificate Profile Attributes .............................................................................................58

List of Tables

33 Table 2-1 Identity Management Profiles .............................................................................................6
34 Table 2-2 MobileIron Core Settings .....................................................................................................6
35 Table 2-3 SQL Server Components ....................................................................................................54
1 Introduction

This guide shows information technology (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, this guide shows 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 National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate a Derived Personal Identity Verification (PIV) Credential (DPC) life-cycle solution. This reference design is modular and can be deployed in whole or in part.

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 following topics:

- challenges enterprises face in issuing strong, multifactor credentials to mobile devices
- the 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 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 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 DPC solution.
IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-12C*, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the 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 the DPC example solution. 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. Vol B, Section 3.6, Technologies, lists the products that 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 DPC in Special Publication (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 DPC. NIST’s Applied Cybersecurity Division then created a National Cybersecurity Center of Excellence (NCCoE) project to provide an example implementation 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 by 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 demonstrates life-cycle 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>file names and path names; references to documents that are not hyperlinks; new terms; and placeholders</td>
<td>For detailed definitions of terms, see the <em>NCCoE Glossary</em>.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>names of menus, options, command buttons, and fields</td>
<td>Choose <em>File &gt; Edit</em>.</td>
</tr>
<tr>
<td><em>Monospace</em></td>
<td>command-line input, on-screen computer output, sample code examples, and status codes</td>
<td><code>mkdir</code></td>
</tr>
<tr>
<td><em>Monospace Bold</em></td>
<td>command-line user input contrasted with computer output</td>
<td><code>service sshd start</code></td>
</tr>
<tr>
<td><em>blue text</em></td>
<td>link to other parts of the document, a web URL, or an email address</td>
<td>All publications from NIST’s NCCoE are available at <code>https://www.nccoe.nist.gov</code></td>
</tr>
</tbody>
</table>

2 Product Installation Guides

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

In our lab environment, each example implementation was logically separated by a Virtual Local Area Network (VLAN), where 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 implementations 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 Managed Service Architecture with Enterprise Mobility Management (EMM) Integration

Figure 2-1  Architecture

Entrust Datacard IdentityGuard (IDG)

Entrust Datacard contributed test instances of its managed public key infrastructure (PKI) service and IdentityGuard products, the latter of which directly integrates with MobileIron to support the use of DPC with MobileIron Mobile@Work applications. Contact Entrust Datacard (https://www.entrust.com/contact/) to establish service instances in support of DPC with MobileIron (https://www.mobileiron.com/).
2.1.1 Identity Management Profiles

To configure services and issue certificates for DPC 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 DPC for two test identities, as represented in Table 2-1.

<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>

2.1.2 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 managed service. Key configuration files used in this build are listed in Table 2-2 and are available from the NCCoE DPC project website.

<table>
<thead>
<tr>
<th>File Name</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>shared_mdm_profile.mobileconfig</td>
<td>iOS MDM profile used when issuing DPC to devices</td>
</tr>
</tbody>
</table>

2.1.2.1 Installation

Follow the steps below to install MobileIron Core:

2. Follow the MobileIron Core pre-deployment and installation steps in Chapter 1 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.
2.1.2.2 General MobileIron Core Setup

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


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

2.1.2.3 Configuration of MobileIron Core for DPC

The following steps will reproduce this configuration of MobileIron Core.

2.1.2.3.1 Integration with Active Directory

In our implementation, we chose to integrate MobileIron Core with Active Directory by using Lightweight Directory Access Protocol (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 dialogue:

   a. Directory Connection:
b. Directory Configuration—OUs:

New LDAP Setting

Directory Configuration - OUs

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

d. Directory Configuration—Groups:

New LDAP Setting

Directory Configuration - Groups

User Group Base DN: dc=enttrust,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:

![New LDAP Setting dialogue](image)

Note: In our lab environment, we did not enable stronger Quality of Protection or enable the Use Client TLS Certificate or Request Mutual Authentication features. However, we recommend that implementers consider using those additional security mechanisms to secure communications 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** dialogue, click the **Test** button to open the **LDAP Test** dialogue.
   b. In the **LDAP Test** dialogue, 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** dialogue indicates the query was successful:
2.1.2.3.2 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 relevant for 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 Users 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** dialogue:
   
   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**.
4. Navigate to Devices & Users > Labels to confirm that the label was successfully created. It can be applied to DPC-specific MobileIron policies and configurations in future steps.

2.1.2.3.3 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 DPC. For 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 vary 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:
   - Configuring certificate authentication to the user portal
     Note: The root CA certificate or trust chain file can be obtained from Entrust Datacard.
   - Configuring the Entrust IdentityGuard Self-Service Module (SSM) Universal Resource Locator (URL).
     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
   - Adding Web@Work for iOS

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

6. Configuring AppConnect
   - Configuring AppConnect licenses
   - Configuring the AppConnect global policy. The **AppConnect Passcode** policy settings for our implementation are presented below.
Note: 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 step:
   a. Select Add New > Certificate Enrollment > SCEP.

9. Configuring Web@Work to use DPC:
   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>

2.1.3 DPC Lifecycle Workflows

This section describes how to perform the DPC lifecycle activities of initial issuance, maintenance, and termination.

2.1.3.1 DPC Initial Issuance

This section provides the steps necessary to issue a DPC onto a target mobile device.

2.1.3.1.1 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 DPC 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 dialogue:

   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 dialogue:
   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.
e. 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 2.1.3.1.2.

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

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**.
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.

