NIST SPECIAL PUBLICATION 1800-12

Derived Personal Identity Verification (PIV) Credentials

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

William Newhouse
Michael Bartock
Jeffrey Cichonski
Hildegard Ferraiolo
Murugiah Souppaya
Christopher Brown
Spike E. Dog
Susan Prince
Julian Sexton

SECOND DRAFT

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

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SPECIAL PUBLICATION 1800-12

Derived Personal Identity Verification (PIV) Credentials

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

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

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

August 2018

U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter G. Copan, Undersecretary of Commerce for Standards and Technology and Director

NIST SPECIAL PUBLICATION 1800-12A

Derived Personal Identity Verification (PIV) Credentials

Volume A:
Executive Summary

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

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

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

August 2018

SECOND DRAFT

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

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

- Misuse of identity, especially through stolen passwords, is a primary source for cyber breaches. Enabling stronger processes to recognize a user's identity is a key component to securing an organization's information systems.
- Access to federal information systems relies on the strong authentication of the user with a Personal Identity Verification (PIV) Card. These "smart cards" contain identifying information about the user that enables stronger authentication to federal facilities, information systems, and applications.
- Today, access to information systems is increasingly from mobile phones, tablets, and some laptops that lack an integrated smart card reader found in older, stationary computing devices, forcing organizations to have separate authentication processes for these devices.
- Derived PIV Credentials (DPC) leverage identity proofing and vetting results of current and valid credentials used in PIV Cards by enabling the secure storage of an equivalent credential on devices without PIV Card readers.
- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore the development of a security architecture that uses commercially available technology to manage the life cycle of DPC.
- This NIST Cybersecurity Practice Guide demonstrates how organizations can provide multi-factor authentication for users to access PIV-enabled websites and exchange secured emails—from mobile devices that lack PIV Card readers.

CHALLENGE

In accordance with Homeland Security Presidential Directive 12 (HSPD-12), the PIV standard was created to enhance national security by providing a set of common authentication mechanisms that provide logical access to federal systems on PIV-compatible desktop and laptop computers. With the federal government's increased reliance on mobile computing devices that lack PIV Card readers, the mandate to use PIV systems has pushed for the need to derive the credentials on a PIV Card into mobile devices in a manner that enforces the same security policies for the life cycle of a PIV Card.

NIST has published guidance on DPC, including documenting a proof-of-concept research paper. Expanding upon this work, the NCCoE used common mobile devices available in the market today to demonstrate the use of DPC in a manner that meets security policies. The flexibility of the technologies that support PIV, along with a growing understanding of the value of strong digital authentication practices, has developed an ecosystem of vendors able to provide digital authentication solutions that may follow the policies outlined in NIST guidance for DPC.

With experts from the federal sector and technology collaborators who provided the requisite equipment and services, we developed representative use-case scenarios to describe user authentication security challenges based on normal day-to-day business operations. The use cases include issuance, maintenance, and termination of the credential.

SOLUTION

The NCCoE has developed two DPC example solutions that demonstrate how DPC can be added to mobile devices to enable multi-factor authentication to information technology systems while meeting policy guidelines. Although the PIV program and the NCCoE DPC Project are primarily aimed at the federal sector's needs, both are relevant to mobile device users in the commercial sector who use smart-card-based credentials or other means of authenticating identity.

To that end, the example solutions are based on standards and best practices, and derive from a simple scenario that informs the basis of an architecture tailored to the public or private sector, or both.

The NCCoE sought existing technologies that provided the following capabilities:

- authenticate users of mobile devices by using secure cryptographic authentication exchanges
- provide a feasible security platform based on Federal Digital Identity Guidelines
- utilize a public key infrastructure (PKI) with credentials derived from a PIV Card
- support operations in PIV, PIV-interoperable (PIV-I), and PIV-compatible (PIV-C) environments
- issue PKI-based DPC at Level of Assurance 3
- provide logical access to remote resources hosted in either a data center or the cloud

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. 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 solution.

BENEFITS

The NCCoE's practice guide to DPC can help your organization:

- extend authentication measures to devices, without having to purchase expensive and cumbersome external smart card readers
- provide users with the capability to access the information that they need, using the devices that they want to use
- meet authentication standards requirements for protected websites and information across all devices, both traditional and mobile
- manage the DPC centrally through an Enterprise Mobility Management system, reducing integration efforts and associated costs
- leverage the Federal PKI Shared Service Provider Program, enabling cost savings associated with a contractor-provided service, with adequate government oversight and control

SHARE YOUR FEEDBACK

You can view or download the guide at http://www.nccoe.nist.gov/projects/building-blocks/piv-credentials. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at piv-nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build these example solutions.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

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 challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200

NIST SPECIAL PUBLICATION 1800-12B

Derived Personal Identity Verification (PIV) Credentials

Volume B:
Approach, Architecture, and Security Characteristics

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

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

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

August 2018

SECOND DRAFT

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

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-12B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-12B, 83 pages, (August 2018), CODEN: NSPUE2

FEEDBACK

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

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

Public comment period: 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.

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

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

Name	Organization
Matthew Steele	The MITRE Corporation

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

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

Contents

List of Figures

List of Tables

1 Summary

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

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

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

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

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

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

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

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

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

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

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

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

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

1.1 Challenge

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

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

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

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

1.2 Solution

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

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

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

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

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

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

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

1.3 Benefits

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

- providing visibility into how the different device vendors and CMS vendors are implementing solutions for storing the credentials
- demonstrating the use of managed services for the DPC issuance and life cycle management
- demonstrating integration with an EMM solution

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the DPC example implementations. 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 1800-12B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-12C: *How-To Guides* – instructions for building the example solution

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

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

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

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

- Section 3.5.3, Risk, provides a description of the risk analysis we performed
- Section 3.5.4, Security Control Map, maps the security characteristics of the example solutions to cybersecurity standards and best practices

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

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, *NIST SP 1800-12C*, to replicate all or parts of the builds created in our lab. The How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solutions. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create 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 either solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of the DPC example solutions. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products we used and maps them to the cybersecurity controls provided by the reference solutions.

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

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

3 Approach

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

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

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

3.1 Audience

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

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

3.2 Scope

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

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

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

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

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

3.3 Relationship to NIST SP 800-63-3

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

3.4 Assumptions

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

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

3.4.1 Modularity

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

3.4.2 Security

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

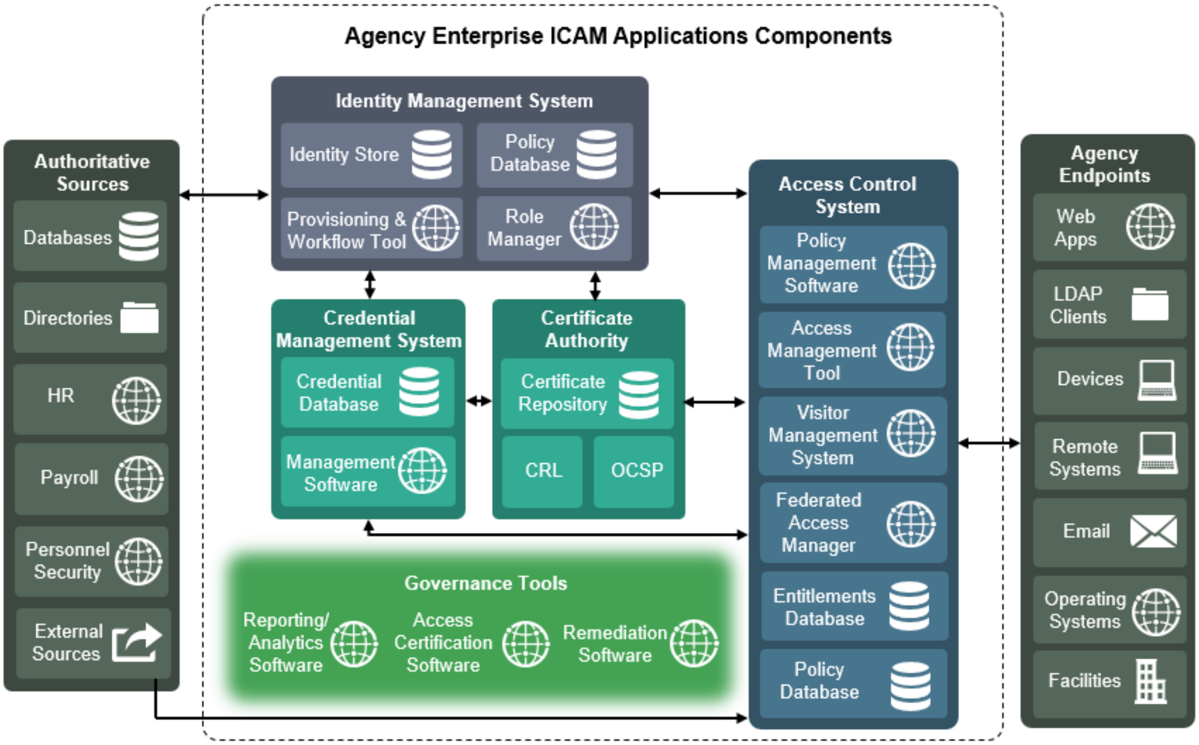
3.4.3 Existing Infrastructure

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

3.4.4 Architecture Components

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

Figure 3-1 Federal ICAM Enterprise Architecture



3.4.4.1 Credential Management System

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

3.4.4.2 Public Key Infrastructure

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

3.4.4.3 Enterprise Mobility Management

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

3.4.4.4 Mobile Device

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

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

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

3.4.4.5 Authenticator

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

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

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

3.5 Risk Assessment

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

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

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

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

A DPC solution is part of an overall mobile security architecture that protects enterprise data by using strong multifactor authentication to access remote resources. A DPC solution also supplements a basic centralized enterprise mobility security policy, as NIST SP 800-124 recommends. The publication further recommends that organizations design and acquire one or more solutions that collectively mitigate current workforce mobile device security risk. For an in-depth discussion on digital identity risk management, we encourage review of Section 3.5.1, which presents a list of possible identity risks and how they are covered by DPC, based on NIST SP 800-63-3 guidelines related to digital identity risk. An organization can apply the guidelines while executing all relevant Cybersecurity Framework and RMF life-cycle phases [7].

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

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

3.5.1 Threats

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

Table 3-1 Enrollment and Identity Proofing Threats

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

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

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

484

485 Table 3-2 Authenticator Threats to DPC

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

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

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

486

3.5.1.1 Other Threats

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

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

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

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

Table 3-3 Mobile Threat Classes and Categories

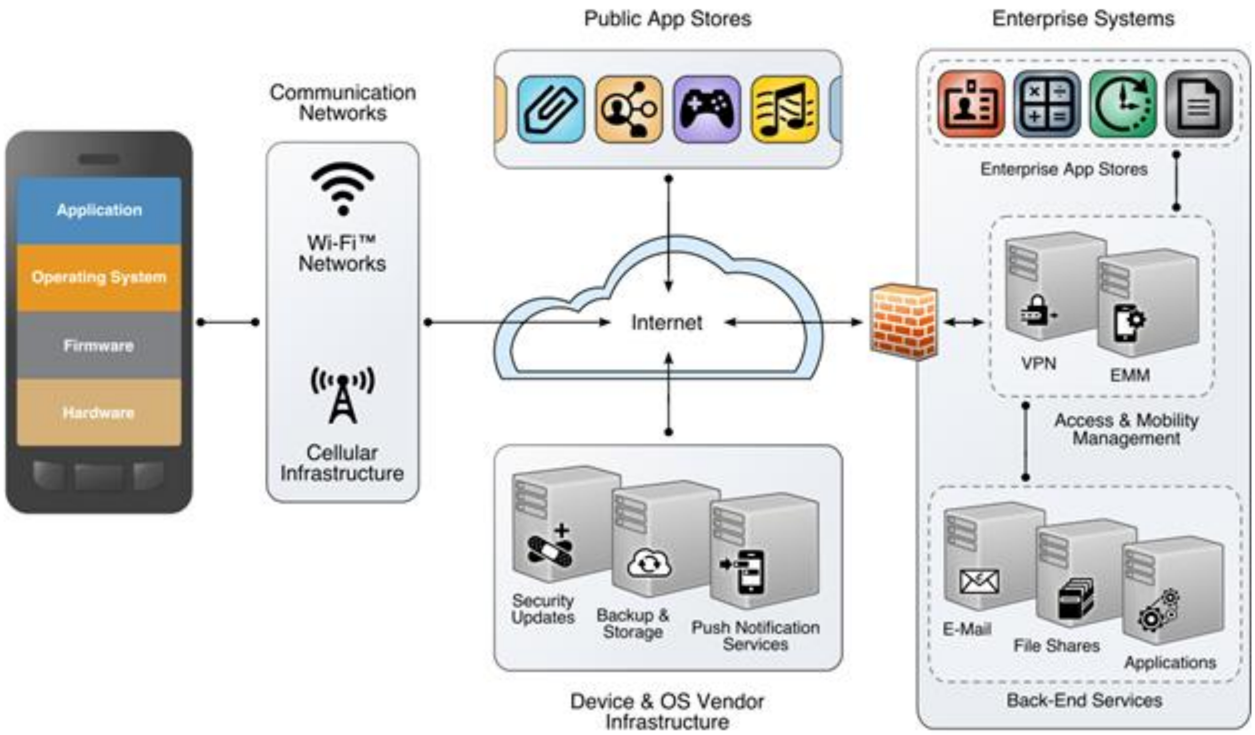
Threat Class	Threat Category
Application	Malicious or Privacy-Invasive Application
	Vulnerable Applications
Authentication	Authentication: User or Device to Network
	Authentication: User or Device to Remote Service
	Authentication: User to Device
Cellular	Carrier Infrastructure
	Carrier Interoperability
	Cellular Air Interface
LAN & PAN	Network Threats: Bluetooth
	Network Threats: NFC
	Network Threats: Wi-Fi
Payment	Application-Based
	In-App Purchases
	NFC-Based
Physical Access	Physical Access
Privacy	Behavior Tracking

	Consumer-Grade Femtocell
	SMS/MMS/RCS
	USSD
	VoLTE
Ecosystem	Mobile Application Store
	Mobile OS and Vendor Infrastructure
EMM	Enterprise Mobility
GPS	GPS

Supply Chain	Supply Chain
Stack	Baseband Subsystem
	Boot Firmware
	Device Drivers
	Isolated Execution Environments
	Mobile Operating System
	SD Card
	USIM/SIM/UICC Security

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

Figure 3-2 The Mobile Ecosystem



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

3.5.2 Vulnerabilities

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

3.5.2.1 Mobile Device Vulnerabilities

Vulnerabilities discovered within mobile applications and rich operating systems are important to any deployment of DPC. The DPC issuer must ensure strong protections on the use of the credential via a PIN or pass phrase [6, Section 3] while also making sure that other applications on the device cannot access the credential. Sensitive cryptographic material can be stored in software at AAL-2, leaving the mobile device open to exploits that attack vulnerable code. To thwart these types of attacks, it is common for mobile applications to be sandboxed in some manner to prevent unexpected and unwanted interaction among the system, its applications, and data access between disparate applications (including user data) [18]. However, a search of the NVD yields examples of software vulnerabilities [20] that might allow exploits to *break* sandboxing protections. A full discussion on these topics, including mitigations, can be found in NIST IR 8144, *Assessing Threats to Mobile Devices & Infrastructure: the Mobile Threat Catalogue* [18] and NIST SP 800-163, *Vetting the Security of Mobile Applications* [21]. Vulnerabilities are also introduced by downloading nonapproved applications. We recommend that only vetted and approved applications be downloaded. NIST's AppVet is an example of an application vetting platform.