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

   a. In the **Signed By** field, confirm that 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** dialogue:
   a. Enter your device unlock code.
   b. Tap **Done**.
14. In the **Install Profile** dialogue, tap **Install**.
15. In the Warning dialogue, tap Install.
16. In the **Remote Management** dialogue, tap **Trust**.

Note: The root certificate presented in this step may vary based on the CA used to sign the MDM profile. This build uses the [Let’s Encrypt](https://letsencrypt.org) certificate authority.
17. In the **Profile Installed** dialogue, tap **Done**.

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

   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 DPC is associated with Mobile@Work, *PIV-D Entrust* displays a screen for managing your DPC. You will return to this application in a later step.

4. Insert your valid PIV Card into the reader attached to your laptop or computer workstation.
To request a DPC 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 dialogue:

i. Select your PIV Authentication certificate from the list of available certificates. See Step 4 of Section 2.1.3.1.1 for additional steps to identify this certificate, as necessary.

ii. Click OK.

iii. Continue with Step 6.
To request a DPC 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 dialogue:
   i. Select your PIV Authentication certificate from the list of available certificates. See Step 4 of Section 2.1.3.1.1 for additional steps to identify this certificate, as necessary.
   ii. Click OK.
d. In the authentication dialogue:

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).

![Self-Administration Actions](image1)

- I'd like to update my personal information.
- I'd like to request a grid.
- I'd like to change my Entrust IdentityGuard password.
- I've forgotten my Entrust IdentityGuard password.
- I'd like to request a soft token.
- I'd like to unblock my smart credential.
- I've permanently lost my smart credential or it has been compromised.
- I've temporarily forgotten or misplaced my smart credential.
- I'd like to enroll for a derived mobile smart credential.

![Done](image2)

8. On the **Smart Credential enabled Application** page, select **Option 2: I've successfully downloaded and installed the Smart Credential enabled application**.

![Smart Credential enabled Application](image3)

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 application that is open on the target mobile device.

Note: Steps 11–13 must be completed by using the target mobile device within approximately three minutes, otherwise Steps 7–10 must be repeated to generate new activation codes.

11. In the **PIV-D Entrust** application that is 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 that is 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 application should automatically launch Mobile-Iron. Go to **Mobile@Work > Settings > Entrust Credential** to view its details.
2.1.3.2 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.

2.1.3.3 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 check box in the row identifying the mobile device to be retired.

3. Select Actions > Retire.
4. In the **Retire** dialogue that appears:
   a. In the **Note** text box, 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 application now no longer reflects management by MobileIron. As a result, the DPC has been cryptographically wiped (destroyed) and its recovery is computationally infeasible.
2.2 Hybrid Architecture for PIV and DPC Life-Cycle Management

This section describes the installation and configuration of key products for the architecture depicted in Figure 2-4 and Figure 2-5, as well as demonstration of the DPC lifecycle management activities of initial issuance and termination. Figure 2-4 focuses on the mobile device implementation. Here, the Identity Agent application is used to manage the DPC. The DPC authentication key is stored in a software keystore within the secure container. The supporting cloud and enterprise systems as described above are also shown. Figure 2-5 Error! Reference source not found. depicts the architecture when an Intel-based device that supports Intel Authenticate is used to store the DPC.

Figure 2-4 Mobile Device Hybrid Architecture for PIV Card and DPC Lifecycle Management (Software Keystore)
2.2.1 Intercede MyID CMS

Intercede offers its identity and credential management system (CMS) product, MyID, as a software solution that can be hosted in the cloud or deployed on premises. The MyID server platform is composed of an application server, database, and web server. It provides connectors to infrastructure components such as directories and PKIs, and application programming interfaces to enable integration with the organization’s identity and access management system. The MyID CMS is the core component for the architecture; as such, it should be fully configured and operational before other components.
2.2.1.1 Installation

Detailed instructions to install an instance of the MyID CMS are in the Intercede document *MyID Version 10.8 Installation and Configuration Guide*. Here, we document specific installation instructions for our environment.

The MyID system is modularly designed with web, application, and database tiers. In a production environment, it is likely that these tiers are separated onto multiple systems depending on performance and disaster recovery requirements. However, in our architecture, all tiers were installed on a Windows Server 2012 system due to resource constraints. Finally, role separation within the MyID system is not addressed here but should be considered before any deployment.

1. Install a supported version of Microsoft Structured Query Language (SQL) Server on the target MyID server. Our environment uses SQL Server 2012 with the SQL Server Database Engine and SQL Server Management Tools. See Components for specific component versions. A full settings document (*Exported-2017-07-27.vssettings*) is available from the NCCoE DPC project website. Refer to [Microsoft’s online documentation](https://docs.microsoft.com) for specific installation procedures.

Table 2-3 SQL Server Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server Management Studio</td>
<td>11.0.5058.0</td>
</tr>
<tr>
<td>Microsoft Analysis Services Client Tools</td>
<td>11.0.5058.0</td>
</tr>
<tr>
<td>Microsoft Data Access Components (MDAC)</td>
<td>6.3.9600.17415</td>
</tr>
<tr>
<td>Microsoft Extensible Markup Language (MSXML)</td>
<td>3.0 6.0</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>9.11.9600.18739</td>
</tr>
<tr>
<td>Microsoft .NET Framework</td>
<td>4.0.30319.42000</td>
</tr>
<tr>
<td>Operating System (OS)</td>
<td>6.3.9600</td>
</tr>
</tbody>
</table>

2.2.1.2 Verizon Shared Service Provider (SSP) PKI Integration

Detailed instructions to integrate Verizon SSP with MyID are in Intercede’s *UniCERT UPI Certificate Authority Integration Guide*. Here, we document the specific configurations used within our builds.