3.5.2.2 Network Vulnerabilities

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

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

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

3.5.3 Risk

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

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

3.5.4 Security Control Map

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

Table 3-4 Security Control Mappings

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

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

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

3.6 Technologies

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

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

3.6.1 Entrust Datacard

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

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

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

3.6.2 Intel Authenticate

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

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

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

3.6.3 Intercede

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

3.6.4 MobileIron

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

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

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

3.6.5 Verizon Shared Service Provider

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

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

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

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

3.6.6 Mobile Endpoints

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

Table 3-5 Mobile Endpoints

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

3.6.7 Technology Mapping

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

Table 3-6 Products and Technologies

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

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

4 Architecture

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

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

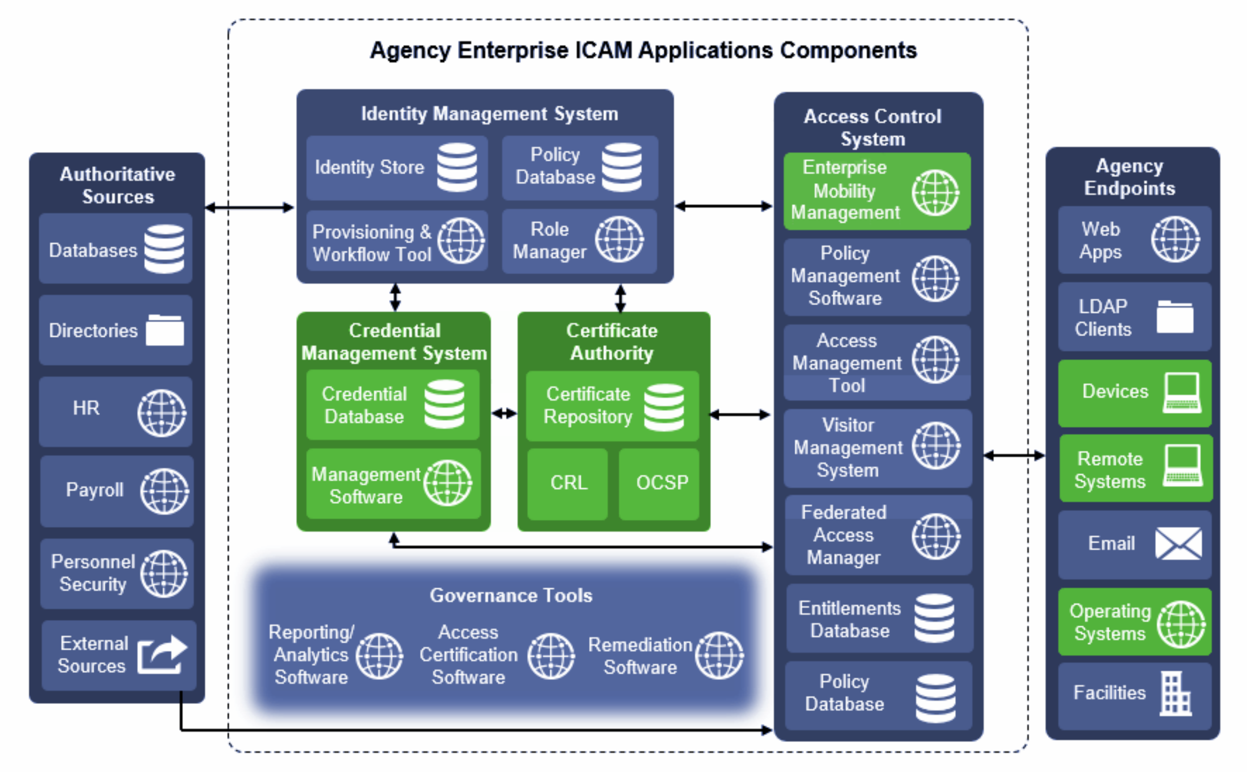
4.1 Architecture Description

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

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

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

Figure 4-1 Federal ICAM Enterprise Architecture

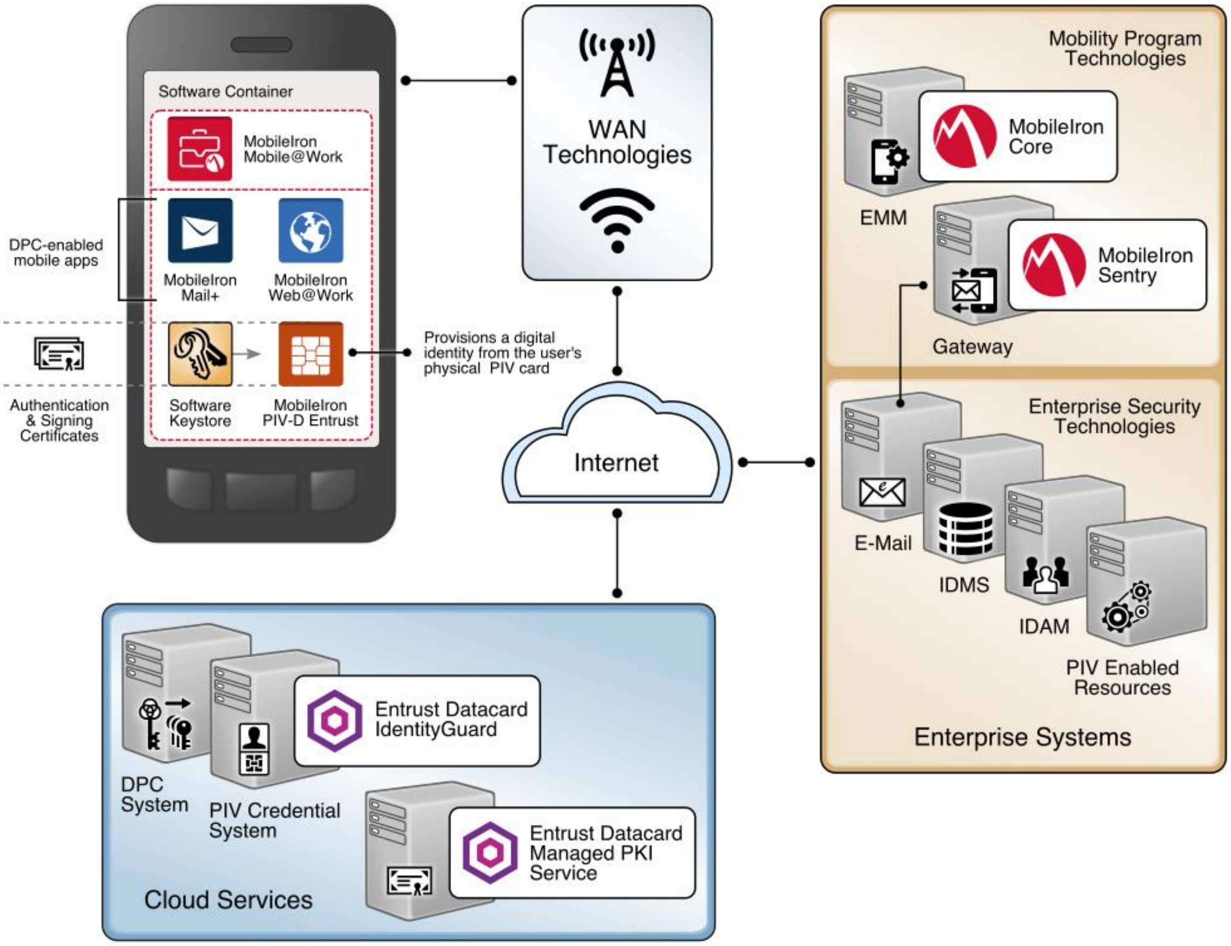


4.2 Managed Architecture with EMM Integration

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

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

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



4.3 Hybrid Architecture for PIV and DPC Life-Cycle Management

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

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

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

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

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

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

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

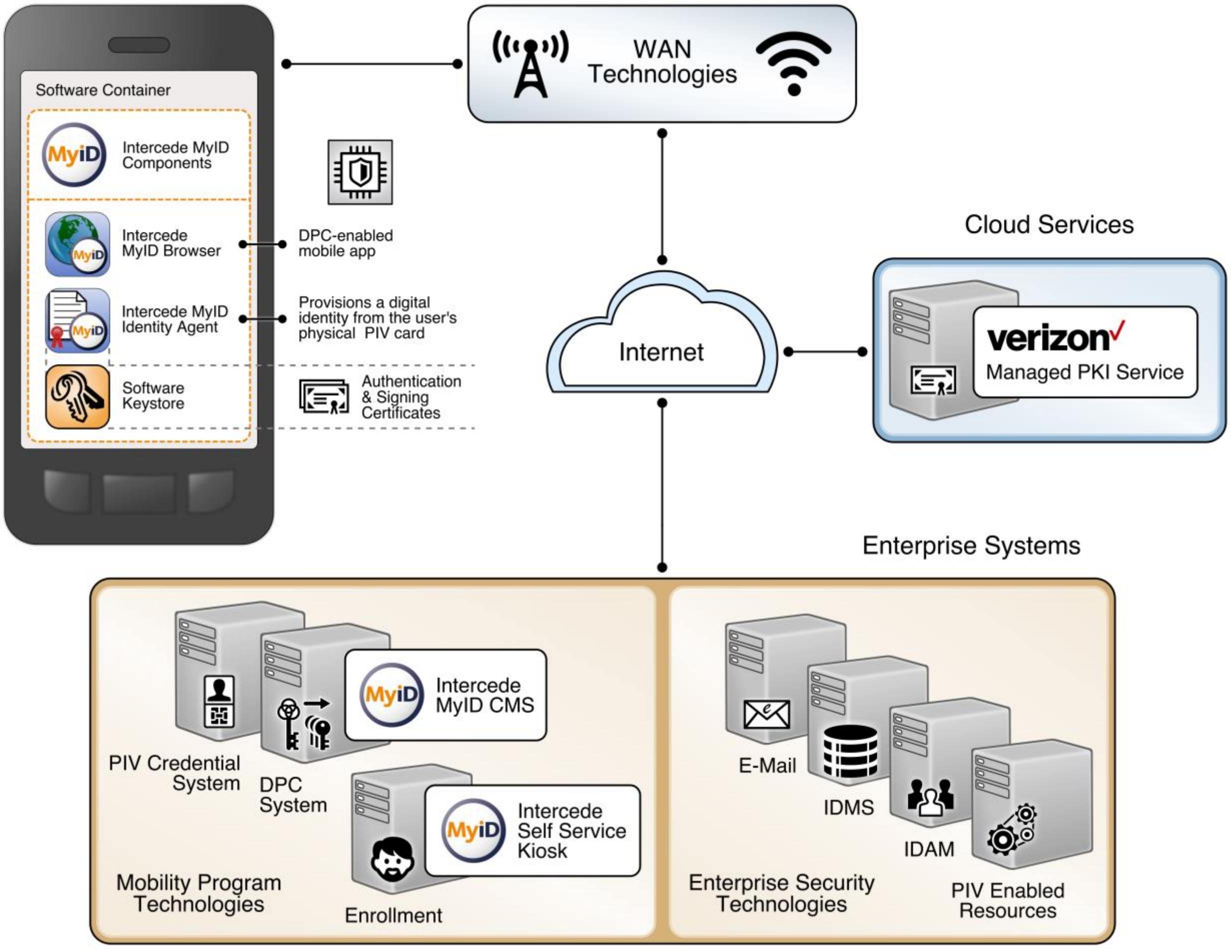
Table 4-1 MyID CMS Component Descriptions

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

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

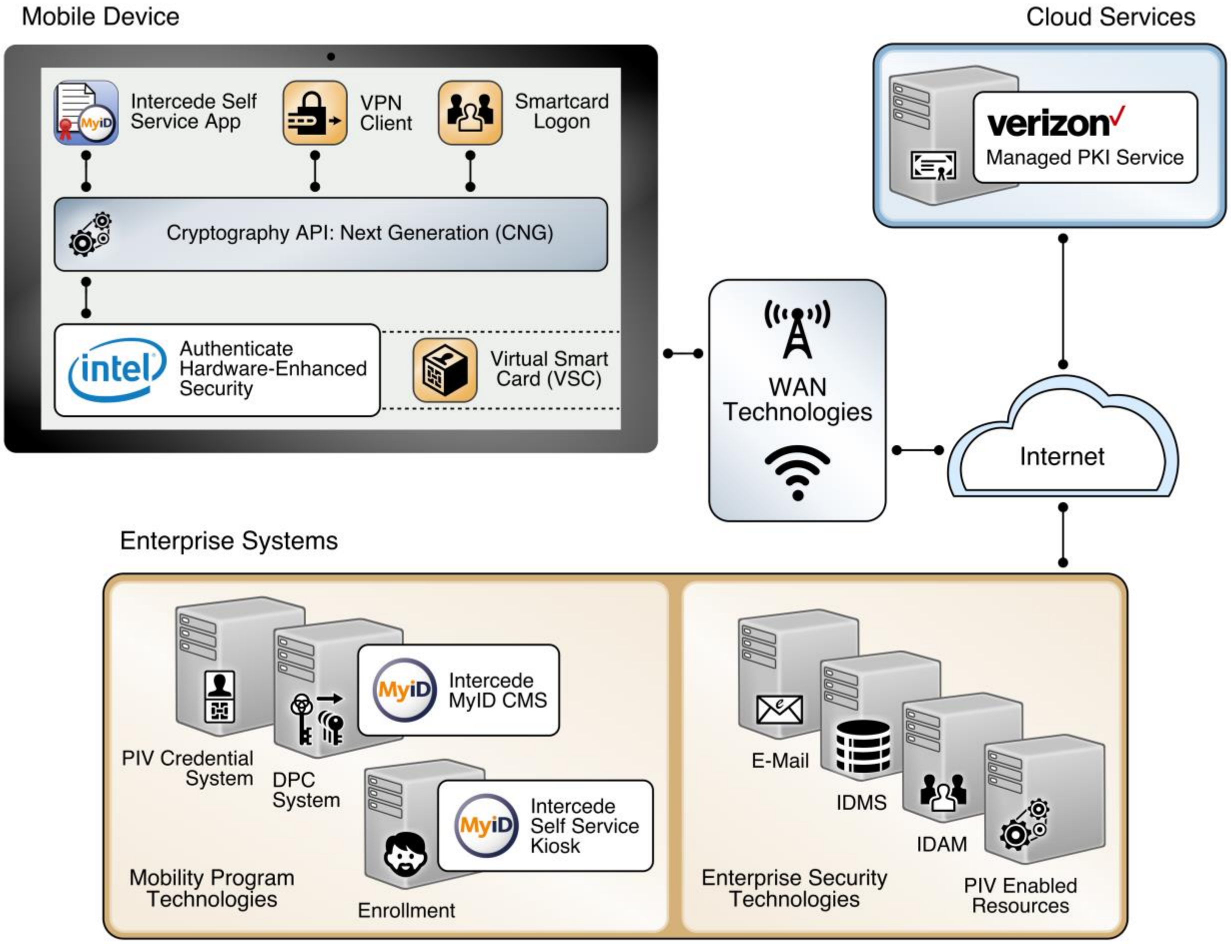
The figures below depict high-level views of the example implementations of the hybrid architecture used for this solution for DPC. Detailed, system-level figures can be found in Part C of this guide. Figure 4-3 focuses on the mobile device implementation. Here, the Identity Agent application is used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

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



790

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



5 Security Characteristics Analysis

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

5.1 Assumptions and Limitations

The security characteristics analysis has the following limitations:

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

5.2 Build Testing

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

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

5.2.1 Managed Architecture Build Testing

5.2.1.1 Initial Issuance

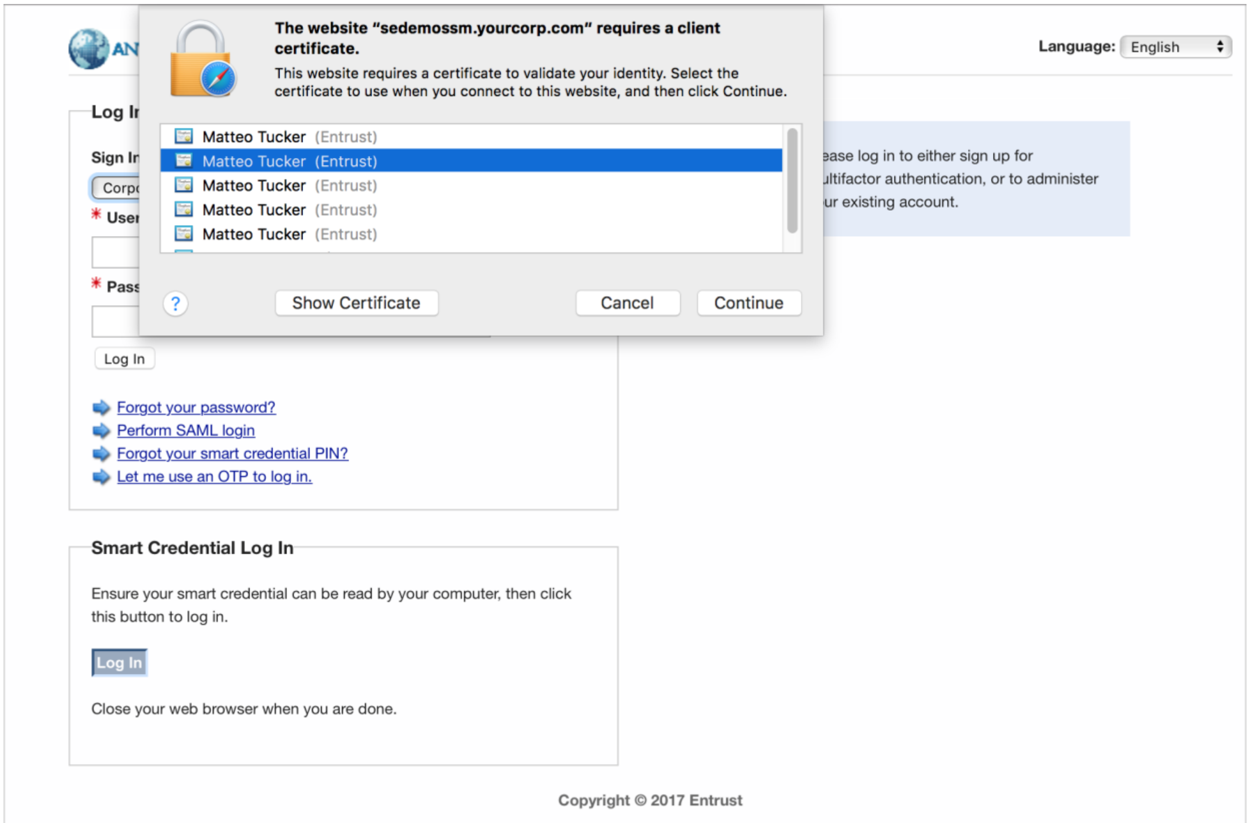
With our Entrust Datacard example solution, the mobile device connects to the IdentityGuard system, and the IdentityGuard connects to the CA, thereby handling delivery of the public certificate to the mobile device, which follows the same process for issuing a PIV Card except that a QR is involved. In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

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

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

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

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



The website “sedemossm.yourcorp.com” requires a client certificate.

This website requires a certificate to validate your identity. Select the certificate to use when you connect to this website, and then click Continue.

- Matteo Tucker (Entrust)
- Matteo Tucker (Entrust)
- Matteo Tucker (Entrust)
- Matteo Tucker (Entrust)
- Matteo Tucker (Entrust)

Language: English

ease log in to either sign up for ultifactor authentication, or to administer ur existing account.

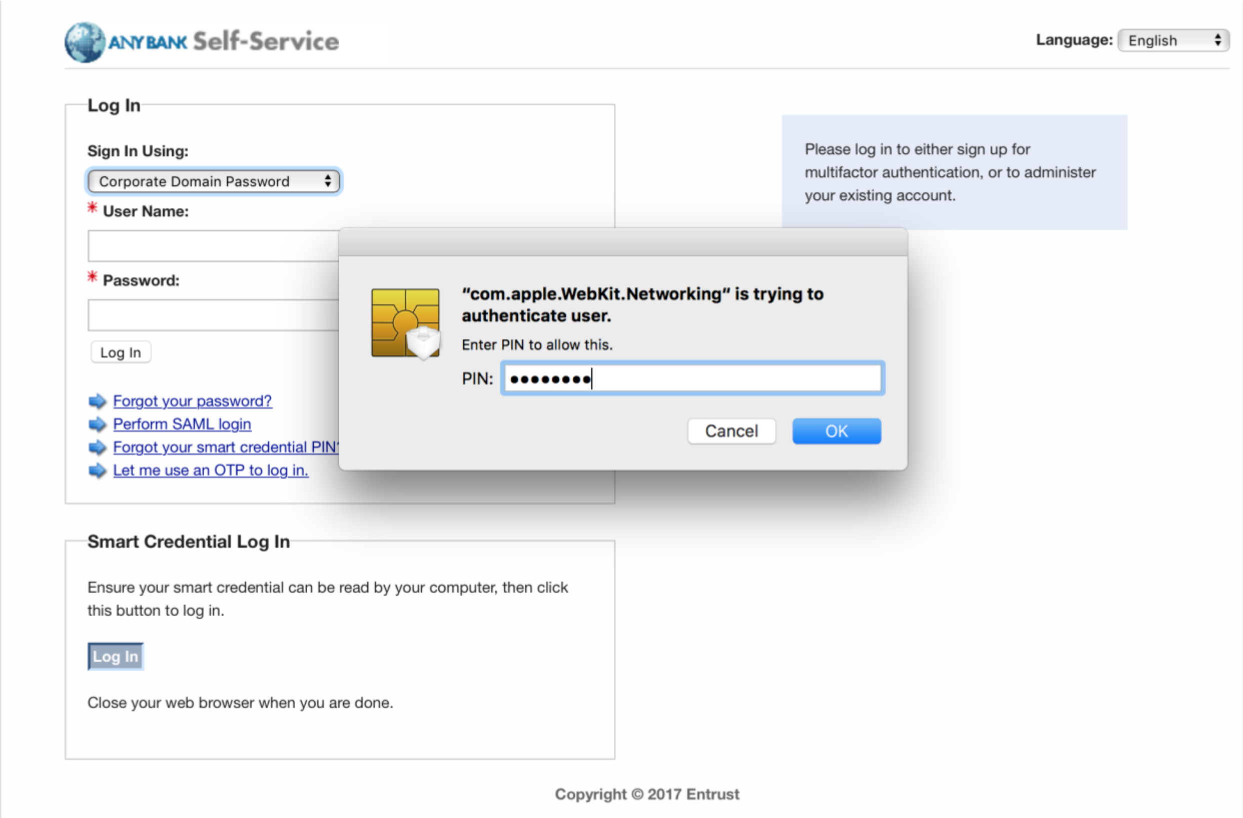
Smart Credential Log In

Ensure your smart credential can be read by your computer, then click this button to log in.

Close your web browser when you are done.

Copyright © 2017 Entrust

Figure 5-2 Password-Based Subscriber Authentication via PIN



ANYBANK Self-Service

Language: English

Log In

Sign In Using: Corporate Domain Password

* User Name:

* Password:

Log In

Forgot your password?
Perform SAML login
Forgot your smart credential PIN
Let me use an OTP to log in.

Please log in to either sign up for multifactor authentication, or to administer your existing account.

"com.apple.WebKit.Networking" is trying to authenticate user.

Enter PIN to allow this.

PIN: ●●●●●●●●●

Cancel OK

Smart Credential Log In

Ensure your smart credential can be read by your computer, then click this button to log in.

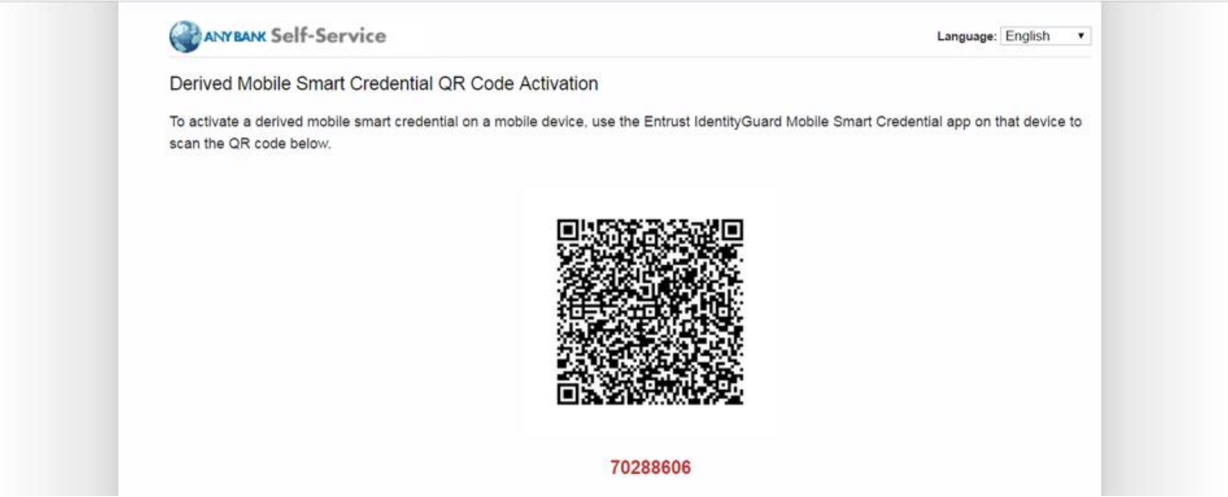
Log In

Close your web browser when you are done.

Copyright © 2017 Entrust

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

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



Derived Mobile Smart Credential QR Code Activation

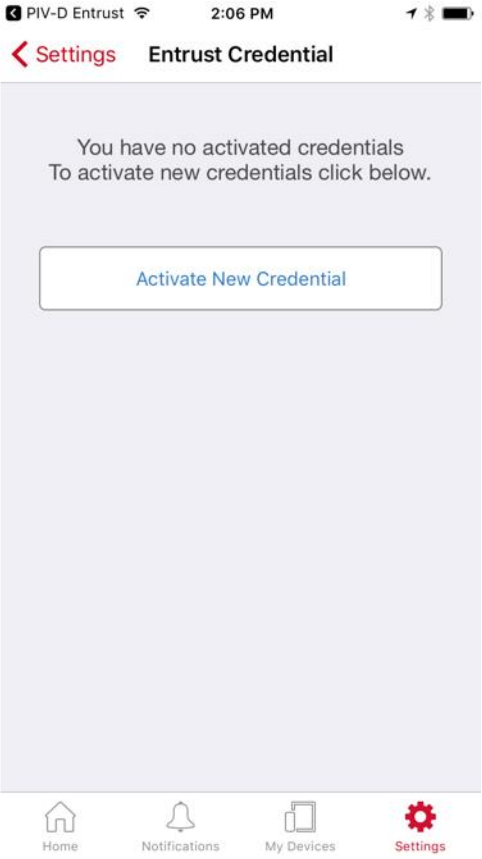
To activate a derived mobile smart credential on a mobile device, use the Entrust IdentityGuard Mobile Smart Credential app on that device to scan the QR code below.