1. Install the following prerequisites on the MyID server:

<table>
<thead>
<tr>
<th>Component</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java Runtime Environment 8.0</td>
<td>Download and install the latest update from the Oracle website. This build uses 8u121.</td>
</tr>
<tr>
<td>Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8</td>
<td>Download and install from the Oracle website.</td>
</tr>
</tbody>
</table>

2. Obtain the following configuration settings from your managed PKI instance:
3. Create a CA configuration by using the following procedures:

a. In MyID Desktop, select the Configuration category.

b. Select Certificate Authorities from the Configuration menu.

c. Select New from the Select a CA drop-down menu.

d. From the CA Type drop-down menu, select Entrust JTK. A form with a setting specifically for the Entrust Datacard CA will appear.

e. Fill in the Certificate Authority form with the following settings from Step 2:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verizon SSP CA Path</td>
<td>Distinguished name to directory instance supplied by Verizon</td>
</tr>
<tr>
<td>Verizon SSP Enrollment Agent</td>
<td>Distinguished name for the Registration Authority supplied by Verizon</td>
</tr>
<tr>
<td>Verizon SSP Service Point</td>
<td>URI endpoint of the Verizon SSP web service supplied by Verizon</td>
</tr>
<tr>
<td>Verizon SSP Registration Authority Operator PKCS#12</td>
<td>Credentials are supplied by Verizon SSP</td>
</tr>
<tr>
<td>Verizon SSP Registration Authority Operator PKCS#12 Password</td>
<td></td>
</tr>
</tbody>
</table>
4. Enable Verizon SSP CA policies by using the following procedures.
   
a. Within MyID Desktop, click the Configuration category and choose Certificate Authorities.
   
b. From the CA Name drop-down, select the Verizon SSP CA configured in Step 3.
   
c. Click Edit.
   
d. In the Available Certificates list, select PIV-SSP-Derived-Auth-sw-1yr-v3 to enable it for DPC issuance.
   
e. Click the Enabled (Allow Issuance) check box.
f. Set the following options for the policy.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Arbitrary name for this policy</td>
</tr>
<tr>
<td>Description</td>
<td>Optional description for this policy</td>
</tr>
<tr>
<td>Allow Identity Mapping</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Reverse DN</td>
<td>Checked</td>
</tr>
<tr>
<td>Archive Keys</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Certificate Lifetime</td>
<td>365</td>
</tr>
<tr>
<td>Automatic Renewal</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Certificate Storage</td>
<td>Both</td>
</tr>
<tr>
<td>Recovery Storage</td>
<td>Both</td>
</tr>
<tr>
<td>CSP Name</td>
<td>Microsoft Enhanced Cryptographic Provider 1.0</td>
</tr>
<tr>
<td>Requires Validation</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Private Key Exportable</td>
<td>Unchecked</td>
</tr>
<tr>
<td>User Protected</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Key Algorithm</td>
<td>RSA 2048</td>
</tr>
<tr>
<td>Key Purpose</td>
<td>Signature</td>
</tr>
</tbody>
</table>

g. Click **Edit Attributes** and set the following values:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NACI Indicator</td>
<td>Dynamic</td>
<td>NACI Status</td>
</tr>
<tr>
<td>Subject Alt Microsoft UPN</td>
<td>Dynamic</td>
<td>User Principal Name</td>
</tr>
<tr>
<td>Subject Alt Uniform Resource Identifier</td>
<td>Dynamic</td>
<td>UUID</td>
</tr>
</tbody>
</table>
5. Repeat Step 4 for the PIV-Auth-1-yr-v2, PIV-CardAuth-1yr-v1, and PIV-Sig-1yr-v1 certificate profiles.
2.2.1.3 Configuration for DPC

Detailed instructions to configure an instance of the MyID CMS for DPC are in Intercede’s Derived Credentials Installation and Configuration Guide. Here, we document the specific configurations used within our builds. Before you begin, you need the Test Federal Common Policy CA root certificate file, which can be downloaded from the Federal PKI test repository. Also obtain the intermediate certificates for the Verizon SSP certificate chain (Verizon SSP CA A2 Test and Verizon SSP CA C1 Test) from the Verizon certificate test repositories.

The first step in configuration is to create a content signing certificate that is used to sign data stored on the DPC mobile container. This certificate (and associated private key) must be made available to MyID through the Windows Cryptographic Application Interface (CAPI) store on the same server where the MyID server is installed. There are various ways to generate a certificate; in our environment we chose to create a certificate authority on a separate instance of Windows Server 2012.

1. Install Microsoft Certificate Services. There are a few online resources that can assist in the installation process. We suggest the Adding Active Directory Certificate Services to a Lab Environment tutorial from the Microsoft Developer Network.

   a. Add a certificate template. For reference, we have exported the certificate template (PIVContentSigning) that we used for the content signing certificate. The configuration file (CertificateTemplates.xml) is available for download from the NCCoE DPC project website. A script to import the certificate template can be found at the Microsoft Script Center.

2. Request a content signing certificate from the MyID system by using the procedures noted in the “Request a Certificate” TechNet article.

3. Save the content signing certificate in binary format to the Components folder of the MyID installation folder.

4. Edit the system registry with the following procedures:

   a. From the Start menu:

      i. Select Run.

      ii. Type regedit in the dialogue displayed.

      iii. Click OK.

   b. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\ContentSigning.
c. Check that the value of the following string is set:

   **Active** – set to **WebService**.

d. Set the value of the following string to the full path of the certificate on the application server:

   For example: `C:\Program Files (x86)\Intercede\MyID\Components\contentcert.cer`

5. Set the location of the MyID web service that allows a mobile device to collect the DPC by using the following procedures within MyID Desktop:

   a. From the **Configuration** category, select the **Operation Settings** workflow.

   b. Click the **Certificates** tab.

   c. Set the **Mobile Certificate Recovery Service URL** option to the location of the MyID Process Driver web service host.

      For example: `https://<replace-with-your-hostname>`

   d. Click **Save Changes**.

6. Set which PIV Cards are available for DPC by using the following procedures within MyID Desktop:

   a. From the **Configuration** category, select the **Operation Settings** workflow.

   b. Click the **Certificates** tab.

   c. To allow eligibility for all PIV Federal Agency Smart Card Number (FASC-N) values, set **Cards allowed for derivation** to `.+` (dot plus).

   d. Click **Save Changes**.

7. Configure the system to check the revocation status of the PIV Authentication certificate to seven days by using the following procedures within MyID Desktop:

   a. From the **Configuration** category, select **Operation Settings**.

   b. On the **Certificates** tab, set **Derived credential revocation check offset** to 7.

   c. Click **Save Changes**.
8. Grant access to the following workflows by using the MyID Desktop: Request Derived Credentials, Cancel Credential, Enable/Disable ID, Request Replacement ID, Unlock Credential, Collect My Updates.
   a. From the **Configuration** category, select the **Edit Roles** workflow.
   b. Select the check box for each of the roles to which you want to grant access. In our environment, **Startup User** was selected for all workflows.
   c. Click **Save Changes**.

9. Edit the workflows from Step 8 with the appropriate permissions.
   a. From the **Configuration** category, select the **Edit Roles** workflow.
   b. Click **Show/Hide Roles**.
   c. Select the check boxes for **Mobile User**, **Derived Credential Owner**, and **PIV Applicant**.
   d. Click **Close**.
   e. Select the corresponding roles:

<table>
<thead>
<tr>
<th>Role</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile User</td>
<td>Console Logon, Request Derived Credentials (part 1), Mobile Certificate Recovery, Collect My Updates, Issue Device</td>
</tr>
<tr>
<td>Derived Credential Owner</td>
<td>Console Logon, Request Derived Credentials (part 2), Collect My Updates, Issue Device</td>
</tr>
<tr>
<td>PIV Applicant</td>
<td>Request Derived Credentials (part 2), Collect My Updates</td>
</tr>
</tbody>
</table>

10. Import the Test Federal Common Policy CA certificate into the MyID application server by using the following command as an administrator. This enables the administrator to control the PKI hierarchy that is trusted when verifying PIV cards:

    ```
certutil -addstore -f -Enterprise DerivedCredentialTrustedRoots RootCA.cer
    ```

11. Configure the MyID system with the PIV Authentication and Digital Signature certificate policy Object Identifiers (OIDs) by using the following procedures. The values shown below are production values, so they may need to be changed for your organization:

   a. From the MyID Desktop **Configuration** category, select **Operation Settings**.
b. On the **Certificates** tab, set the following values:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derived credential certificate OID</td>
<td>2.16.840.1.101.3.2.1.3.13</td>
</tr>
<tr>
<td>Derived credential signing certificate OID</td>
<td>2.16.840.1.101.3.2.1.3.6;</td>
</tr>
<tr>
<td></td>
<td>2.16.840.1.101.3.2.1.3.7;</td>
</tr>
<tr>
<td></td>
<td>2.16.840.1.101.3.2.1.3.16</td>
</tr>
</tbody>
</table>

12. Create an Identity Agent credential profile for the DPC by using the following procedures:

   a. From the MyID Desktop **Configuration** category, select **Credential Profiles**.

   b. Click **New**.

   c. In the **Name** field, enter a descriptive name for the profile.

   d. In **Card Encoding**, select **Identity Agent (Only)** and **Derived Credential**.

   e. In **Services**, leave default selections **MyID Logon** and **MyID Encryption**.

   f. In **Issuance Settings**, in the **Mobile Device Restrictions** drop-down, select **Any**.

   g. In **Issuance Settings**, **Require Facial Biometrics**, select **Never Required**.

   h. In **PIN Settings**, configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Mode</td>
<td>PIN</td>
</tr>
<tr>
<td>Maximum PIN Length</td>
<td>12</td>
</tr>
<tr>
<td>Minimum PIN Length</td>
<td>6</td>
</tr>
<tr>
<td>Repeated Characters Allowed</td>
<td>1</td>
</tr>
<tr>
<td>Sequential Characters Allowed</td>
<td>1</td>
</tr>
<tr>
<td>Logon Attempts</td>
<td>5</td>
</tr>
<tr>
<td>PIN Inactivity Time</td>
<td>180</td>
</tr>
<tr>
<td>PIN History</td>
<td>0</td>
</tr>
<tr>
<td>Issue With</td>
<td>User specified PIN (default)</td>
</tr>
<tr>
<td>Email PIN</td>
<td>Unselect</td>
</tr>
<tr>
<td>Length</td>
<td>0</td>
</tr>
</tbody>
</table>

   i. In **Device Profiles**, select **PIVDerivedCredential.xml** from the **Card Format** drop-down.
j. Click Next.


l. Click Next.

m. Select the roles that receive, issue, and validate DPC. All was chosen in this example.

n. Click Next.

o. Select PIV_CON in the Select Card Layout tab.

p. Click Next.

q. Enter text into the Comments and click Next, then Finish.