70288606

853

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

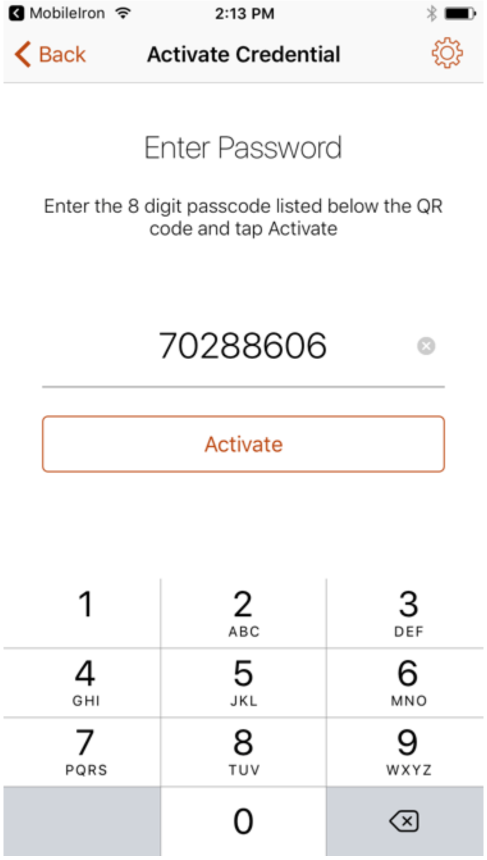
856 **Figure 5-4 MobileIron PIV-D Entrust App**



You have no activated credentials
To activate new credentials click below.

857

Figure 5-5 Entrust DPC Activation



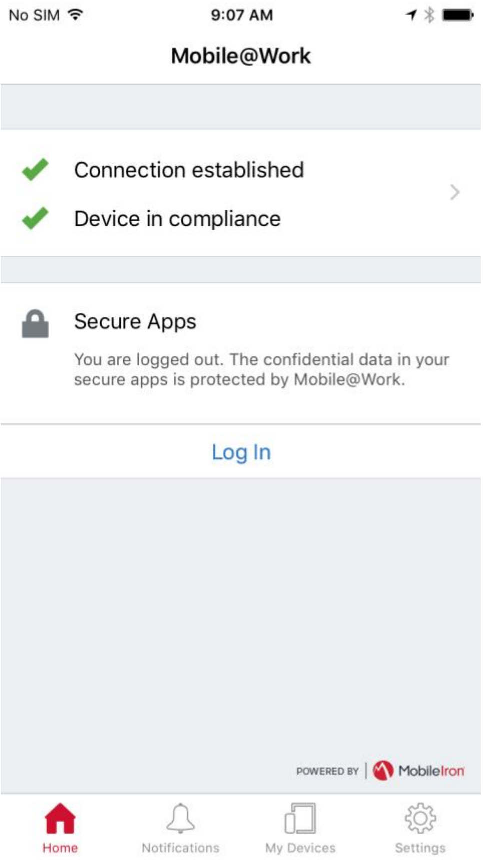
Enter Password

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

70288606

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

Figure 5-6 PIV-D Application



No SIM 9:07 AM

Mobile@Work

✓ Connection established

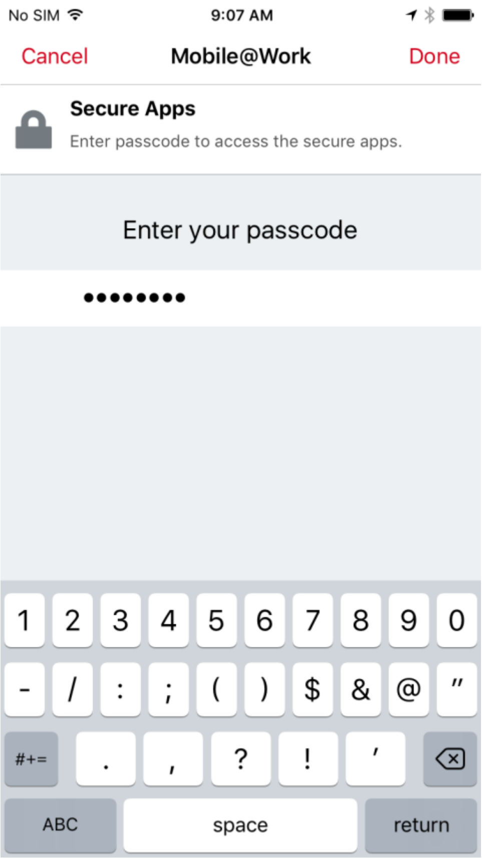
✓ Device in compliance

Secure Apps

You are logged out. The confidential data in your secure apps is protected by Mobile@Work.

Log In

Figure 5-7 PIV-D Passcode Entry


No SIM 9:07 AM

Cancel Mobile@Work Done

Secure Apps

Enter passcode to access the secure apps.

Enter your passcode

••••••••

5.2.1.2 Maintenance

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

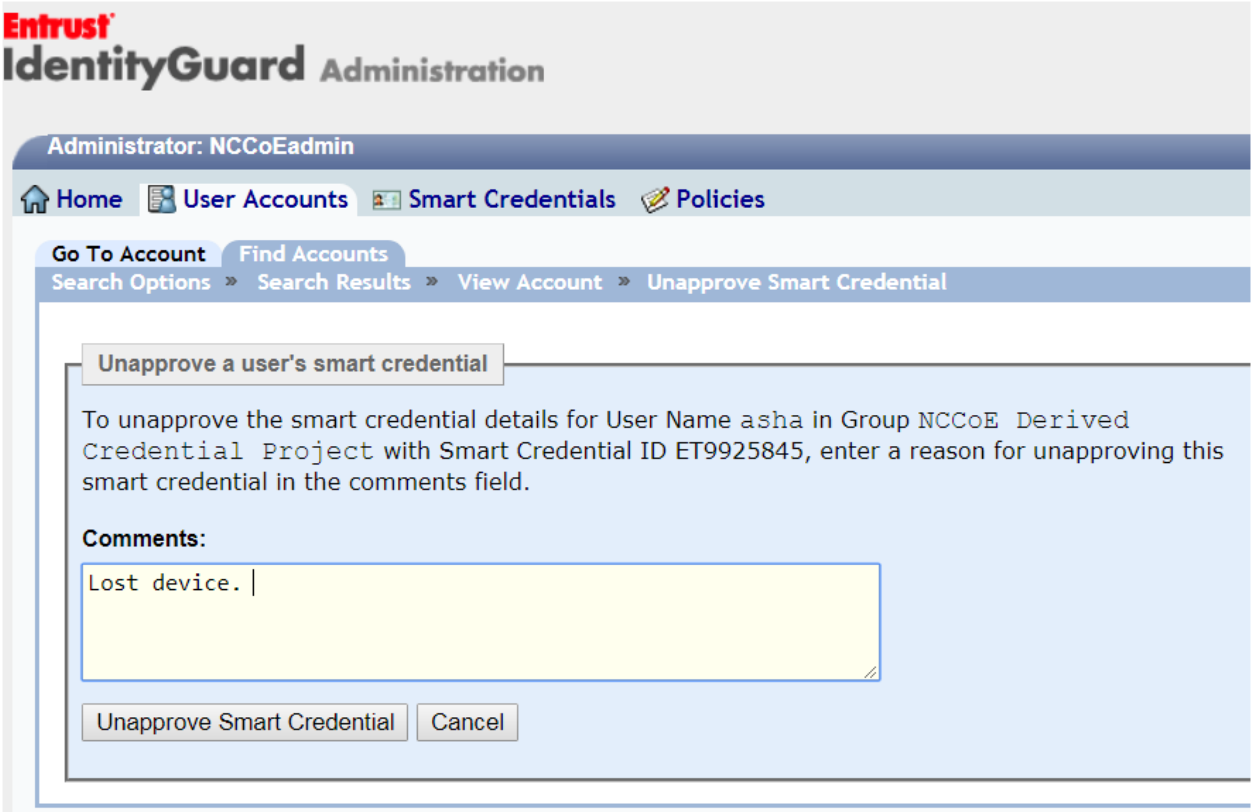
Linkage requirements between the status of the subscriber's PIV Card and DPC are covered by both the CA and CMS being under control of Entrust Datacard. These systems exchange identity management system data, and any necessary changes to the status of the subscriber's DPC will occur automatically.

5.2.1.3 Termination

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

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

Figure 5-8 DPC IdentityGuard Termination


Entrust
IdentityGuard Administration
Administrator: NCCoEadmin
Home
User Accounts
Smart Credentials
Policies
Go To Account
Find Accounts
Search Options » Search Results » View Account » Unapprove Smart Credential
Unapprove a user's smart credential

To unapprove the smart credential details for User Name asha in Group NCCoE Derived Credential Project with Smart Credential ID ET9925845, enter a reason for unapproving this smart credential in the comments field.

Comments: Lost device.

Unapprove Smart Credential
Cancel

5.2.1.4 DPC Authentication Certificate Management

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

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

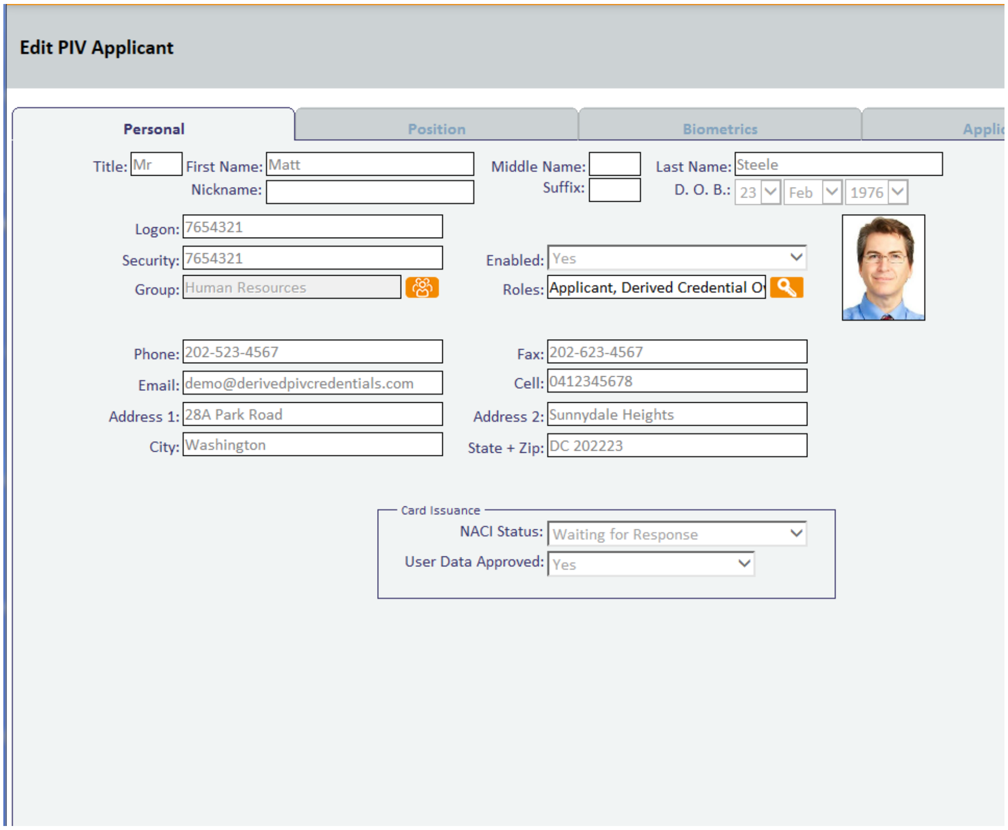
Standards (PKCS) #10 format over PKIX-CMP. The Entrust Datacard Managed CA returns the signed DPC certificate to the Entrust IdentityGuard service.

5.2.2 Hybrid Architecture Build Testing

5.2.2.1 Initial Issuance

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

Figure 5-9 Test PIV Card User



Edit PIV Applicant

Title: Mr First Name: Matt Middle Name: Last Name: Steele
Nickname: Suffix: D. O. B.: 23 Feb 1976

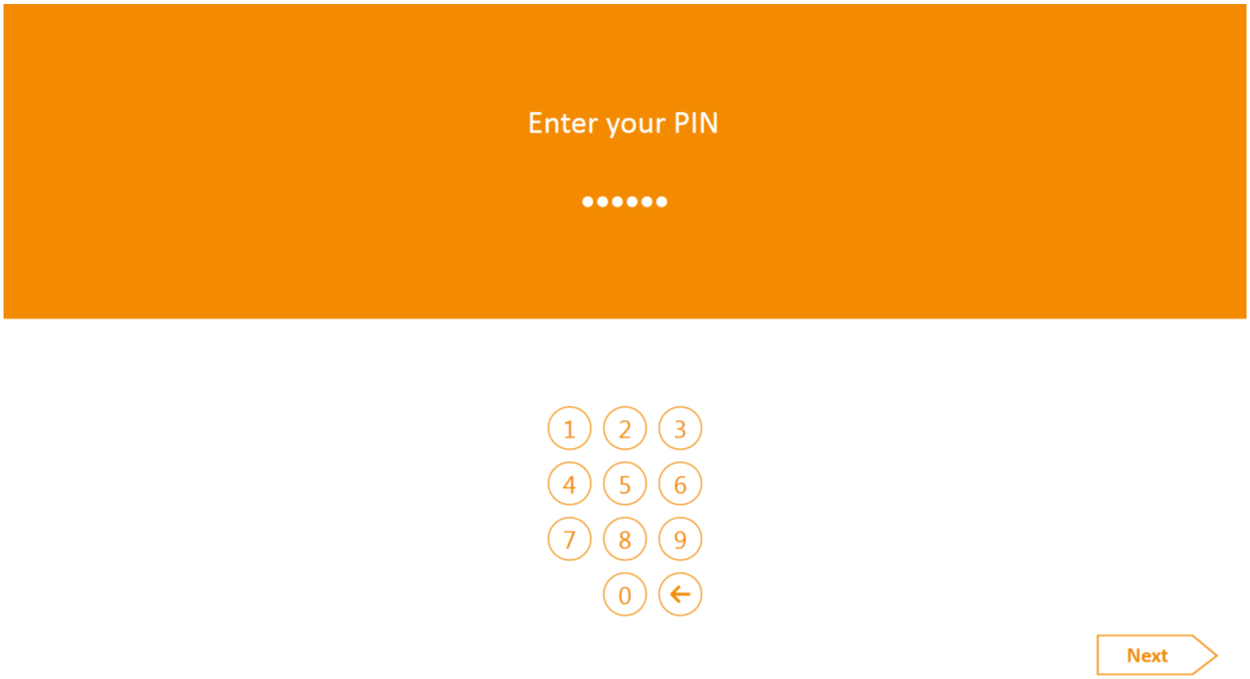
Logon: 7654321
Security: 7654321 Enabled: Yes
Group: Human Resources Roles: Applicant, Derived Credential O

Phone: 202-523-4567 Fax: 202-623-4567
Email: demo@derivedpivcredentials.com Cell: 0412345678
Address 1: 28A Park Road Address 2: Sunnydale Heights
City: Washington State + Zip: DC 202223

Card Issuance
NACI Status: Waiting for Response
User Data Approved: Yes

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

Figure 5-10 Kiosk Workflow


Enter your PIN

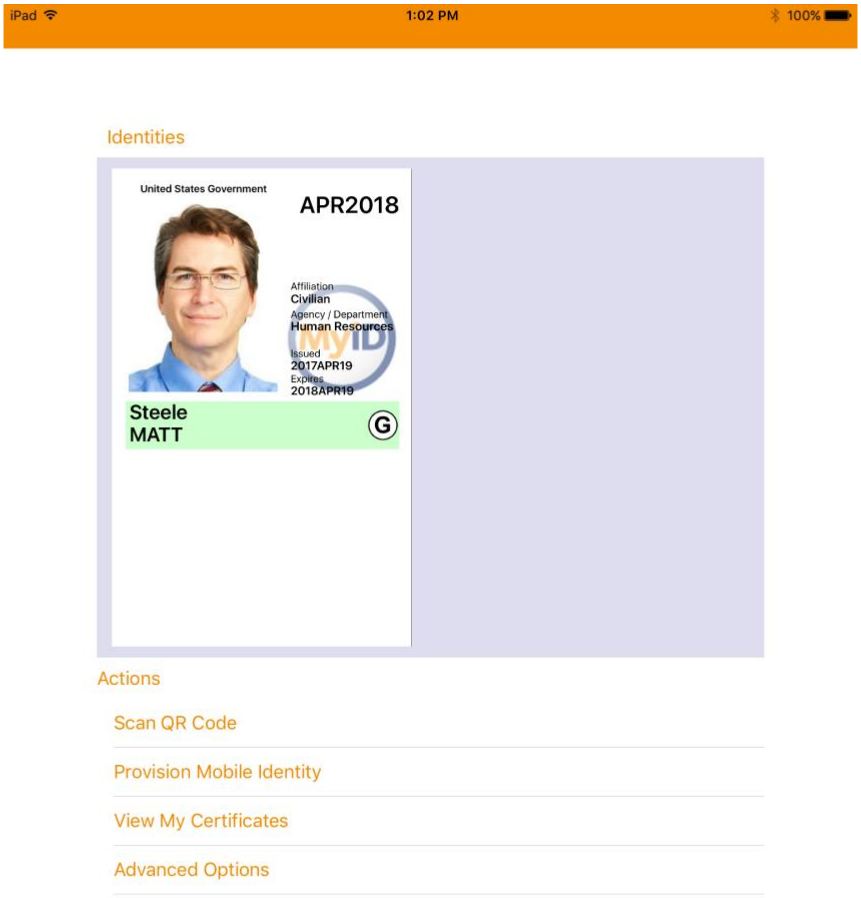
●●●●●●

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

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

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

Figure 5-11 DPC in MyID Identity Agent



United States Government

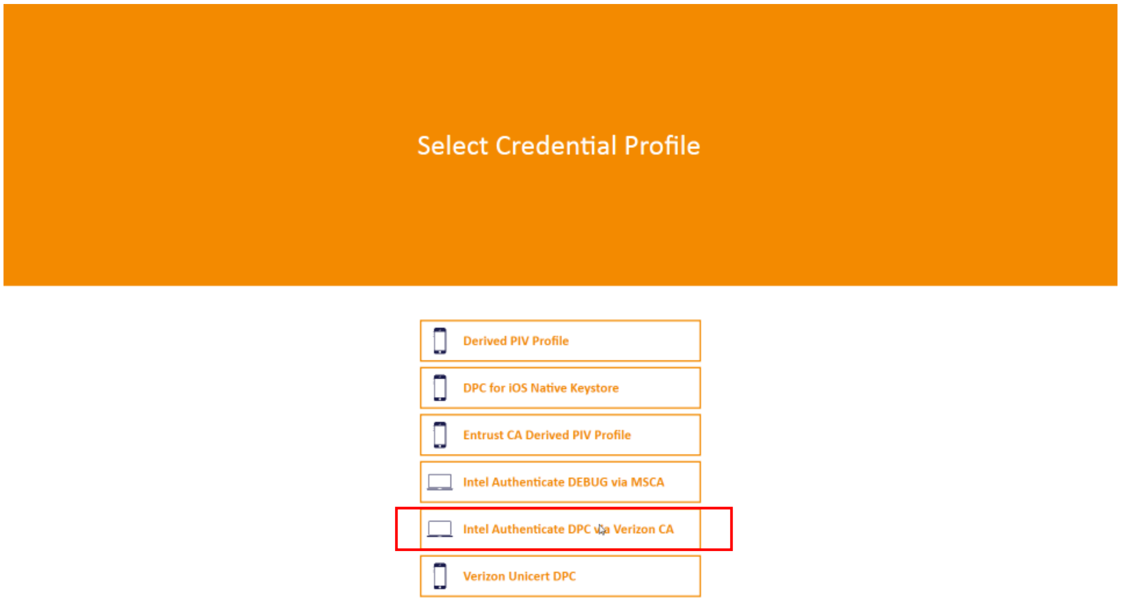
APR2018

Affiliation
Civilian
Agency / Department
Human Resources
Issued
2017APR19
Expires
2018APR19