2.2.2 Intercede MyID Identity Agent

The MyID Identity Agent runs as an application and interfaces with the MyID CMS and supports a wide range of mobile devices and credential stores, including the device native key store, software key store, and microSD. The MyID Identity Agent mobile application is required to issue and manage DPC. No special configuration is necessary after installing the application; scanning the QR code during the initial enrollment directs the Identity Agent to your instance of MyID CMS. MyID Identity Agent is supported for both iOS and Android platforms.

2.2.2.1 Installation

MyID Identity Agent is available on the Google Play Store and Apple App Store. Detailed installation procedures are found on the Google Play Store and Apple App Store support sites.

2.2.3 Intercede Desktop Client

The Intercede Desktop component of this example solution serves as the main point of administration of the MyID CMS. It was installed on a Dell Latitude E6540 laptop running Windows 7. The procedures below are adapted from the Installation and Configuration Guide Version 10.8, Section 7.4.

2.2.3.1 Installation

Before installation, have available the hostname and the Distinguished Name (DN) of the issuer of the Transport Layer Security (TLS) certificate used to communicate with the MyID application server.

1. Run the provided .msi file as an administrator.

2. Select the destination location, then click Next.
3. Select the desired shortcuts to be installed.

4. Click **Next**.

5. In the **MyID Desktop InstallShield Wizard**:
   a. In the **Server URL** field, enter the **URL** for your instance of MyID Server.
   b. In the **SSL Certificate Issuer DN** field, leave empty as this prompt is applicable only when mutual TLS is implemented.
   c. Click **Next**.
   d. Click **Install**.

### 2.2.4 Intercede Self-Service Kiosk

The MyID Self-Service Kiosk serves as a DPC issuance station for eligible PIV holders. While the software is designed to run on a shared Windows system as a kiosk in public space, in this example it is installed on a Dell Latitude E6540 laptop running Windows 7. The procedures below are adapted from *Self-Service Kiosk Installation and Configuration* and *Derived Credentials Installation and Configuration Guide*.
2.2.4.1 Installation

Before installation, have available the hostname and the issuer distinguished name of the TLS certificate used to communicate with the MyID application server.

1. Click Next.

2. Accept default and click Next.

3. In the MyID Self-Service Kiosk InstallShield Wizard:
   a. In the Server URL field, enter the URL of your instance of MyID Server.
   b. In the SSL Certificate Issuer DN field, leave empty as this prompt is applicable only when mutual TLS is implemented.
   c. Select Next.
   d. Select Install.
   e. Select Finish.
2.2.4.2 Configuration

Use the following procedures to configure the MyID Self-Service Kiosk for DPC issuance:

1. Set the timeout for the PIN entry screen by using the following procedures:
   a. Open C:\Program Files (x86)\Intercede\MyIDSelfServiceKiosk\MyIDKiosk.exe.config by using a text editor.
   b. Edit the value parameter in the following line:

   ```xml
   <add key="DerivedCredentialsPageTimeoutSeconds" value="120"/>
   ```

   c. Edit the value parameter in the following line with the MyID application server address:

   ```xml
   <add key="Server" value="http://myserver.example.com/"/>
   ```

   d. Save changes to the file.

2.2.5 Windows Client Installation for MyID and Intel Authenticate

The Intel Authenticate Integration Guide for Active Directory Policy Objects provides instructions on how to set up Group Policy Objects for various functions of the Intel Authenticate installation process. The following instructions are primarily repurposed from the Intel Authenticate Integration Guide.
2.2.5.1 Installing the MyID Self-Service Application

1. Run SSP-2.3.1000.1_E.msi on the client computer.

2. Click Next.

3. Click Next.

4. Enter the Server URL for your organization’s MyID server. Leave the SSL Certificate Issuer DN field empty, as this prompt is applicable only when mutual TLS is implemented.
5. Click **Next**.

6. Click **Install**.

7. Click **Finish**.
2.2.5.2 Installing the WSVC Service

1. Run WSVC-1.6.1000.1_B.msi.

2. Click Next.

3. Enter the username and password for the account that will install the service.

4. Click Next.
5. Click **Next**.

6. Click **Install**.
2.2.5.3 Installing Prerequisites for Intel Authenticate

This process may differ depending on the client system. Primarily, it is important that the Intel Management Engine is installed and that any Intel drivers are up-to-date so that the Intel Authenticate Precheck is successful.

1. Run n1cra26w.exe. (The name may differ based on your system—this is the Intel Management Engine.)

2. Click Next.
3. Select I accept the agreement.

4. Click Next.

5. Click Next.
6. Click **Install**.

7. Check the box next to **Install Intel Management Engine 11.6 Software for Windows 10 now**.

8. Click **Finish**.
9. Run `u2vdo22us14avc.exe`. (The name may differ based on your system—this is the graphics driver update.)

10. Click **Next**.
11. Select **I accept the agreement**.

12. Click **Next**.

13. Click **Next**.
14. Click **Install**.

15. Check the box next to **Install Intel HD Graphics Driver now**.
16. Click Finish.

2.2.5.4 Installing the Intel Authenticate Client

The Intel Authenticate Client should be installed automatically by the Group Policy Object (GPO), but it can also be installed manually by running IAx64-2.5.0.68.msi.

1. Run IAx64-2.5.0.68.msi.

2. Click Next.
3. Select I accept the terms in the License Agreement.

4. Click Next.

5. Click Install.
6. Click Finish.

2.2.5.5 Configuring Intel Authenticate

1. Once the Enforce Policy GPO is run, the window for configuring Intel Authenticate will open on the client machine. You can also open this manually by searching for Intel Authenticate in the Start Menu.

2. Click the right arrow button.
3. Click the **right arrow button**.

4. Click **Enroll Factor**.
5. Click Proceed.

6. Enter a PIN for Intel Authenticate, which will be used for any certificates issued to the device.

7. Re-enter the PIN.

8. Click Return to home.
2.2.6 Intel Authenticate GPO

The Intel Authenticate Integration Guide for Active Directory Policy Objects provides instructions on how to set up GPOs for various functions of the Intel Authenticate installation process. The following instructions are primarily repurposed from the Intel Authenticate Integration Guide.
2.2.6.1 Preparing a Digital Signing Certificate

1. In a new PowerShell window, generate a new self-signed certificate to sign the Intel Policy. Enter the command:

   ```powershell
   New-SelfSignedCertificate -Subject "CN=TestCert" -KeyUsageProperty All -KeyAlgorithm RSA -KeyLength 2048 -KeyUsage DigitalSignature -Provider "Microsoft Enhanced RSA and AES Cryptographic Provider" -CertStoreLocation "Cert:CurrentUser\My"
   ```

2. Run `mmc.exe` from the Start menu to open the Microsoft Management Console window.

3. Select File > Add/Remove Snap-In. Add the Certificates snap-in.
4. The newly created certificate should be in the Certificates – Current User > Personal > Certificates store.

5. Right-click the newly created certificate and select Copy.
6. Navigate to Certificates – Current User > Trusted Root Certification Authorities > Certificates and paste the certificate there.

7. Click Yes when a warning message appears.
2.2.6.2 Creating a Profile

1. Run the ProfileEditor.exe file as an administrator.

2. Click Create a New Profile....

3. Click Select Signing Certificate.
4. Select the newly created certificate and click Select.

5. Under Authentications Factors, check the box next to Protected PIN.

6. Click the Edit button.
7. Set the PIN length and the minimum number of unique digits.

8. Click *Close*.

9. Under *Actions > OS Login*, check the box next to *Enable OS Login*.

10. Check the box next to *Protected PIN*.

11. Click *Advanced Settings*.
12. Uncheck the box next to **Require the system drive to be encrypted**.

13. Click **Close**.

14. Click the **Save As** button and save the profile.
2.2.6.3 Creating a Shared Folder

1. Create a new folder on the network.

2. Give it a name such as `shared-gpo-folder`.

3. Right-click the folder and select **Properties**.

4. Go to the **Security** Tab.

5. Click **Edit**.

6. Click **Add**.
7. Enter **Domain Computers** in the text box.

8. Click **OK**.

9. Ensure that the Domain Computers have read permissions on this folder.

10. Click **OK**.
11. Click OK.

12. Copy all the files from the HostFiles folder, as well as the Intel Profile you created, into this shared folder.

2.2.6.4 Creating WMI Filters for the GPOs

1. Open the Group Policy Management window by running gpmc.msc from the Start menu.

2. Right-click WMI Filters and select New....
3. Enter a name such as *Is Intel Authenticate Supported* and click Add.

4. In the Query field, enter `SELECT * FROM Intel_Authenticate WHERE Supported="true"`.

5. Click OK.
Click Save.

Right-click WMI Filters and select New....
Enter a name such as Is Intel Authenticate Installed and click Add.
9. In the **Query** field, enter `SELECT * FROM Intel_Authenticate WHERE isClientInstalled="true" AND isEngineInstalled="true"`.

10. Click **OK**.

11. Click **Save**.
2.2.6.5 Creating a GPO to Discover Intel Authenticate

1. Open Group Policy Management.

2. In the Group Policy Management tree, right-click the domain and select Create a GPO in the domain and Link it here.

3. Enter a name for this GPO.
4. Right-click the GPO just created and select Edit.

5. Right-click Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks and select New > Scheduled Task (At least Windows 7).

6. Select Replace from the drop-down list for Action.

7. Enter a descriptive name.

8. Click Change User or Group.

9. Enter SYSTEM and click OK.
10. Check the box next to **Run whether user is logged on or not**.

11. A window will open asking for a password. Click **Cancel**.

12. Check the box next to **Do not store password. The task will only have access to local resources**.

13. Check the box next to **Run with highest privileges**.
14. Select the **Triggers** tab.

15. Click **New**.

16. Select **At task creation/modification** for **Begin the task**.

17. Click **OK**.
18. Select the **Actions** tab.

19. Click **New**.

20. Select **Start a program**.
21. For **Program/script**, enter the network location of the **CopyFilesLocally.bat** file.

22. Click **OK**.

![New Action dialog box](image1.png)

23. Click **OK**.

![New Task (At least Windows 7) Properties](image2.png)
24. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.