Steele
MATT

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

Figure 5-12 DPC Applicant Chooses Intel Credential Profile

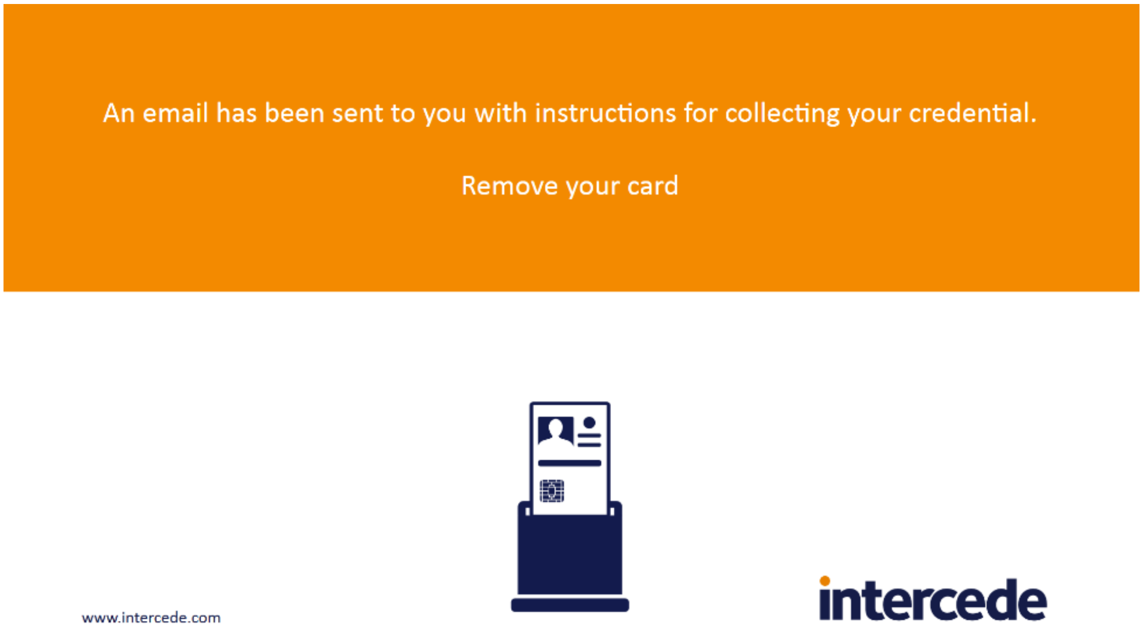


Select Credential Profile

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

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

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

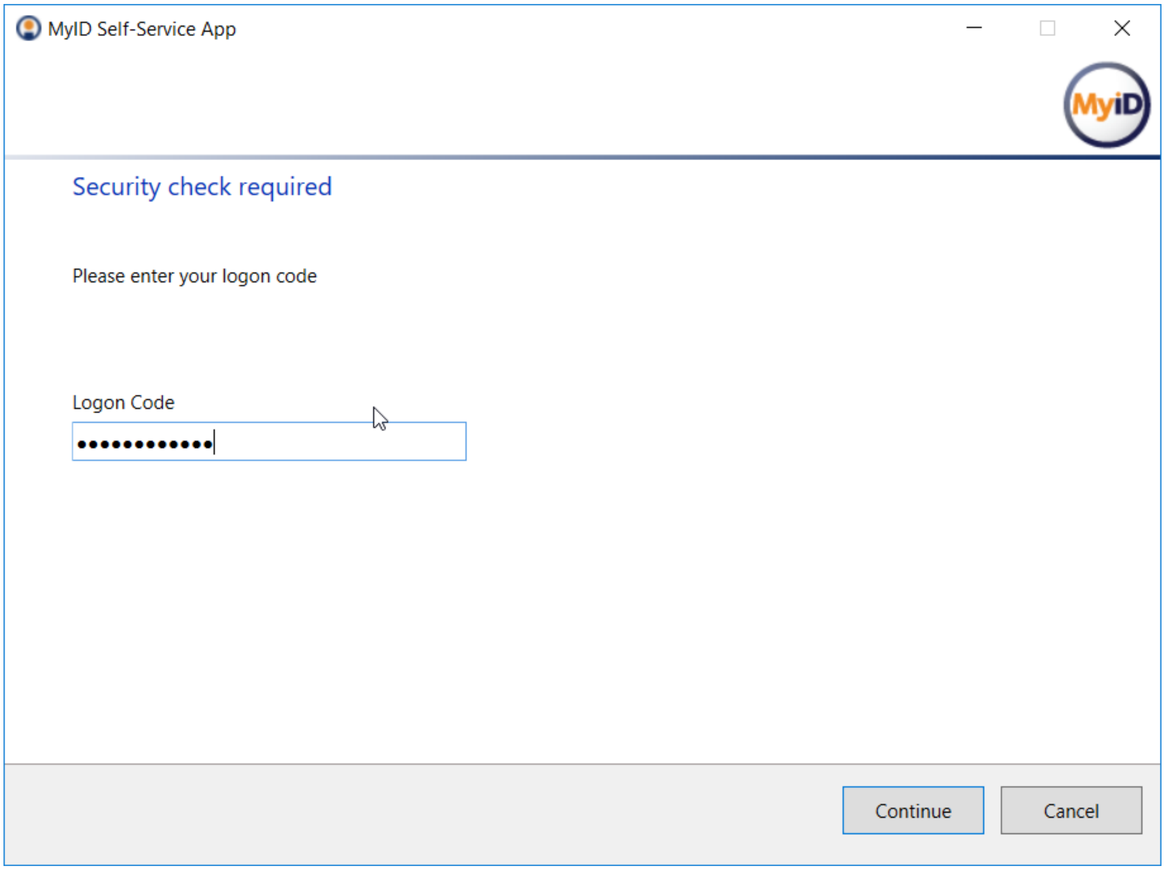


An email has been sent to you with instructions for collecting your credential.

Remove your card

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

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



Security check required

Please enter your logon code

Logon Code: ••••••••••••

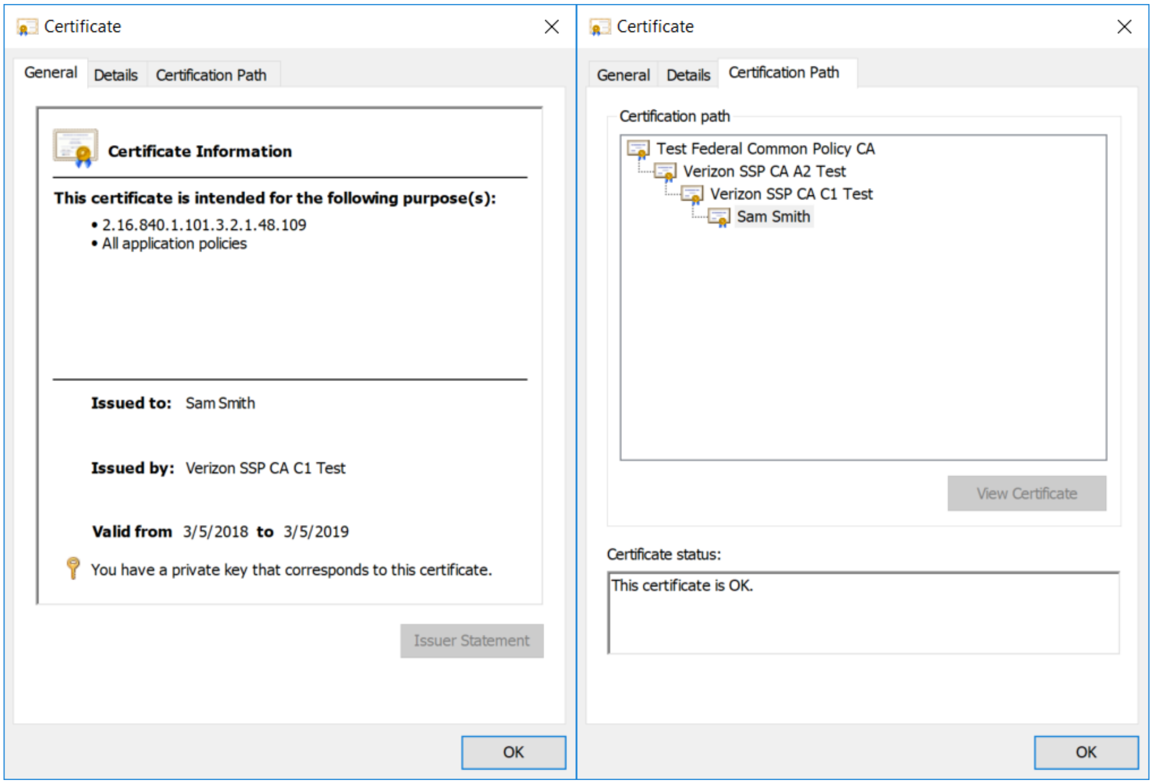
Once the DPC credential is issued to the Intel Authenticate token, it can be activated only by using a PIN set by the DPC applicant through the Intel Authenticate client (see Part C for details). The client allows the user to choose one or more additional *factors* to protect PKI-based keys; however,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

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

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

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

Figure 5-15 Verizon SSP DPC Authentication Certificate



Certificate Information

This certificate is intended for the following purpose(s):

- 2.16.840.1.101.3.2.1.48.109
- All application policies

Issued to: Sam Smith

Issued by: Verizon SSP CA C1 Test

Valid from 3/5/2018 to 3/5/2019

You have a private key that corresponds to this certificate.

Certification path

- Test Federal Common Policy CA
  - Verizon SSP CA A2 Test
    - Verizon SSP CA C1 Test
      - Sam Smith

Certificate status:

This certificate is OK.

5.2.2.2 Maintenance

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

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

5.2.2.3 Termination

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

5.2.2.4 DPC Authentication Certificate Management

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

5.3 Scenarios and Findings

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

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

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

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

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

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

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

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

5.3.2 PR.AC-3: Remote Access Is Managed

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

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

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

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

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

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

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

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

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

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

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

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

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

5.4 Authenticator AAL Mapping

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

Table 4-1.

Table 5-2 AAL-2 Authenticator Requirements Mapping

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

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

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

Table 5-3 AAL Technology Mappings

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

6 Future Build Considerations

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

- **Application Enablement –** To leverage DPC, an organization needs to enable applications on its mobile devices and from the relying-party perspective. Mobile device application development is complicated by the various operating systems, cryptographic token options, and third-party software development kits provided by software containers. Further, modifying the source code of third-party closed mobile applications can be difficult or impossible. Relying parties face similar challenges with legacy systems that can be difficult to make ready for DPC. Future work might focus on adopting native embedded cryptographic tokens provided by hardware manufacturers and on using federations for relying parties such as cloud service providers.

- **Architecture Expansion –** Integrate with an identity management system (IDMS), which retains identity data that is retrieved from authoritative sources, to provide DPC subscriber PIV eligibility status information. NIST SP 800-157 recommends that the issuer of the DPC prevent further use of the DPC when the subscriber is no longer eligible for a PIV Card. Integration with an IDMS would store the eligibility of the DPC subscriber to help determine when DPC could be revoked, and it allows for DPC status to remain independent of the PIV Card status. This is helpful in the case of lost or stolen cards to allow a DPC subscriber to keep working without a PIV Card.
- **Key Management Key Recovery –** Mobile users should be able to recover key management keys from escrow. Unlike a signature key, the same key management key that is stored on the PIV Card is necessary to decrypt encrypted email stored on the device, for example.

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

Appendix A List of Acronyms

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

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

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

Appendix B Glossary

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

applicant An individual who has applied for, but has not yet been issued, a Derived PIV Credential.

asymmetric keys Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

authenticated protected channel An encrypted channel that uses approved cryptography where the connection initiator (client) has authenticated the recipient (server).

authentication The process of establishing confidence of authenticity. In this case, it is the validity of a person's identity and the PIV Card.

card An integrated circuit card.

cardholder An individual possessing an issued PIV Card.

card management system The system that manages the life cycle of a PIV Card application.

card reader An electronic device that connects an integrated circuit card and the card applications therein to a client application.

certificate revocation list A list of revoked public key certificates created and digitally signed by a certification authority.

Certification Authority A trusted entity that issues and revokes public key certificates.

credential Evidence attesting to one's right to credit or authority. In this standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.

cryptographic key (key) A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

demilitarized zone Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's information assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Derived PIV Application A standardized application residing on a removable hardware cryptographic token that hosts a Derived PIV Credential and associated mandatory and optional elements.

Derived PIV Credential An X.509 Derived PIV Authentication certificate with associated public and private key that is issued in accordance with the requirements specified in this document where the PIV Authentication certificate on the applicant's PIV Card serves as the original credential. The Derived PIV Credential is an additional common identity credential under HSPD-12 and FIPS 201 that is issued by a federal department or agency and is used with mobile devices.

e-authentication assurance level A measure of trust or confidence in an authentication mechanism defined in publications OMB-04-04 and NIST SP 800-63 in terms of four levels:

- Level 1: LITTLE OR NO confidence
- Level 2: SOME confidence
- Level 3: HIGH confidence
- Level 4: VERY HIGH confidence

Federal Information Processing Standards A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST. A FIPS covers a specific topic in information technology to achieve a common level of quality or some level of interoperability.

identity The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

identity management system One or more systems or applications that manage the identity verification, validation, and issuance process.

identity proofing The process of providing sufficient information (e.g., identity history, credentials, documents) to establish an identity.

identity verification The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those credentials previously proven and stored in the PIV Card or system and associated with the identity being claimed.

issuer The organization that is issuing the PIV Card (or DPC) to an applicant. Typically, this is an organization for which the applicant is working.

level of assurance OMB Memorandum M-04-04 describes four levels of identity assurance and references NIST technical standards and guidelines, which are developed for agencies to use in identifying the appropriate authentication technologies that meet their requirements.

mobile device A portable computing device that (1) has a small form factor so it can easily be carried by a single individual; (2) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (3) possesses local, non-removable or removable data storage; and (4) includes a self-contained power source. Mobile devices may also include voice communication capabilities, onboard sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and e-readers.

multifactor authentication Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

personal identification number A secret number that a cardholder memorizes and uses to authenticate his or her identity as part of multifactor authentication.

personal identity verification (card) A physical artifact (e.g., identity card, “smart” card) issued to an individual, which contains a PIV Card application that stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable).

PKI-PIV Authentication key (PKI-AUTH) A PIV Authentication mechanism that is implemented by an asymmetric key challenge/response protocol by using the PIV Authentication key of the PIV Card and a contact reader or a contactless card reader that supports the virtual contact interface.

private key The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

public key The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

public key infrastructure A support service to the PIV System that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of enterprise data.

sponsor Submits a Derived PIV Credential request on behalf of the applicant.

subscriber The individual who is the subject named or identified in a Derived PIV Authentication certificate and who holds the token that contains the private key that corresponds to the public key in the certificate.

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

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

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

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

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

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

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

Appendix D References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NIST SPECIAL PUBLICATION 1800-12C

Derived Personal Identity Verification (PIV) Credentials

Volume C:
How-To Guides

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

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

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

August 2018

SECOND DRAFT

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

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-12C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-12C, 151 pages, (August 2018), CODEN: NSPUE2

FEEDBACK

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

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

Public comment period: 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.

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

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

Name	Organization
Matthew Steele	The MITRE Corporation

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

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

Contents

List of Figures

List of Tables

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 1800-12B: *Approach, Architecture, and Security Characteristics* – what we built and why
- 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.

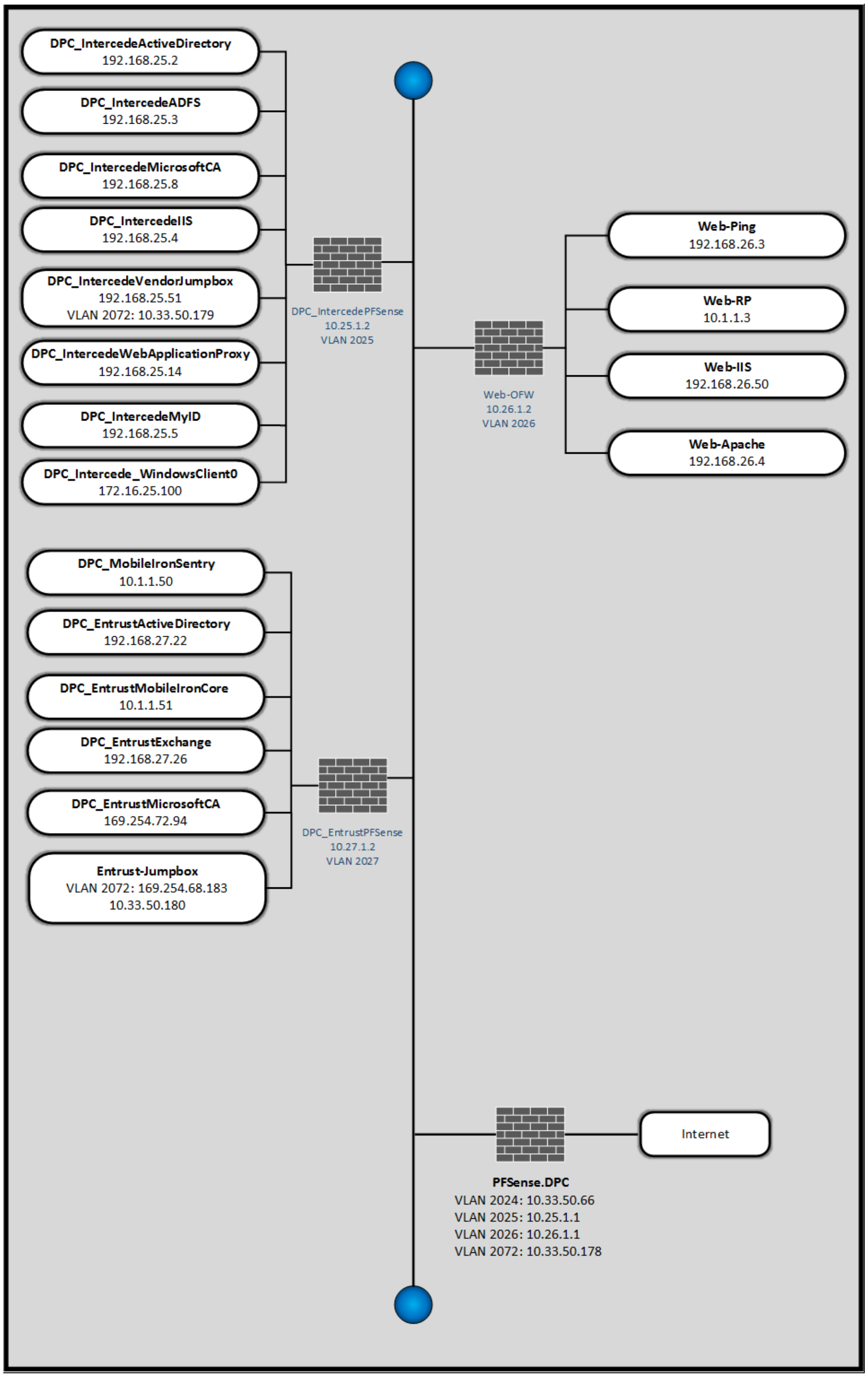
1.2 Build Overview

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.

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

2 Product Installation Guides

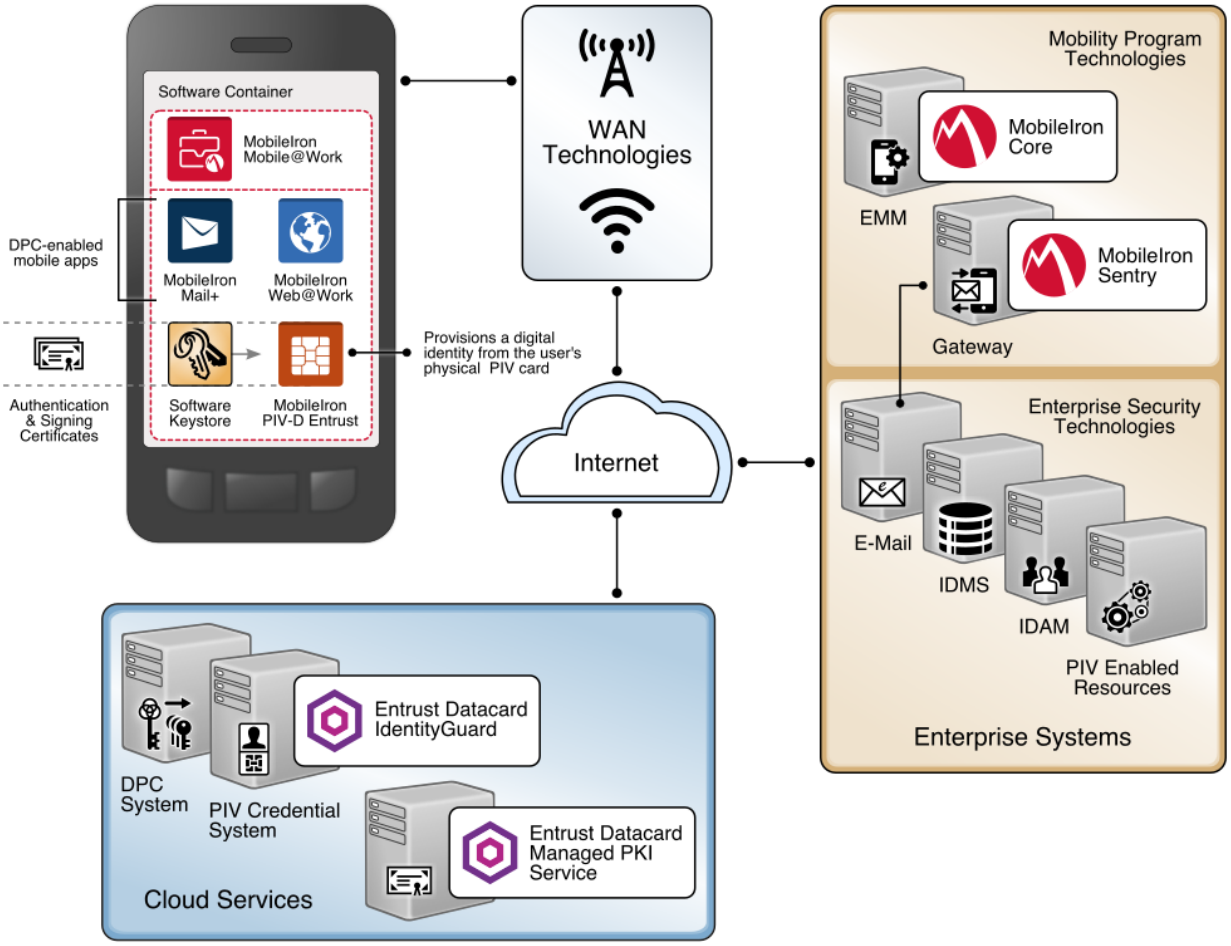
This section of the practice guide contains detailed instructions for installing and configuring key products used for the depicted architectures documented below, as well as demonstration of the DPC lifecycle management activities of initial issuance and termination.

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



2.1.1 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/).

2.1.1.1 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 2-1 Identity Management Profiles

User Name	Email Address	User Principal Name (UPN)
Patel, Asha	asha@entrust.dpc.nccoe.org	asha@entrust.dpc.nccoe.org
Tucker, Matteo	matteo@entrust.dpc.nccoe.org	matteo@entrust.dpc.nccoe.org

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 2-2 MobileIron Core Settings

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

2.1.2.1 Installation

Follow the steps below to install MobileIron Core:

1. Obtain a copy of the *On-Premise Installation Guide for MobileIron Core, Sentry, and Enterprise Connector* from the MobileIron support portal.

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.

1. Obtain a copy of *MobileIron Core Device Management Guide for iOS Devices* from the MobileIron support portal.
2. Complete all instructions provided in Chapter 1, Setup Tasks.

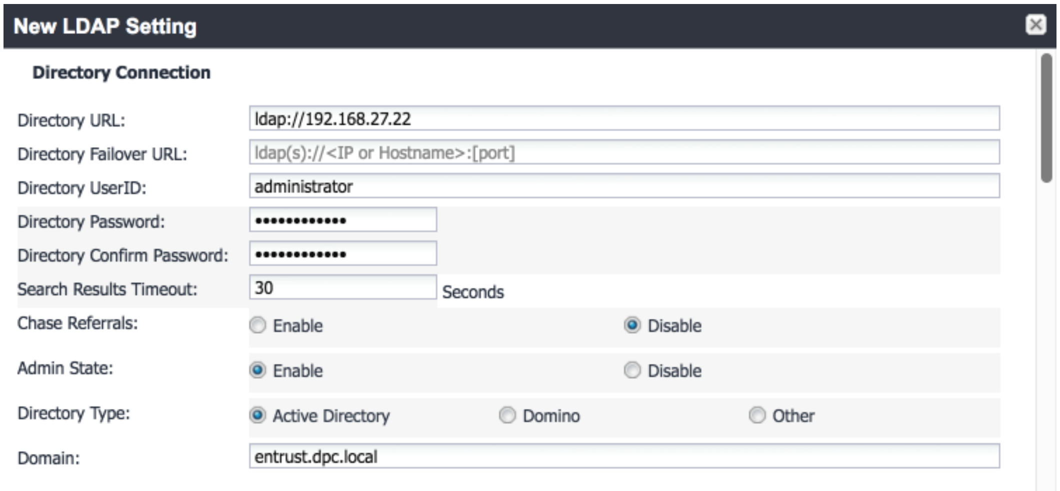
2.1.2.3 Configuration of MobileIron Core for DPC

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:

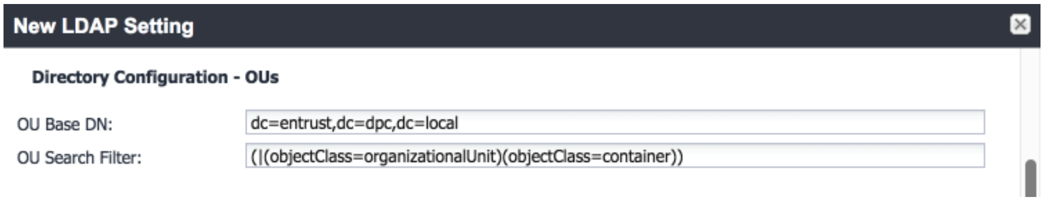


New LDAP Setting

Directory Connection

Directory URL: ldap://192.168.27.22
Directory Failover URL: ldap(s)://<IP or Hostname>:[port]
Directory UserID: administrator
Directory Password: •••••••••••••
Directory Confirm Password: •••••••••••••
Search Results Timeout: 30 Seconds
Chase Referrals: ○ Enable ● Disable
Admin State: ● Enable ○ Disable
Directory Type: ● Active Directory ○ Domino ○ Other
Domain: entrust.dpc.local

b. Directory Configuration—OUs:

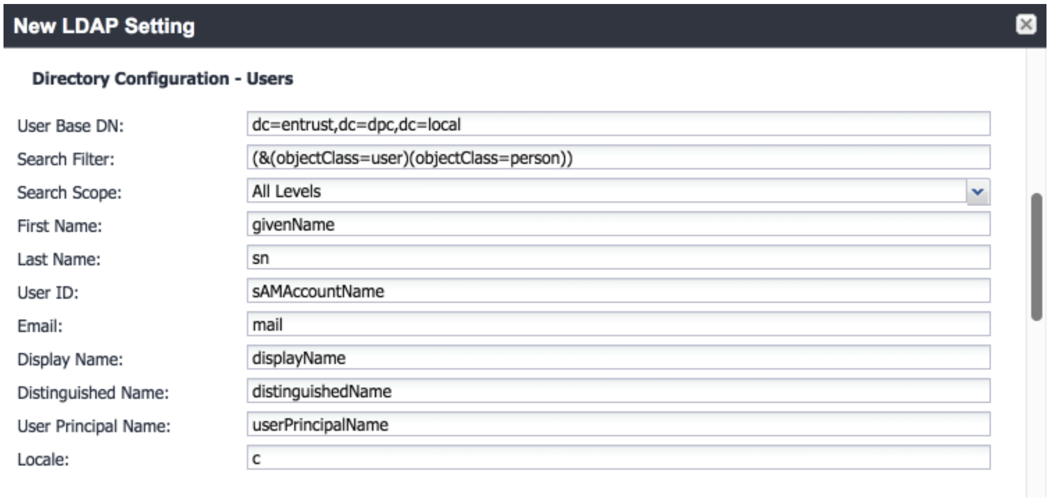


New LDAP Setting

Directory Configuration - OUs

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

c. Directory Configuration—Users:

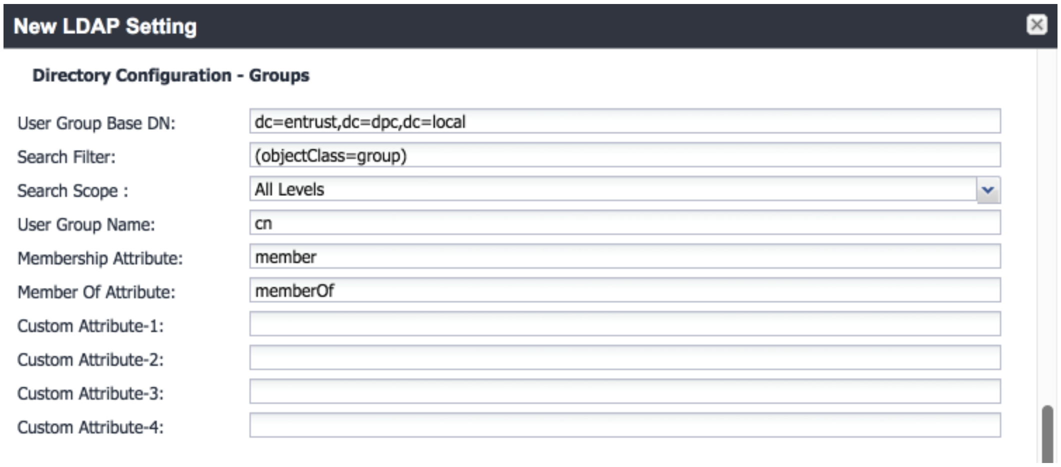


New LDAP Setting

Directory Configuration - 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

d. Directory Configuration—Groups:



New LDAP Setting

Directory Configuration - 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:	

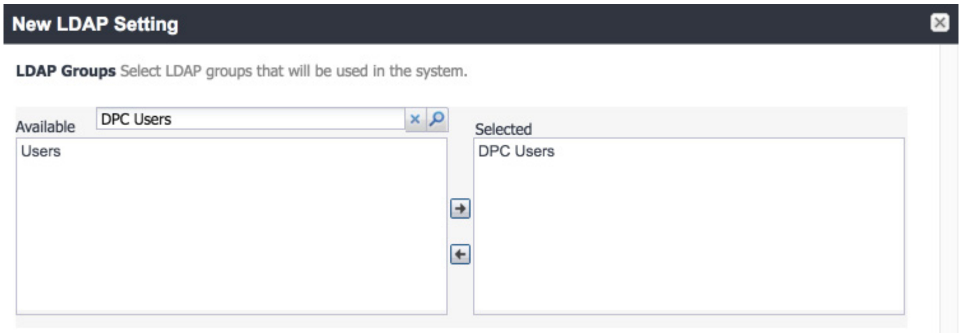
e. LDAP Groups:

   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.



New LDAP Setting

LDAP Groups Select LDAP groups that will be used in the system.

Available: DPC Users

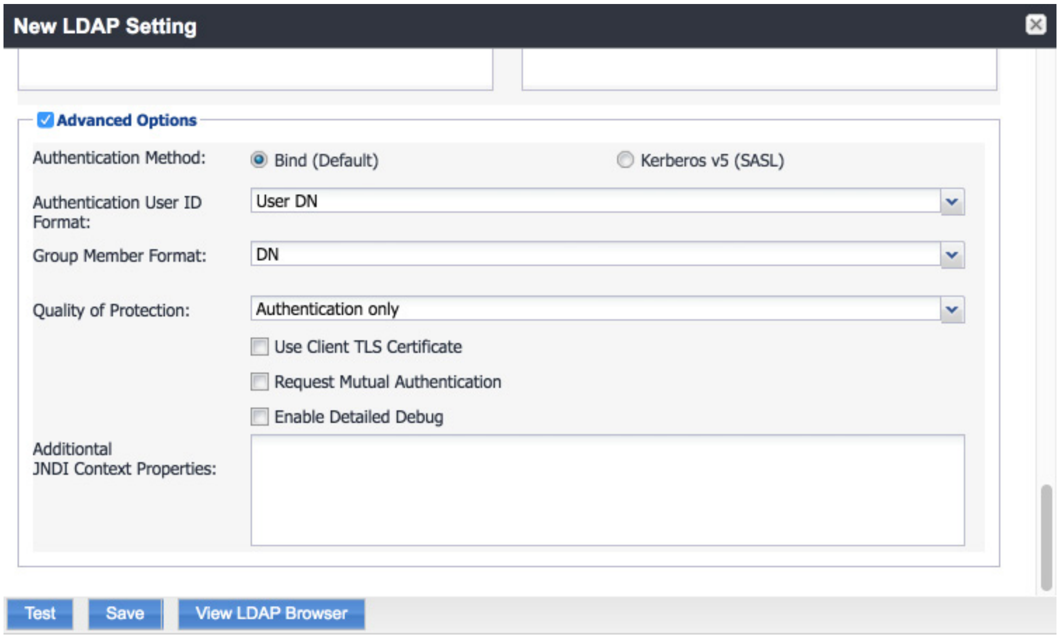
Users

Selected

DPC Users

f. Custom Settings: Custom settings were not specified.

g. Advanced Options:



New LDAP Setting

☑ Advanced Options

Authentication Method: ● Bind (Default) ○ Kerberos v5 (SASL)

Authentication User ID Format: User DN

Group Member Format: DN

Quality of Protection: Authentication only

□ Use Client TLS Certificate

□ Request Mutual Authentication

□ Enable Detailed Debug

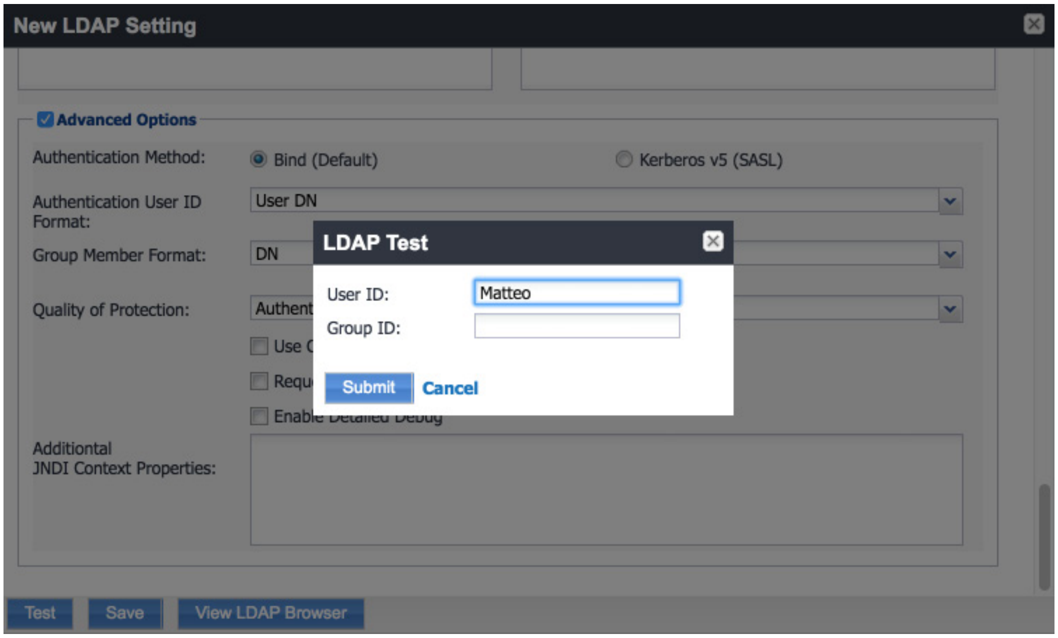
Additiontal JNDI Context Properties:

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**.



☑ Advanced Options

Authentication Method: ● Bind (Default) ○ Kerberos v5 (SASL)

Authentication User ID Format: User DN

Group Member Format: DN

Quality of Protection: Authent

□ Use C

□ Requ

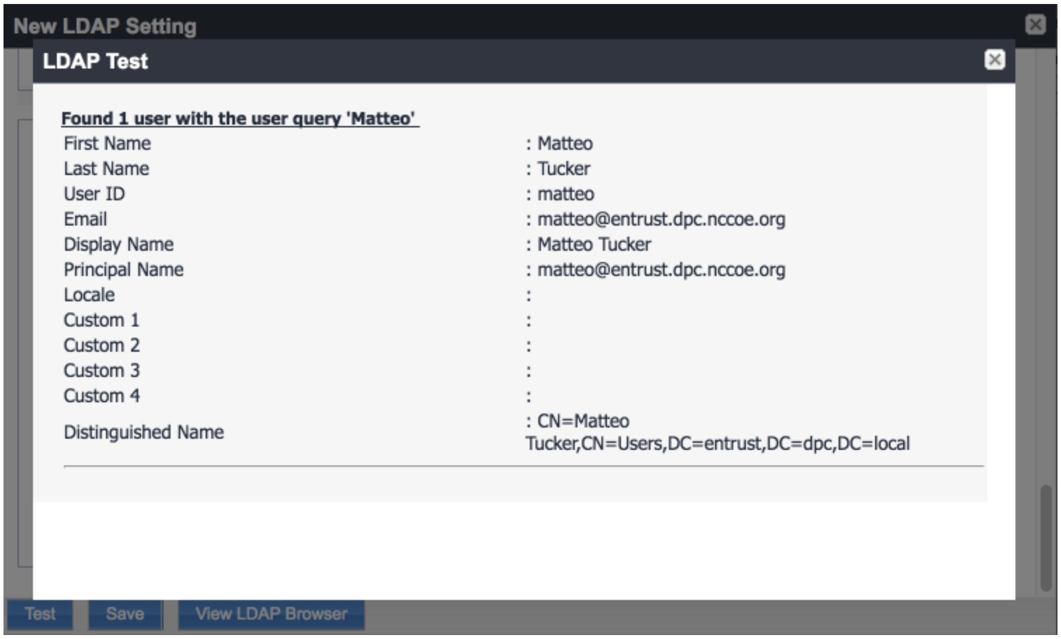
□ Enable Detailed Debug

Additiontal JNDI Context Properties:

User ID: Matteo

Group ID:

c. The **LDAP Test** dialogue indicates the query was successful:



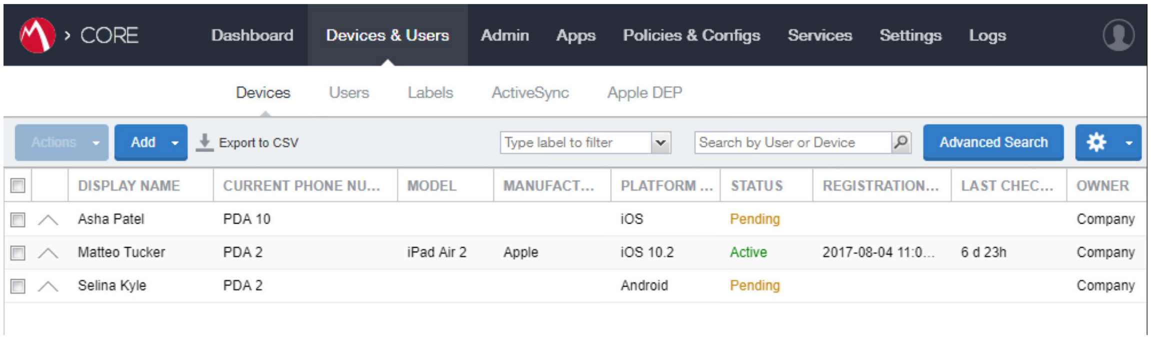
Found 1 user with the user query 'Matteo'

First Name	: Matteo
Last Name	: Tucker
User ID	: matteo
Email	: matteo@entrust.dpc.nccoe.org
Display Name	: Matteo Tucker
Principal Name	: matteo@entrust.dpc.nccoe.org
Locale	:
Custom 1	:
Custom 2	:
Custom 3	:
Custom 4	:
Distinguished Name	: CN=Matteo Tucker,CN=Users,DC=entrust,DC=dpc,DC=local

2.1.2.3.2 Create a DPC Users Label

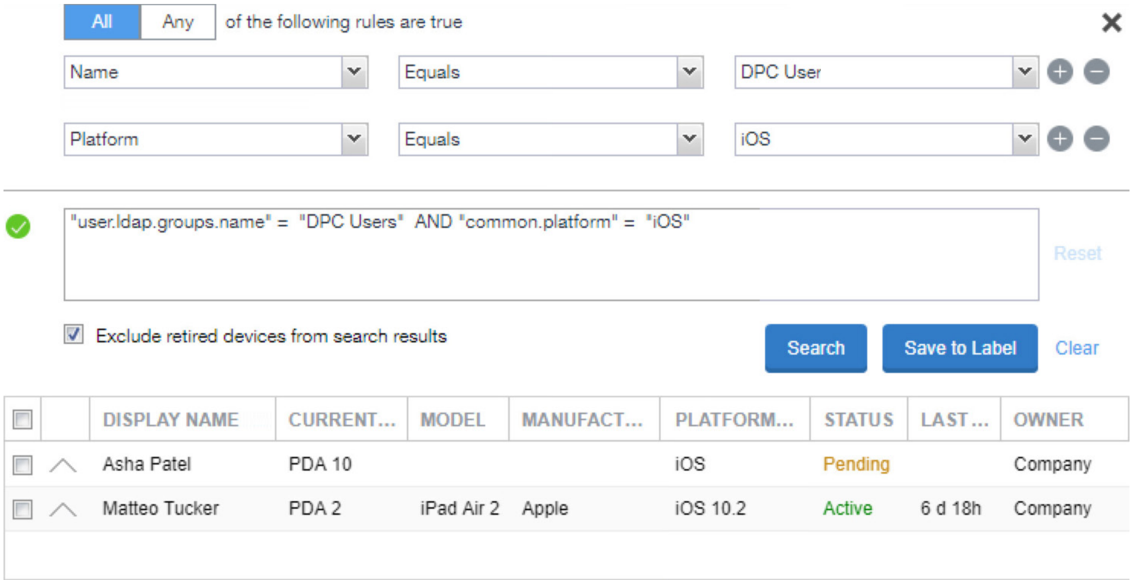
MobileIron uses labels to link policies and device configurations with users and mobile devices. Creating a unique label for DPC users allows mobile device administrators to apply controls relevant for mobile devices provisioned with a derived credential specifically to those devices. We recommend applying 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).



☐		DISPLAY NAME	CURRENT PHONE NU...	MODEL	MANUFACT...	PLATFORM ...	STATUS	REGISTRATION...	LAST CHEC...	OWNER
☐	︿	Asha Patel	PDA 10			iOS	Pending			Company
☐	︿	Matteo Tucker	PDA 2	iPad Air 2	Apple	iOS 10.2	Active	2017-08-04 11:0...	6 d 23h	Company
☐	︿	Selina Kyle	PDA 2			Android	Pending			Company

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**.