25. Select **Replace** from the drop-down list for **Action**.

26. Enter a descriptive name.

27. Click **Change User or Group**.

28. Enter **SYSTEM** and click **OK**.

29. Check the box next to **Run whether user is logged on or not**.

30. A window will open asking for a password. Click **Cancel**.
31. Check the box next to **Do not store password. The task will only have access to local resources.**

32. Check the box next to **Run with highest privileges.**

33. Select the **Triggers** tab.

34. Click **New....**

35. Select **At task creation/modification** for **Begin the task.**

36. Click **OK.**
37. Select the **Actions** tab.

38. Click **New**....

39. Select **Start a program**.

40. For **Program/script**, enter `C:\Temp\DetectIntelAuthenticate.bat`.

41. For **Start In**, enter `C:\Temp`.

42. Click **OK**.
43. Click OK.
2.2.6.6 Creating a GPO to Install Intel Authenticate

1. Open Group Policy Management.

2. In the Group Policy Management tree, right-click the domain and select Create a GPO in the domain and Link it here.

3. Enter a name for this GPO.

4. Click OK.

5. Select the GPO you just created and select Is Intel Authenticate Supported in the WMI Filtering section.

6. Click Yes.
7. Right-click the GPO just created and select **Edit**.

8. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.

9. Select **Replace** from the drop-down list for **Action**.

10. Enter a descriptive name.

11. Click **Change User or Group**.

12. Enter **SYSTEM** and click **OK**.
13. Check the box next to Run whether user is logged on or not.

14. A window will open asking for a password. Click Cancel.

15. Check the box next to Do not store password. The task will only have access to local resources.

16. Check the box next to Run with highest privileges.

17. Select the Triggers tab.

18. Click New....

19. Select At task creation/modification for Begin the task.

20. Check the box next to Delay task for.

21. Select 30 minutes.

22. Ensure Enabled is selected and Click OK.
23. Select the **Actions** tab.

24. Click **New...**

25. Select **Start a program**.

26. For **Program/script**, enter `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.

27. For **Add arguments**, enter `-executionpolicy unrestricted C:\Temp\RunInstaller.ps1`.

28. For **Start In**, enter `C:\Temp`.

29. Click **OK**.

30. Click **OK**.
31. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.

32. Select **Replace** from the drop-down list for **Action**.

33. Enter a descriptive name.

34. Click **Change User or Group**.

35. Enter **SYSTEM** and click **OK**.

36. Check the box next to **Run whether user is logged on or not**.

37. A window will open asking for a password. Click **Cancel**.

38. Check the box next to **Do not store password. The task will only have access to local resources**.

39. Check the box next to **Run with highest privileges**.
40. Select the **Triggers** tab.

41. Click **New**....

42. Select **At task creation/modification** for **Begin the task**.

43. Check the box next to **Delay task for**.

44. Select **30 minutes**.

45. Ensure **Enabled** is selected and Click **OK**.
46. Select the **Actions** tab.

47. Click **New**.

48. Select **Start a program**.

49. For **Program/script**, enter `C:\Temp\DetectIntelAuthenticate.bat`.

50. For **Start In**, enter `C:\Temp`.

51. Click **OK**.
52. Click OK.
2.2.6.7 Creating a GPO to Enforce the Policy

1. Open **Group Policy Management**.

2. In the Group Policy Management tree, right-click the domain and select **Create a GPO in the domain and Link it here**.

3. Enter a name for this GPO

4. Click **OK**.

5. Select the GPO you just created and select **Is Intel Authenticate Installed** in the **WMI Filtering** section.

6. Click **Yes**.
7. Right-click the GPO just created and select **Edit**.

8. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.

9. Select **Replace** from the drop-down list for **Action**.

10. Enter a descriptive name.

11. Click **Change User or Group**.

12. Enter **SYSTEM** and click **OK**.
13. Check the box next to **Run whether user is logged on or not**.

14. A window will open asking for a password. Click **Cancel**.

15. Check the box next to **Do not store password. The task will only have access to local resources**.

16. Check the box next to **Run with highest privileges**.

17. Select the **Triggers** tab.

18. Click **New**....

19. Select **On a schedule** for **Begin the task**.

20. Select **Daily**.

21. Check the box next to **Delay task for**.
22. Select **30 minutes**.

23. Ensure **Enabled** is selected and Click **OK**.

24. Select the **Actions** tab.

25. Click **New**....

26. Select **Start a program**.

27. For **Program/script**, enter `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.

28. For **Add arguments**, enter `-executionpolicy unrestricted "C:\Temp\EnforcePolicy.ps1"` “C:\Temp\intelprofile.xml”.

29. For **Start In**, enter `C:\Temp`.

30. Click **OK**.
31. Click OK.
2.2.7 Intel VSC Configuration

The Intel Authenticate Integration Guide for Active Directory Policy Objects provides instructions on how to set up GPOs for various functions of the Intel Authenticate installation process. The following instructions are primarily repurposed from the Intel Authenticate Integration Guide.

2.2.7.1 Configuring MyID for Intel VSC

1. Open MyID Desktop.
2. Click New Action.
3. Click Configuration > Operation Settings.
4. Go to the **Devices** tab.

5. Delete the value in **Default Card Data Model**.

6. Set **Enable Intel Virtual Smart Card support** to **Yes**.

7. Click **Save changes**.
2.2.7.2 Setting Up a PIN Protection Key

1. Click **New Action**.

2. Click **Configuration > Key Manager**.
3. For **Select Key Type to Manage**, select **PIN Generation Key**.

4. Click **Next**.

5. Click **Add New Key**.
6. Enter a name and a description.
7. For Encryption Type, select 3DES.
8. Select Automatically Generate Encryption Key in Software and Store on Database.
9. Click Save.
2.2.7.3 Creating a Credential Profile