All | Any of the following rules are true

Name	Equals	DPC User
Platform	Equals	iOS

```
"user.ldap.groups.name" =  "DPC Users"  AND "common.platform" =  "iOS"
```

☑ Exclude retired devices from search results

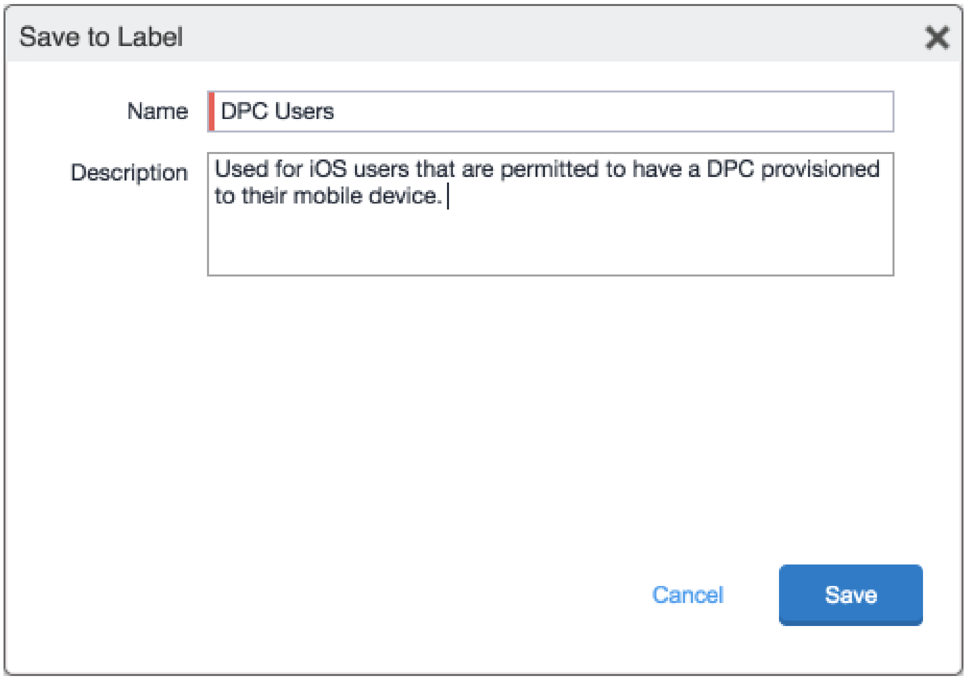
☐		DISPLAY NAME	CURRENT...	MODEL	MANUFACT...	PLATFORM...	STATUS	LAST ...	OWNER
☐		Asha Patel	PDA 10			iOS	Pending		Company
☐		Matteo Tucker	PDA 2	iPad Air 2	Apple	iOS 10.2	Active	6 d 18h	Company

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**.

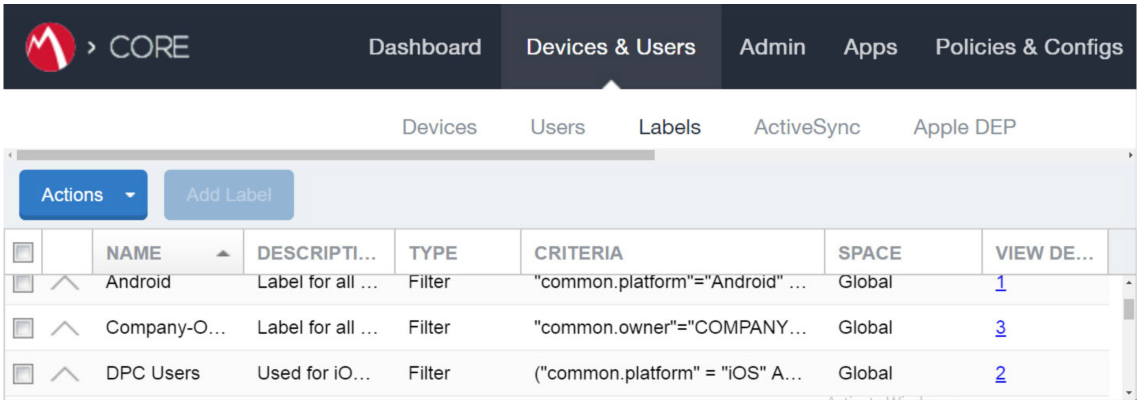


Save to Label

Name: DPC Users

Description: Used for iOS users that are permitted to have a DPC provisioned to their mobile device.

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.



NAME	DESCRIPTI…	TYPE	CRITERIA	SPACE	VIEW DE…
Android	Label for all …	Filter	"common.platform"="Android" …	Global	1
Company-O…	Label for all …	Filter	"common.owner"="COMPANY…	Global	3
DPC Users	Used for iO…	Filter	("common.platform" = "iOS" A…	Global	2

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*.

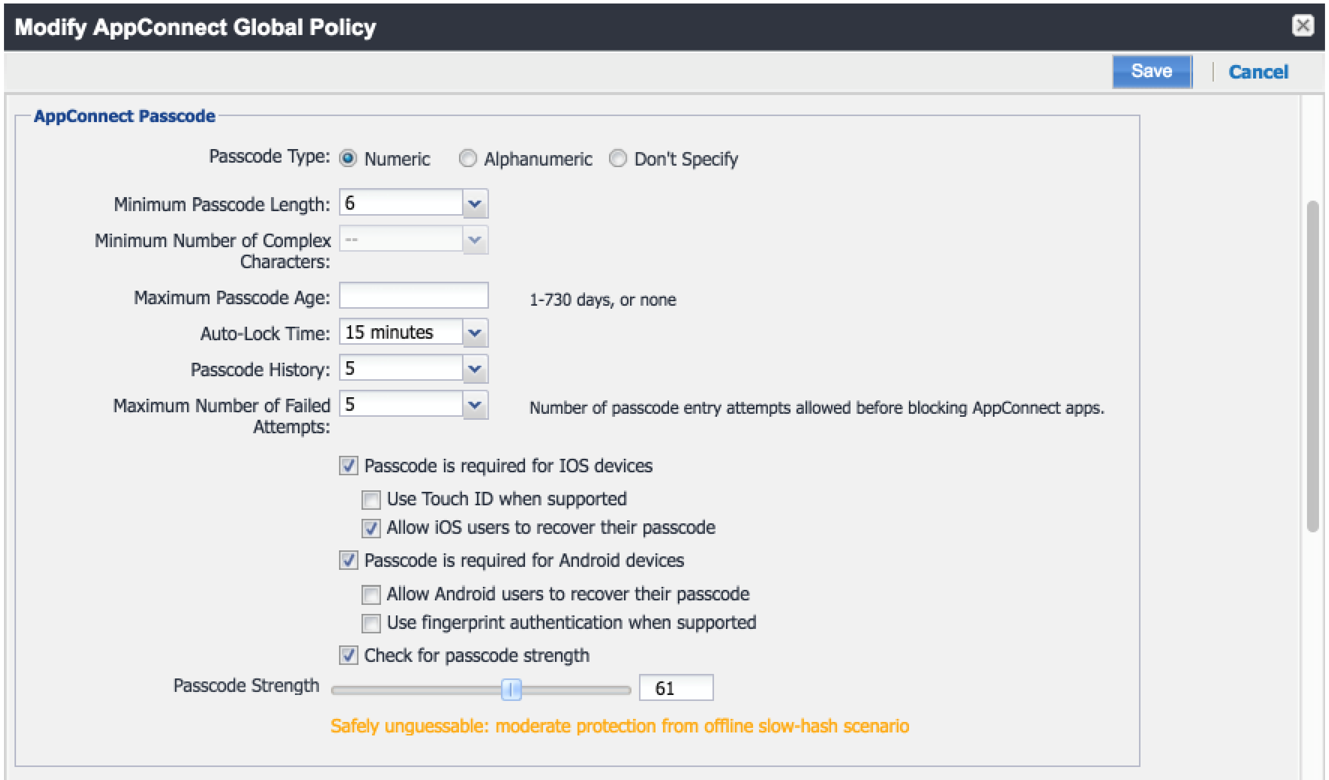
Complete these sections in Chapter 2 of the *MobileIron Derived Credentials with Entrust Guide:*

1. Before beginning:
    a. Configuring certificate authentication to the user portal

       Note: The root CA certificate or trust chain file can be obtained from Entrust Datacard.

    b. 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
    a. Adding Web@Work for iOS
5. Configuring Apps@Work
    a. Setting authentication options
    b. Sending the Apps@Work web clip to devices
6. Configuring AppConnect
    a. Configuring AppConnect licenses
    b. Configuring the AppConnect global policy. The **AppConnect Passcode** policy settings for our implementation are presented below.



AppConnect Passcode

Passcode Type: ● Numeric ○ Alphanumeric ○ Don't Specify

Minimum Passcode Length: 6

Minimum Number of Complex Characters: --

Maximum Passcode Age: 1-730 days, or none

Auto-Lock Time: 15 minutes

Passcode History: 5

Maximum Number of Failed Attempts: 5 Number of passcode entry attempts allowed before blocking AppConnect apps.

☑ Passcode is required for IOS devices

□ Use Touch ID when supported

☑ Allow iOS users to recover their passcode

☑ Passcode is required for Android devices

□ Allow Android users to recover their passcode

□ Use fingerprint authentication when supported

☑ Check for passcode strength

Passcode Strength 61

Safely unguessable: moderate protection from offline slow-hash scenario

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:

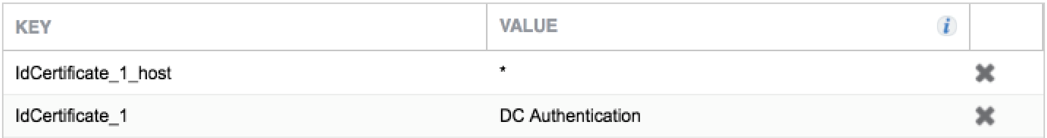
    a. Select **Add New > Certificate Enrollment > SCEP**.

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.



KEY	VALUE	
IdCertificate_1_host	*	✖
IdCertificate_1	DC Authentication	✖

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.

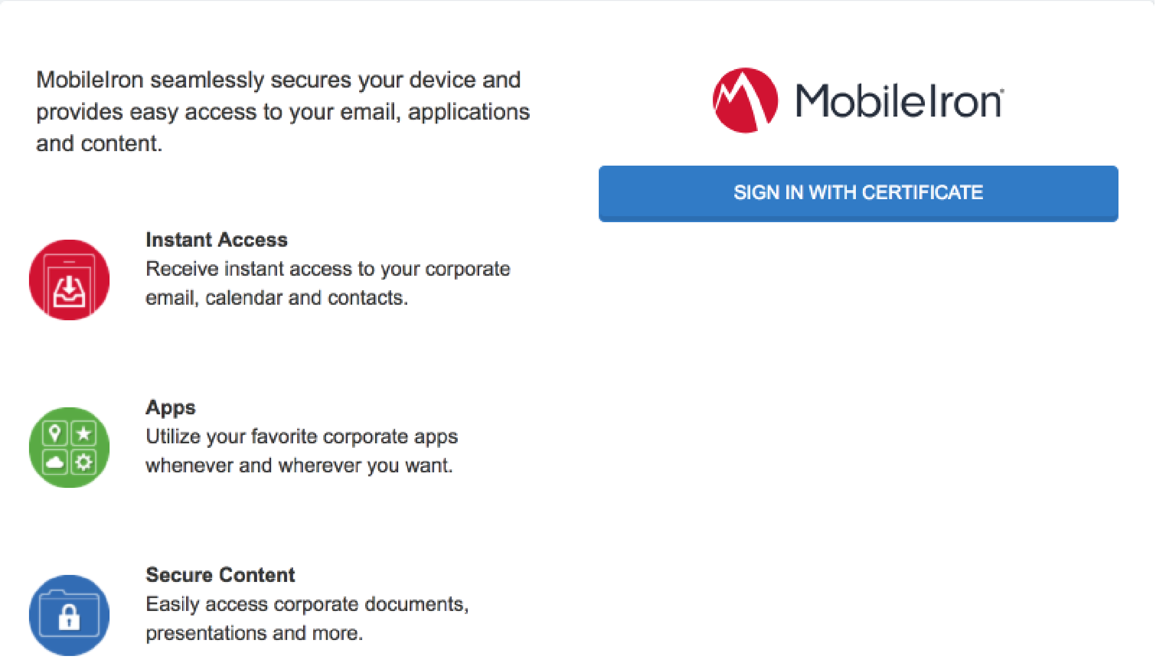
2.1.3.1.1 Register Target Device with MobileIron

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**.



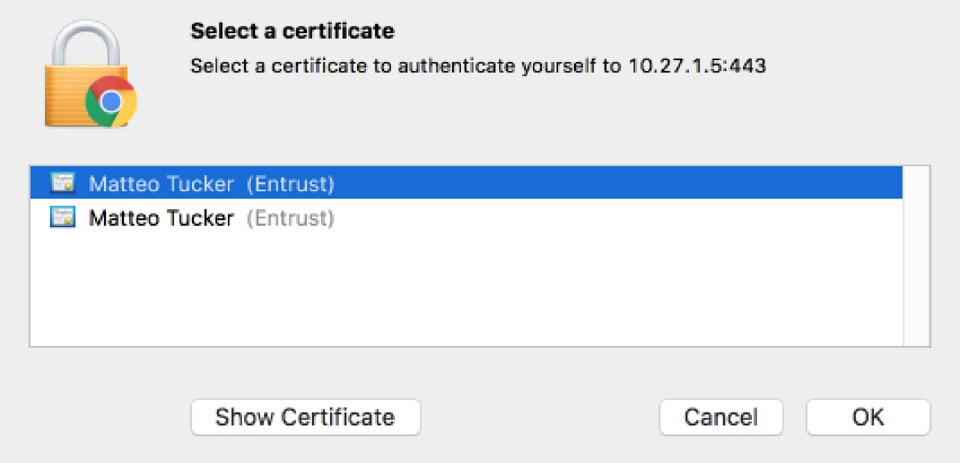
MobileIron seamlessly secures your device and provides easy access to your email, applications and content.

Instant Access
Receive instant access to your corporate email, calendar and contacts.

Apps
Utilize your favorite corporate apps whenever and wherever you want.

Secure Content
Easily access corporate documents, presentations and more.

4. In the certificate selection dialogue:
   a. If necessary, identify your PIV Authentication certificate:
      i. Highlight a certificate.
      ii. Select **Show Certificate**.



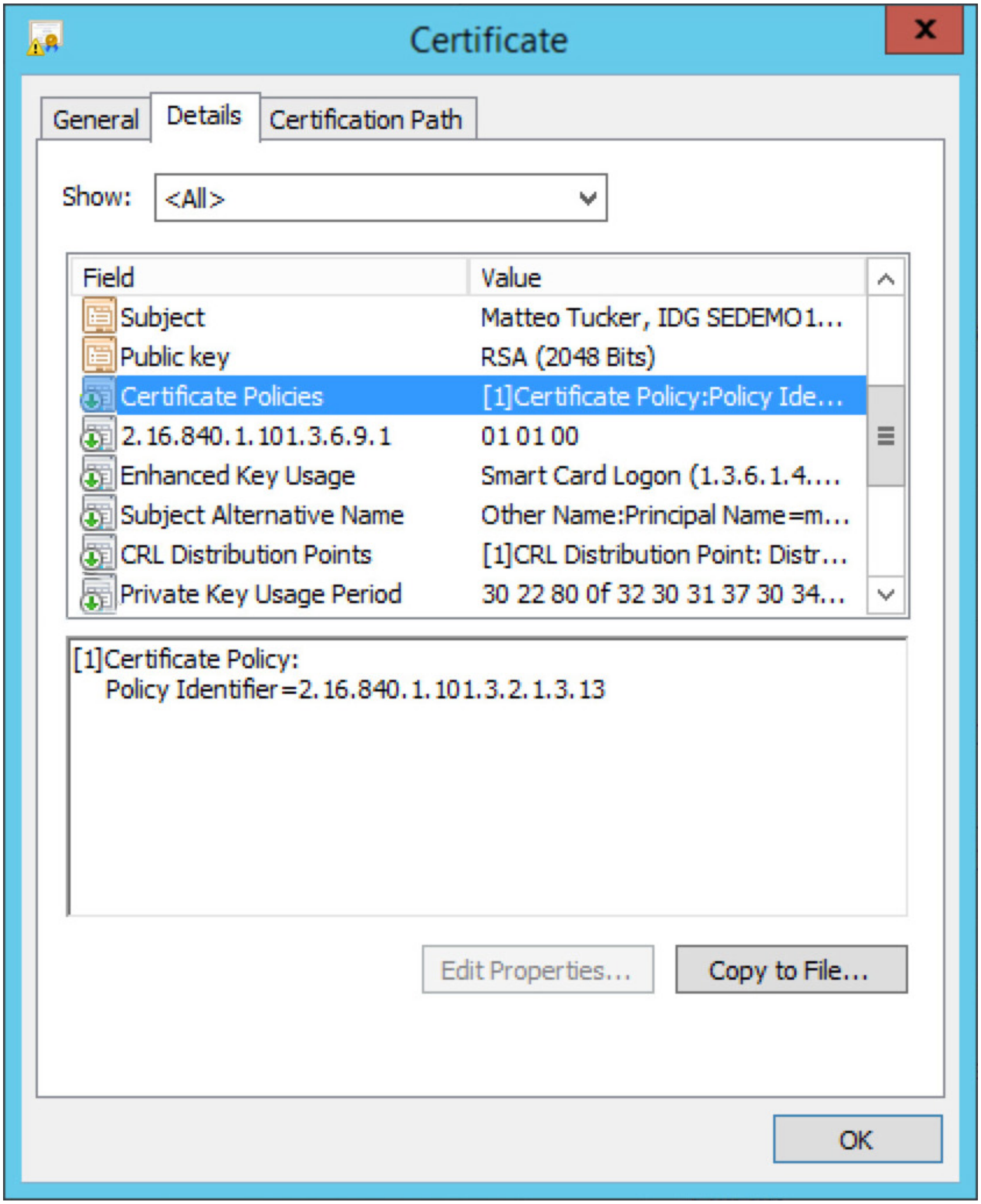
Select a certificate
Select a certificate to authenticate yourself to 10.27.1.5:443

Matteo Tucker (Entrust)
Matteo Tucker (Entrust)

      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.



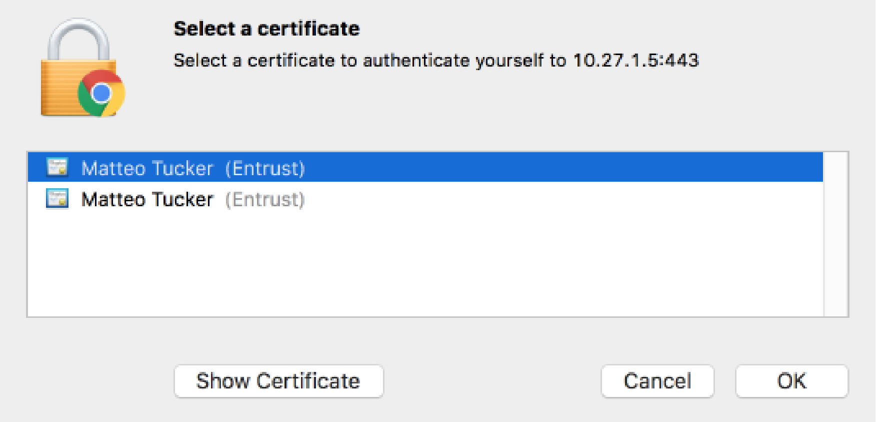
Show: <All>

Field	Value
Subject	Matteo Tucker, IDG SEDEMO1...
Public key	RSA (2048 Bits)
Certificate Policies	[1]Certificate Policy:Policy Ide...
2.16.840.1.101.3.6.9.1	01 01 00
Enhanced Key Usage	Smart Card Logon (1.3.6.1.4....
Subject Alternative Name	Other Name:Principal Name=m...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Private Key Usage Period	30 22 80 0f 32 30 31 37 30 34...

```
[1]Certificate Policy:
   Policy Identifier=2.16.840.1.101.3.2.1.3.13
```

b. Select your PIV Authentication certificate in the list of available certificates.

c. Click **OK**.



Select a certificate

Select a certificate to authenticate yourself to 10.27.1.5:443

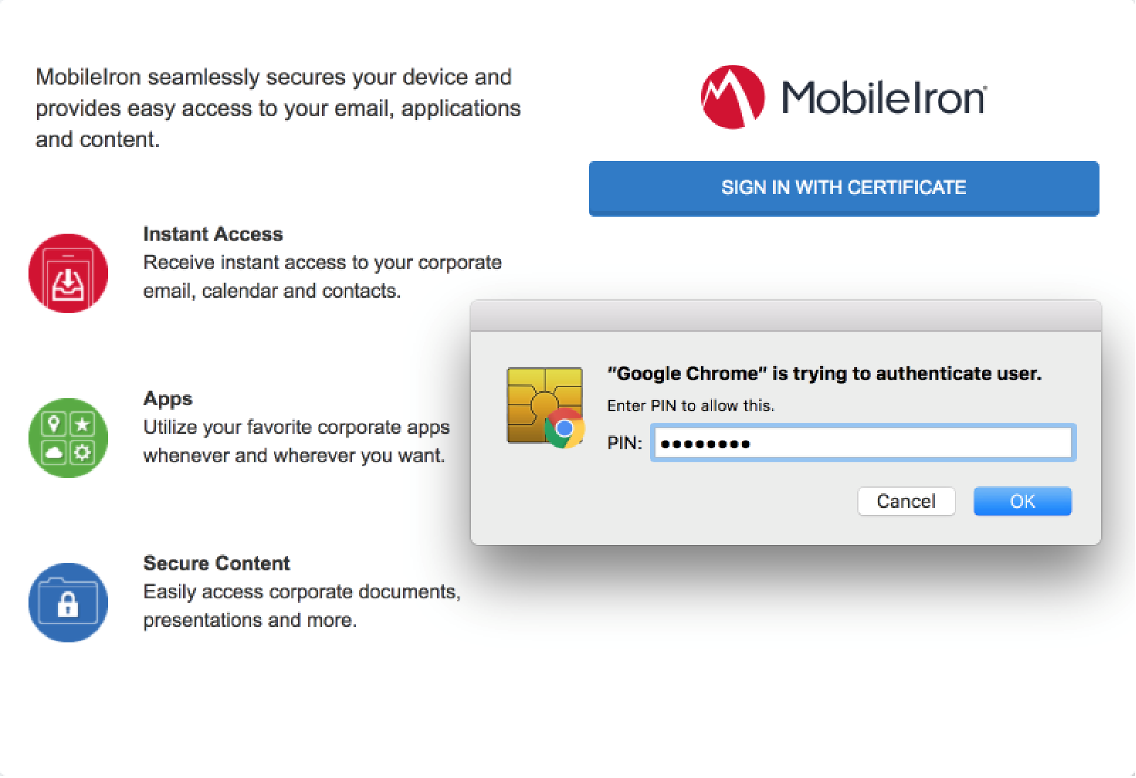
Matteo Tucker (Entrust)

Matteo Tucker (Entrust)

5. In the authentication dialogue:

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

b. Click **OK**.



MobileIron seamlessly secures your device and provides easy access to your email, applications and content.

Instant Access
Receive instant access to your corporate email, calendar and contacts.

Apps
Utilize your favorite corporate apps whenever and wherever you want.

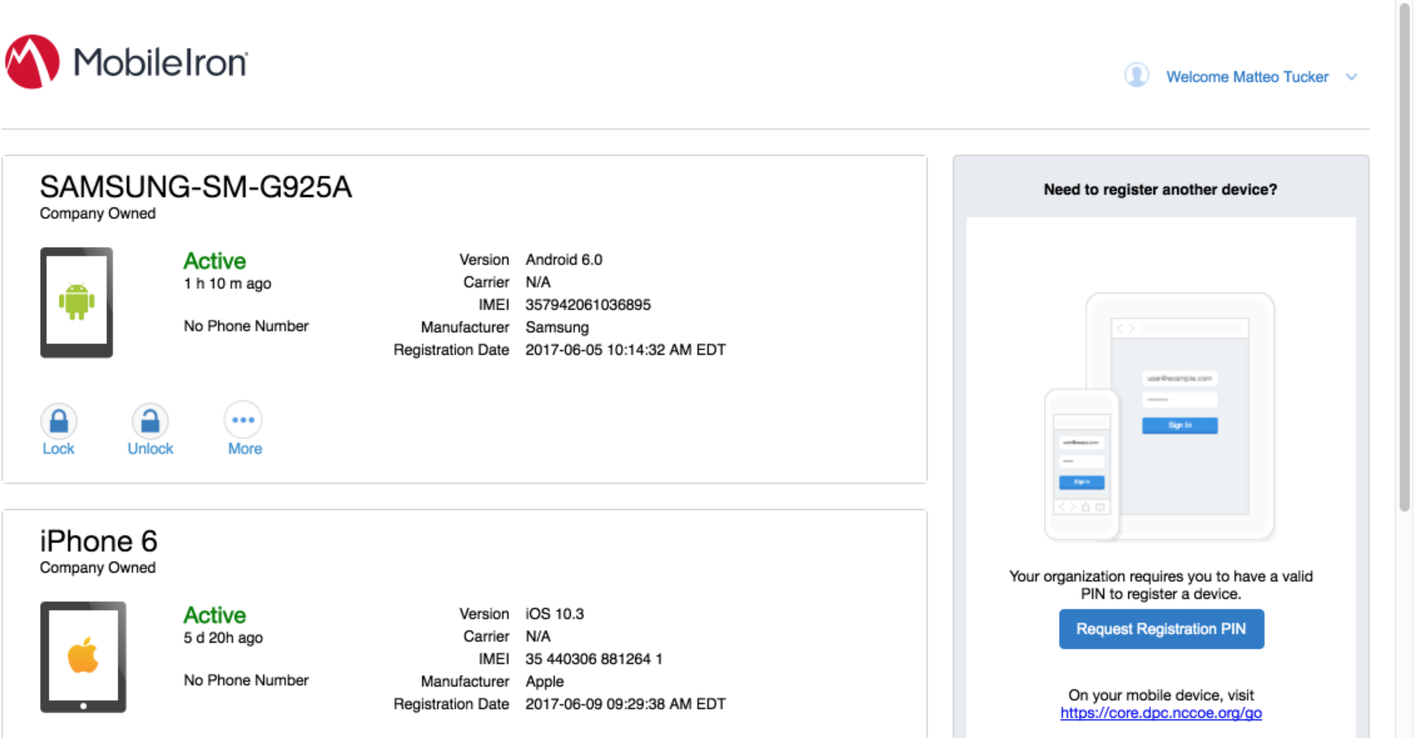
Secure Content
Easily access corporate documents, presentations and more.

"Google Chrome" is trying to authenticate user.

Enter PIN to allow this.

PIN: •••••••••

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



MobileIron

Welcome Matteo Tucker

SAMSUNG-SM-G925A
Company Owned

Active
1 h 10 m ago

No Phone Number

Version	Android 6.0
Carrier	N/A
IMEI	357942061036895
Manufacturer	Samsung
Registration Date	2017-06-05 10:14:32 AM EDT

iPhone 6
Company Owned

Active
5 d 20h ago

No Phone Number

Version	iOS 10.3
Carrier	N/A
IMEI	35 440306 881264 1
Manufacturer	Apple
Registration Date	2017-06-09 09:29:38 AM EDT

Need to register another device?

Your organization requires you to have a valid PIN to register a device.

On your mobile device, visit https://core.dpc.nccoe.org/go

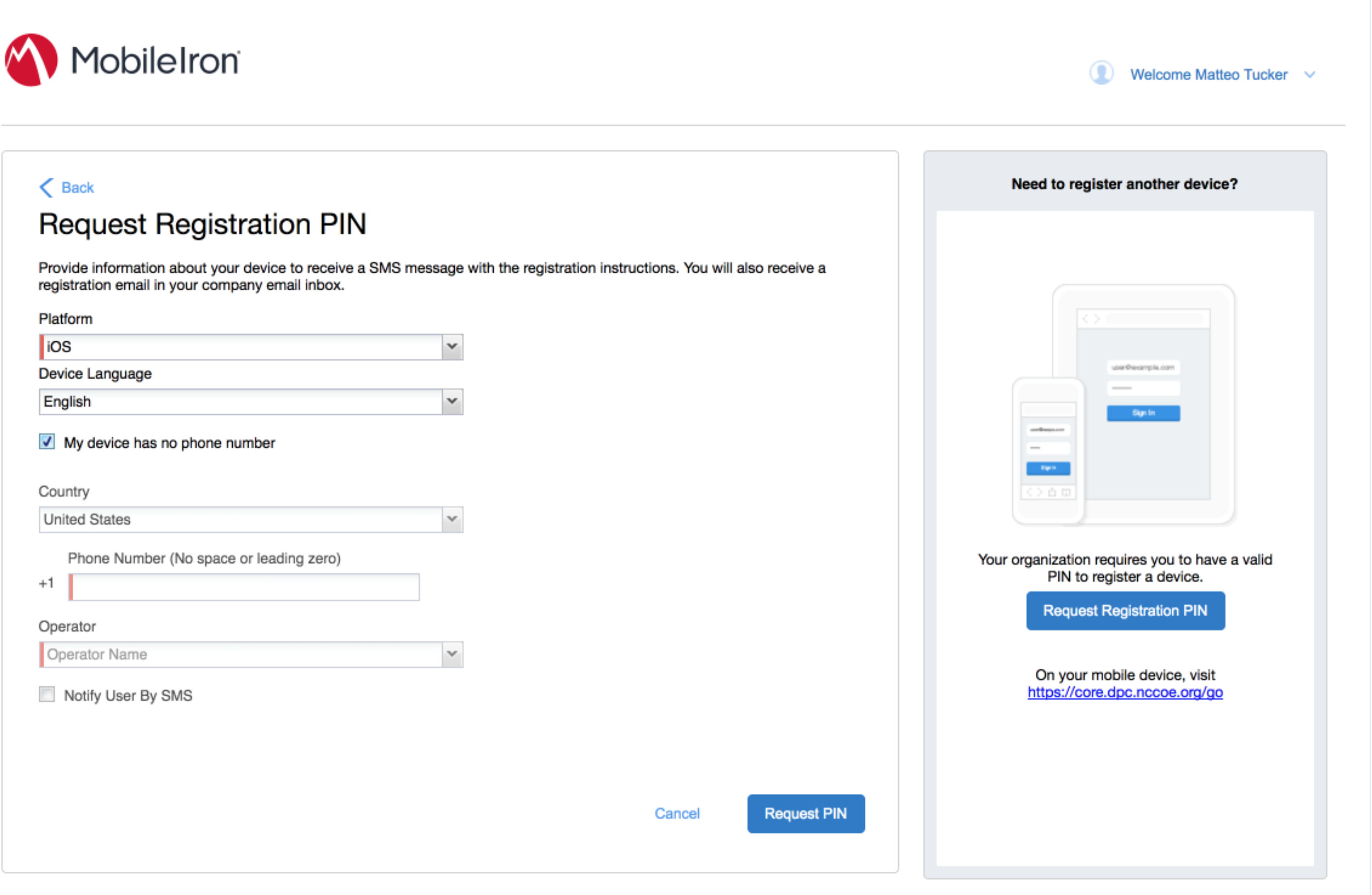
7. In the **Request Registration PIN** page:

   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.

304 d. Click **Request PIN**.



Request Registration PIN

Provide information about your device to receive a SMS message with the registration instructions. You will also receive a registration email in your company email inbox.

Platform: iOS

Device Language: English

☑ My device has no phone number

Country: United States

Phone Number (No space or leading zero): +1

Operator: Operator Name

□ Notify User By SMS

Need to register another device?

Your organization requires you to have a valid PIN to register a device.

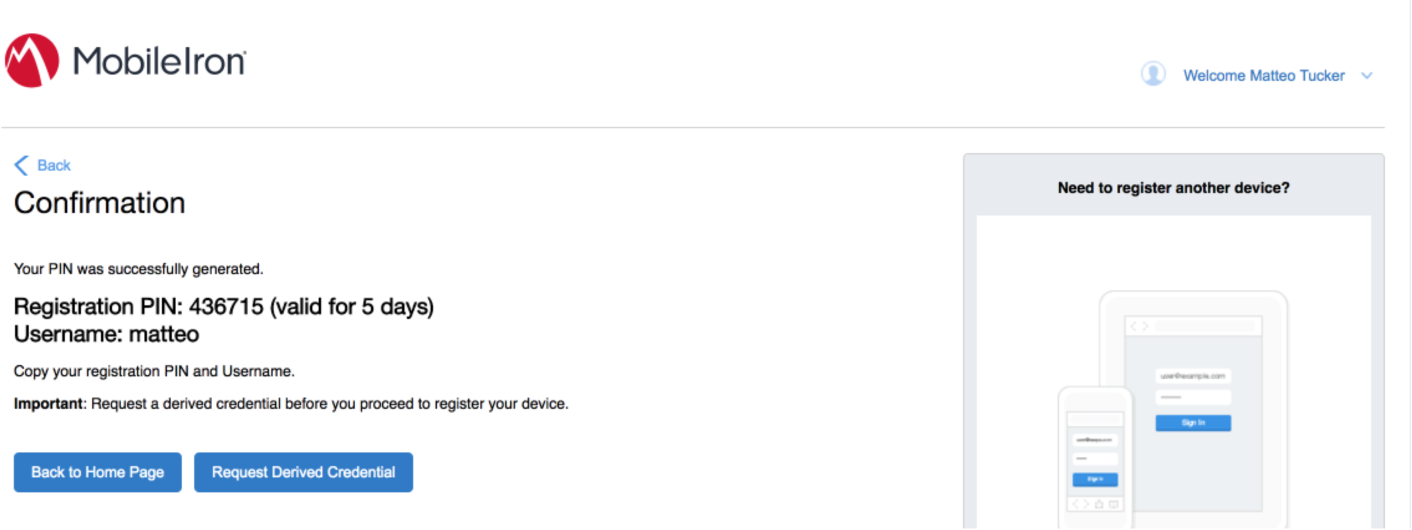
On your mobile device, visit https://core.dpc.nccoe.org/go

305

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



Confirmation

Your PIN was successfully generated.

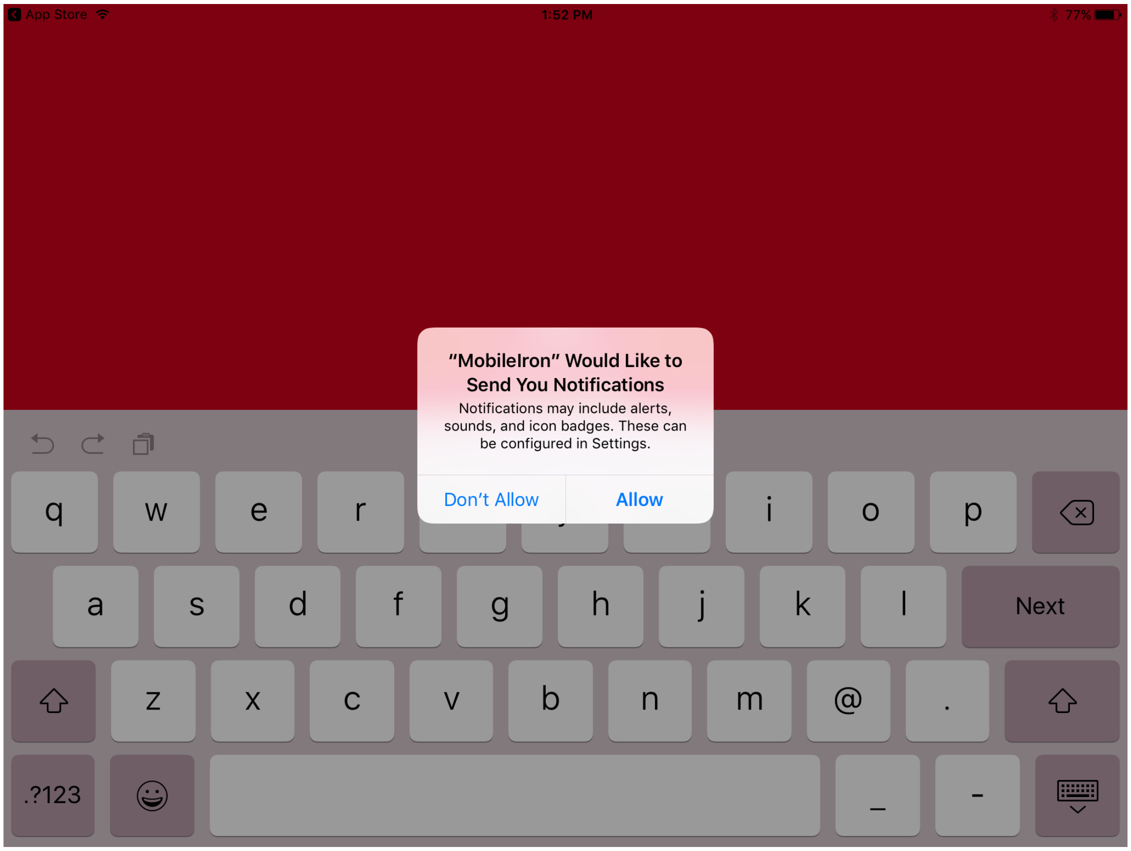
Registration PIN: 436715 (valid for 5 days)
Username: matteo

Copy your registration PIN and Username.

Important: Request a derived credential before you proceed to register your device.

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**.



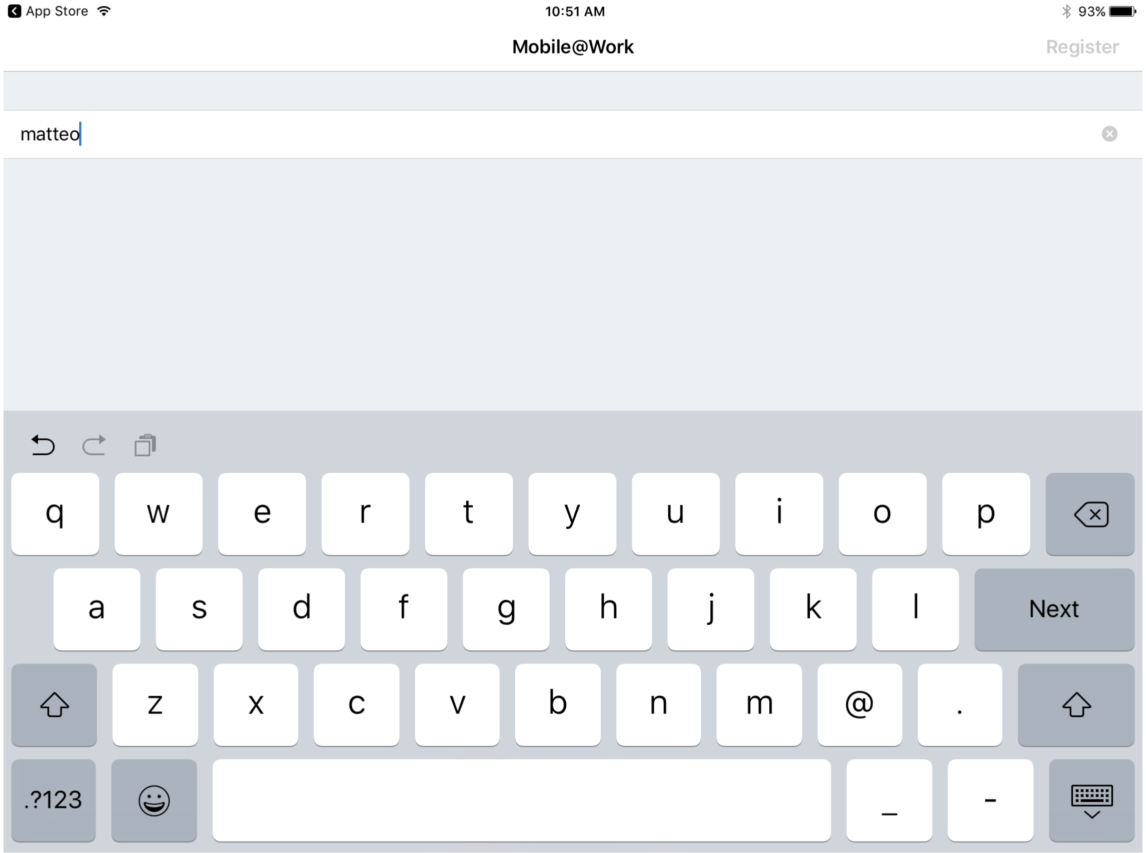
"MobileIron" Would Like to Send You Notifications

Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

10. In **Mobile@Work**:

    a. In the **User Name** field, enter your LDAP or MobileIron user ID.

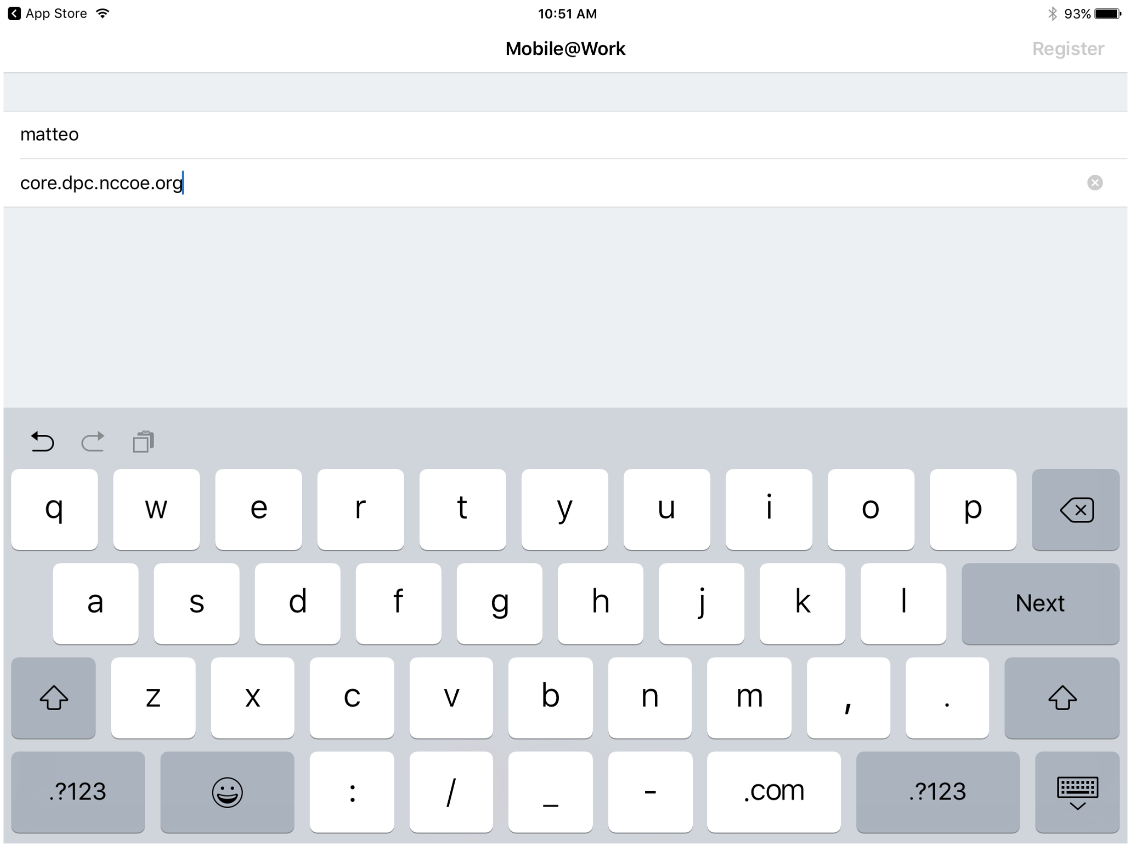
    b. Tap **Next**.