1. Click **New Action**.

2. Click **Configuration > Credential Profiles**.

3. Click **New**.
4. Enter a name and a description.

5. Check the box next to Derived Credential.

6. Check the box next to Intel Virtual Smart Card (Only).
7. Select the **Services** tab.

8. Check the box next to **MyID Logon**.

9. Check the box next to **MyID Encryption**.

10. Select the **Issuance Settings** tab.

11. Set **Require Activation** to **No**.

12. Set **Pre-encode Card** to **None**.

13. Set **Require Fingerprints at Issuance** to **Never Required**.

14. Set **Require Facial Biometrics** to **Never Required**.

15. Set **Additional Authentication** to **None**.

16. Set **Terms and Conditions** to **None**.

17. Set **Proximity Card Check** to **None**.

18. Set **Notification Scheme** to **None**.

19. Uncheck all boxes.

20. Set **Mobile Device Restrictions** to **Any**.
21. Set **Generate Logon Code** to **Simple**.

22. Select the **PIN Settings** tab.

23. For **PIN Algorithm**, select **EdeficePinGenerator**.

24. For **Protected Key**, select the PIN generation key created earlier.
25. Select the **Device Profiles** tab.

26. For **Card Format**, select **PIVDerivedCredential.xml**.

27. Click **Next**.
28. Select the certificates to be issued with the VSC.

29. Click **Next**.

30. Select the roles that are allowed to use this profile.

31. Click **Next**.
32. Enter a description and click **Next**.
2.2.8  DPC Lifecycle Workflows

This section details the steps to perform issuance and termination of the DPC by using the MyID CMS. Issuance is started from the MyID Self-Service Kiosk application, while termination uses the MyID Desktop administration application.

2.2.8.1  Mobile Device Issuance Workflow

The following steps are performed by the DPC Applicant by using the MyID Self-Service Kiosk and the MyID Identity Agent application on the target mobile device.

1. At the Welcome screen of the MyID Self-Service Kiosk, insert your PIV Card into the card reader.

   Welcome to the MyID Kiosk
   Insert your card to begin

2. On the Enter your PIN screen:
   a. Enter the PIN used to activate the inserted PIV Card.
   b. Select Next.
3. On the Select Credential Profile screen:
   a. To provision the DPC to the MyID software token, select Derived PIV Profile.
   b. To provision the DPC to the iOS Secure Enclave hardware-backed token, select DPC for Native iOS Keystore.
   c. The MyID Self-Service Kiosk will display a QR code; the remaining steps are completed by using the MyID Identity Agent application on the target mobile device.
4. Launch MyID Identity Agent.

5. On the initial screen, under Actions, tap Scan QR Code.
6. Use the device camera to capture the QR code displayed by the MyID Self-Service Kiosk.
7. On the Set PIN screen:
   a. In the Enter PIN field, enter a numeric PIN that will be used to activate the DPC.
b. In the Confirm PIN field, enter the same numeric PIN.

8. If DPC provisioning was successful, the Identities screen will provide a visual representation of information for the DPC Subscriber's linked PIV Card.
Identities

Actions
- Scan QR Code
- Provision Mobile Identity
- View My Certificates
- Advanced Options
2.2.8.2 Intel Authenticate Issuance Workflow

2.2.8.2.1 Requesting a DPC for Intel VSC

1. Go to a MyID Kiosk.

2. Insert a PIV Card.

3. Enter the PIN for the PIV Card.

4. Select the profile created for Derived PIV. An email will be sent to the user with a one-time code for collection.
2.2.8.2.2 Collecting the DPC

The following procedures will request and install the DPC in the Intel Authenticate protected token. Note that the DPC will be protected by the enrollment factors set in Section 2.2.5.5.

1. On the client machine, open the MyID Self-Service App with the parameters /nopopup and /iptonly.
   ```
   $ MyIDApp.exe /nopopup /iptonly
   ```

2. Click Continue.
3. Enter the Logon Code from the email.

4. Click Continue.

5. Click Finish after the certificates are successfully collected.
2.2.8.3 Maintenance Workflow

Changes to a DPC Subscriber's PIV Card that would 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 Identity Agent container.

2.2.8.4 Termination Workflow

1. Select the target device associated with the DPC subscriber that will be terminated.
2. Select a reason for termination and enter any other required information for policy compliance.

3. Click Next

4. Confirm the termination of the DPC.
### Appendix A  List of Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CAPI</td>
<td>Cryptographic Application Interface</td>
</tr>
<tr>
<td>CMS</td>
<td>Credential Management System</td>
</tr>
<tr>
<td>CPS</td>
<td>Cryptographic Service Provider</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>EMM</td>
<td>Enterprise Mobility Management</td>
</tr>
<tr>
<td>FASC-N</td>
<td>Federal Agency Smart Card Number</td>
</tr>
<tr>
<td>GPO</td>
<td>Group Policy Object</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>MDAC</td>
<td>Microsoft Data Access Components</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>OID</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identity Verification</td>
</tr>
<tr>
<td>PKCS</td>
<td>Public Key Cryptography Standards</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>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSM</td>
<td>Self-Service Module</td>
</tr>
<tr>
<td>SSP</td>
<td>Shared Service Provider</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UPI</td>
<td>UniCERT Programmatic Interface</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>
<tr>
<td>VSC</td>
<td>Virtual Smart Card</td>
</tr>
<tr>
<td>WMI</td>
<td>Windows Management Instrumentation</td>
</tr>
<tr>
<td>WSVC</td>
<td>World Wide Web Publishing Service</td>
</tr>
</tbody>
</table>