317

318 c. In the **Server** field, enter the URL for your organization's instance of MobileIron Core as provided by a MobileIron Core administrator.

320 d. Tap **Next**.

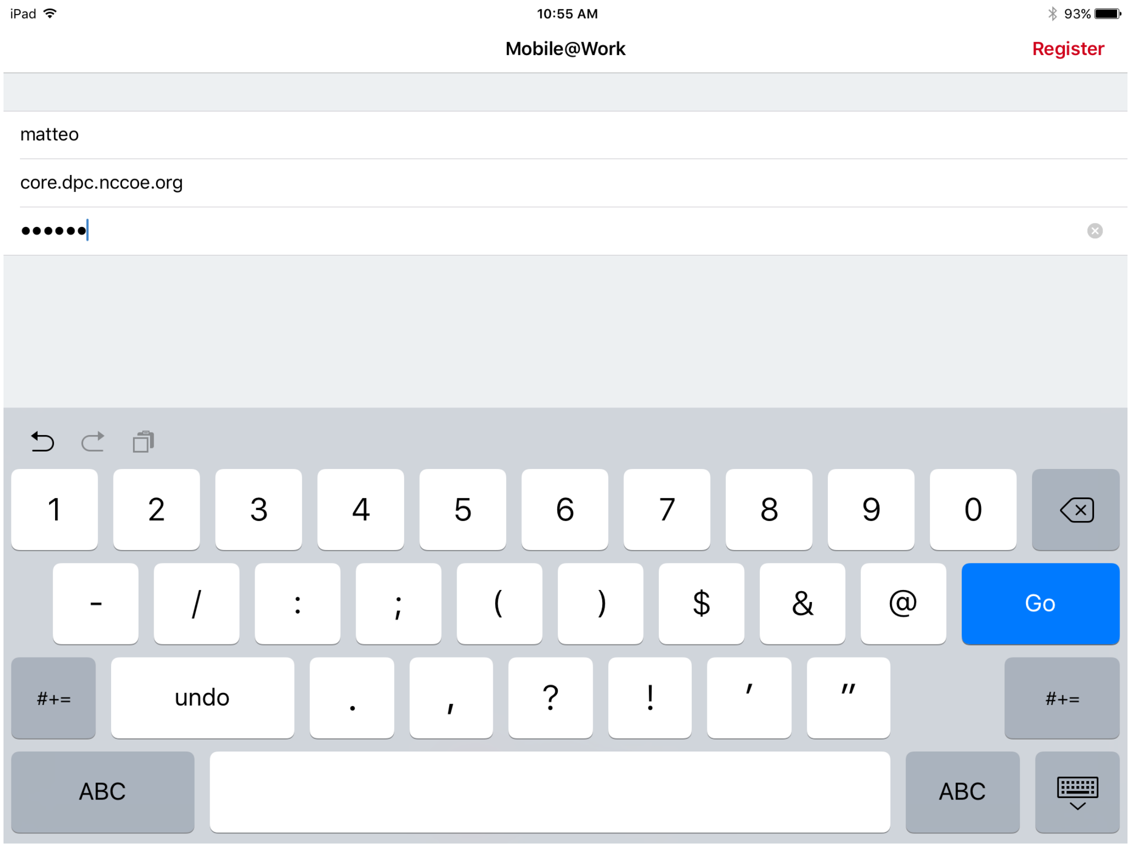


matteo

core.dpc.nccoe.org

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.

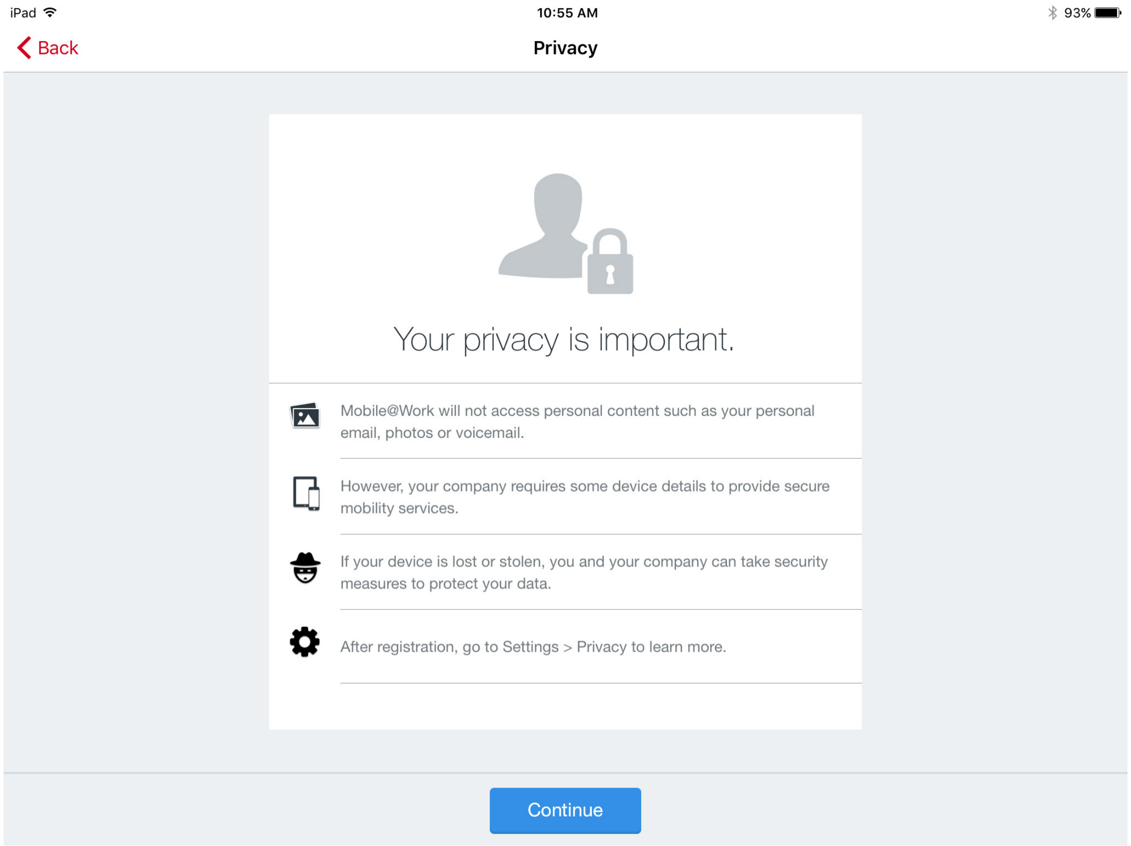


matteo

core.dpc.nccoe.org

••••••

g. In the Privacy screen, tap **Continue**.



Your privacy is important.

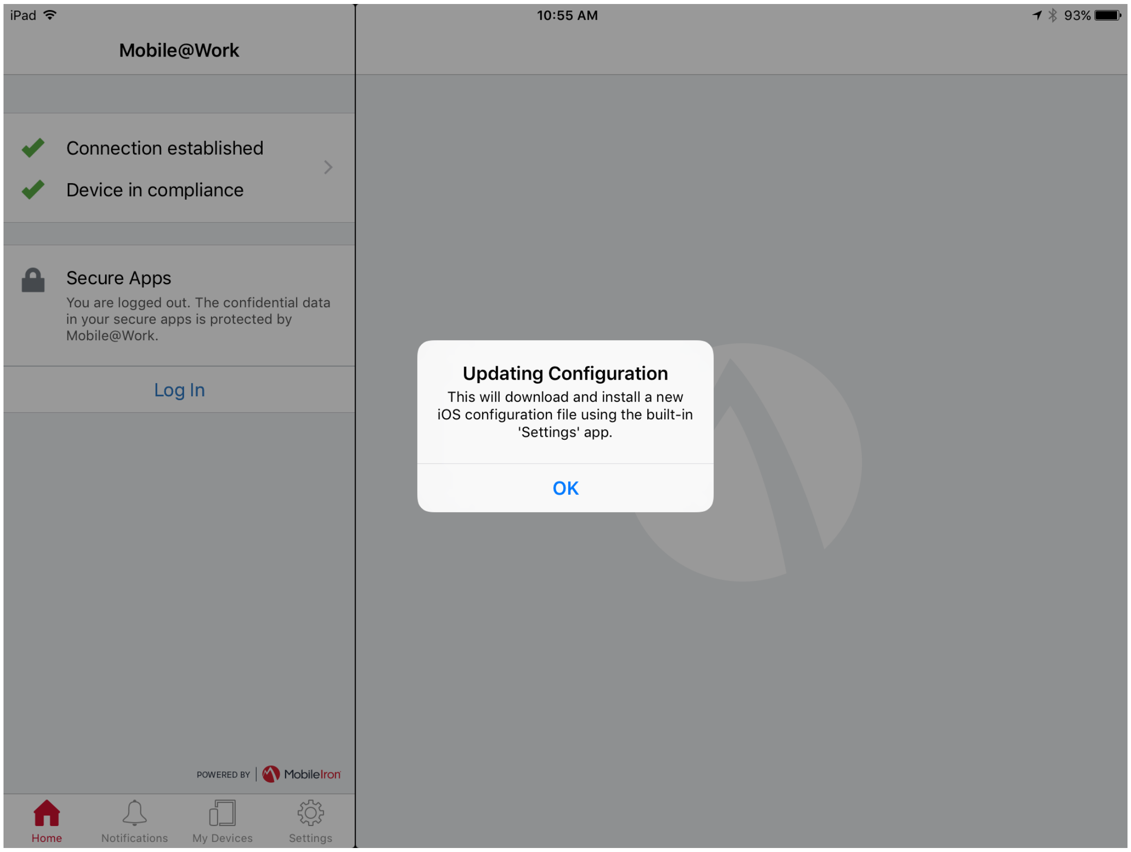
Mobile@Work will not access personal content such as your personal email, photos or voicemail.

However, your company requires some device details to provide secure mobility services.

If your device is lost or stolen, you and your company can take security measures to protect your data.

After registration, go to Settings > Privacy to learn more.

11. In the **Updating Configuration** dialogue, tap **OK**; this will launch the built-in iOS **Settings** application.



Connection established

Device in compliance

Secure Apps

You are logged out. The confidential data in your secure apps is protected by Mobile@Work.

Updating Configuration

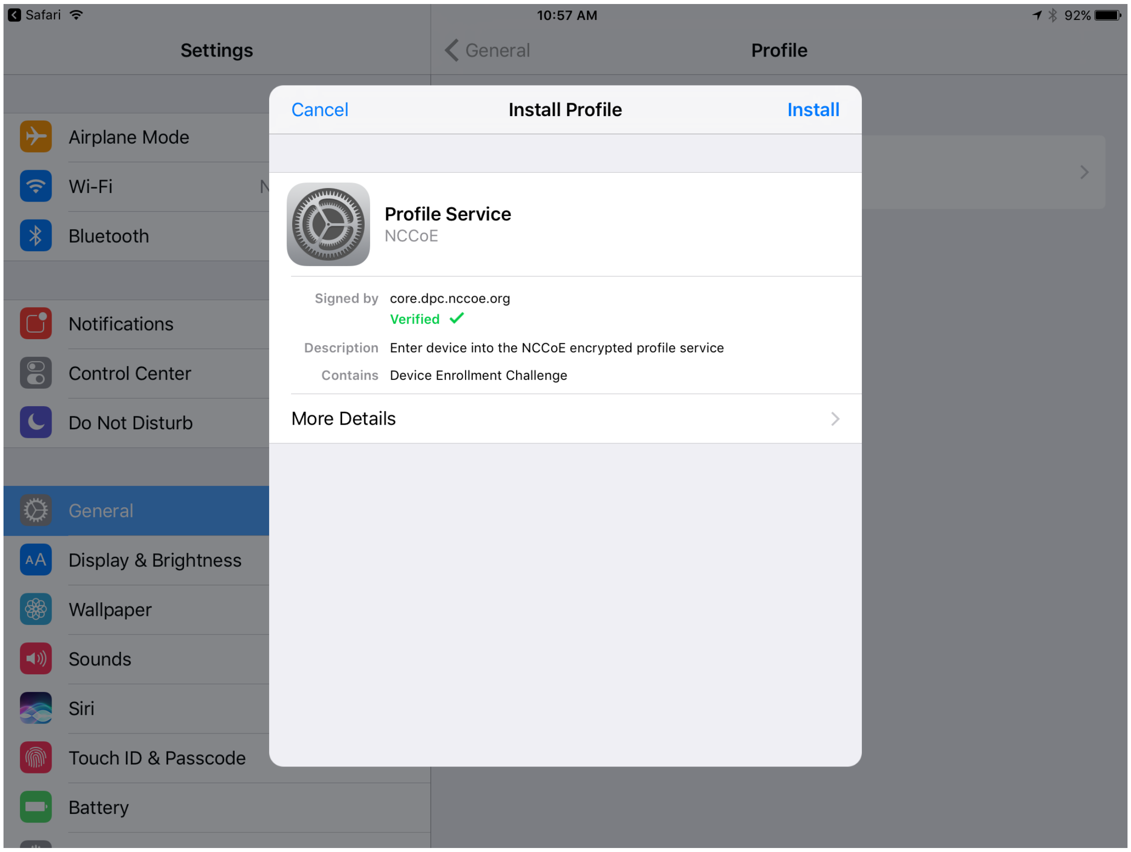
This will download and install a new iOS configuration file using the built-in 'Settings' app.

12. In the **Settings** application, in the **Install Profile** dialogue:

    a. In the **Signed B**y 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**.



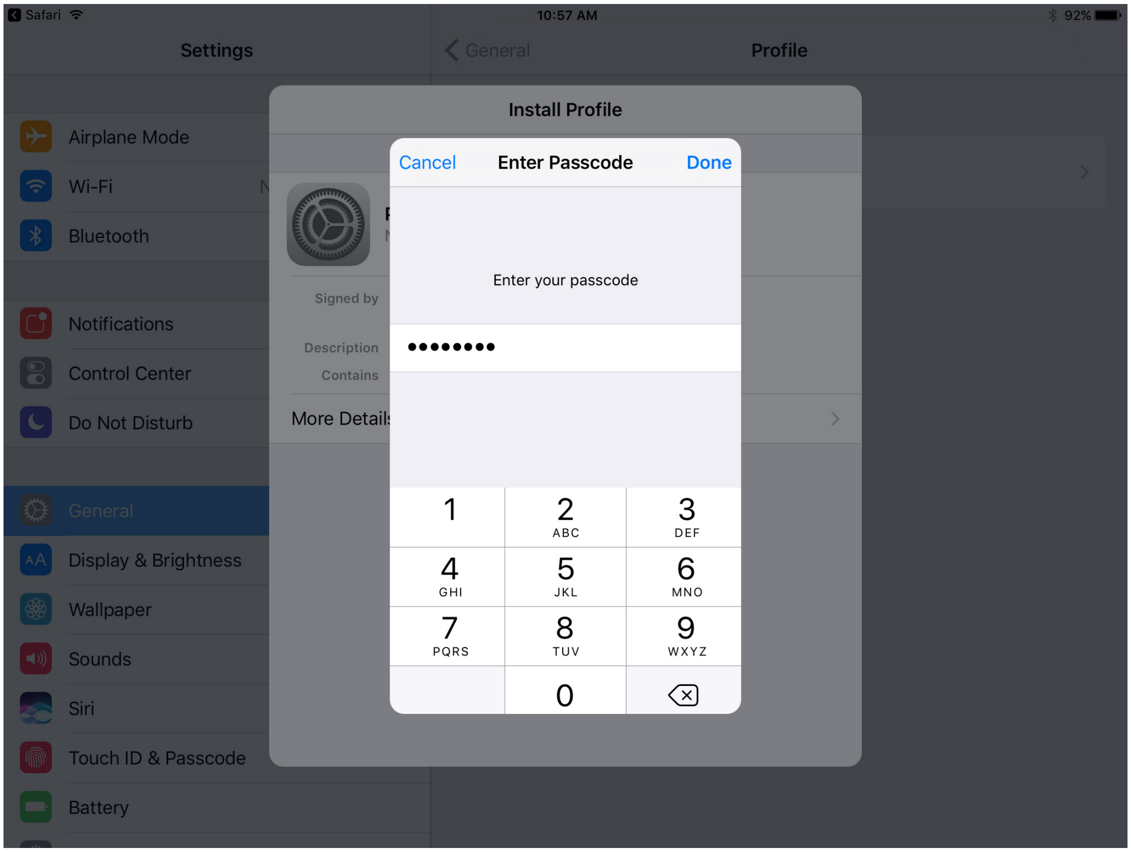
Profile Service
NCCoE

Signed by core.dpc.nccoe.org
Verified ✓

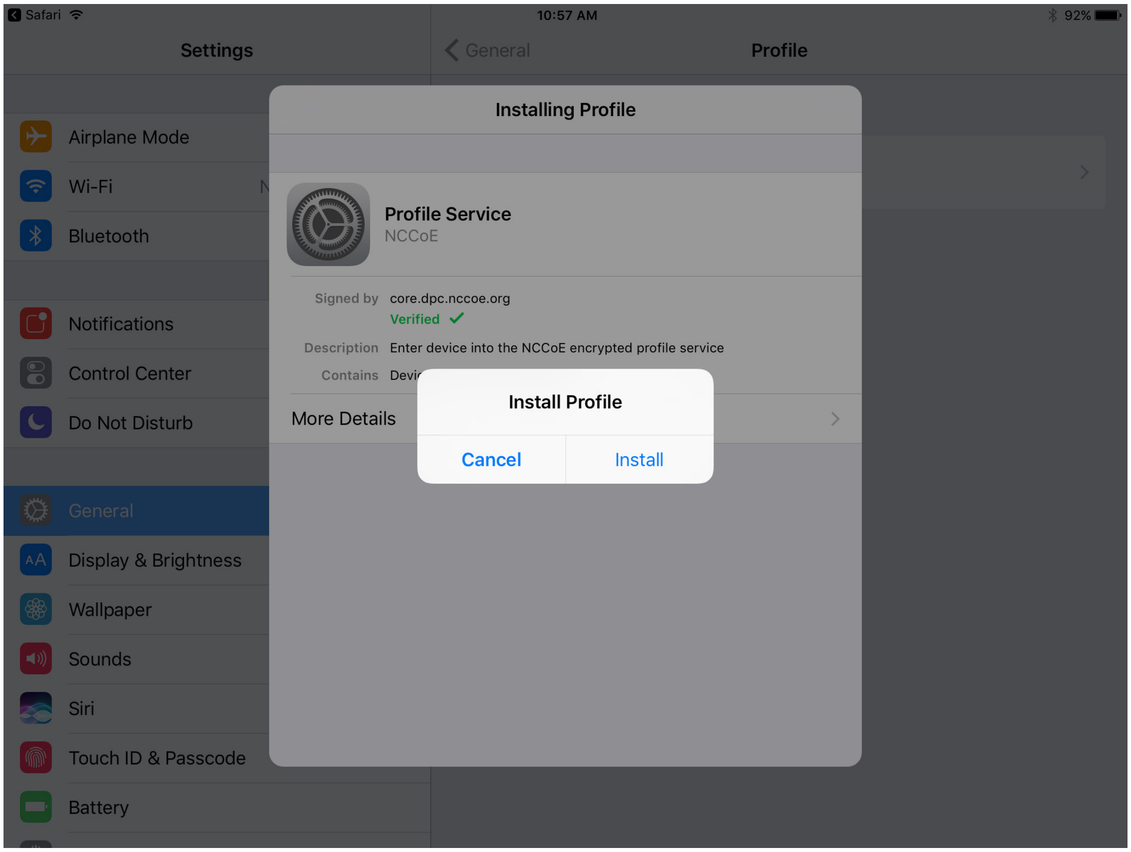
Description Enter device into the NCCoE encrypted profile service

Contains Device Enrollment Challenge

13. In the Enter **Passcode** dialogue:
    a. Enter your device unlock code.
    b. Tap **Done**.

340 

341 14. In the **Install Profile** dialogue, tap **Install**.



Profile Service
NCCoE

Signed by core.dpc.nccoe.org
Verified ✓

Description Enter device into the NCCoE encrypted profile service

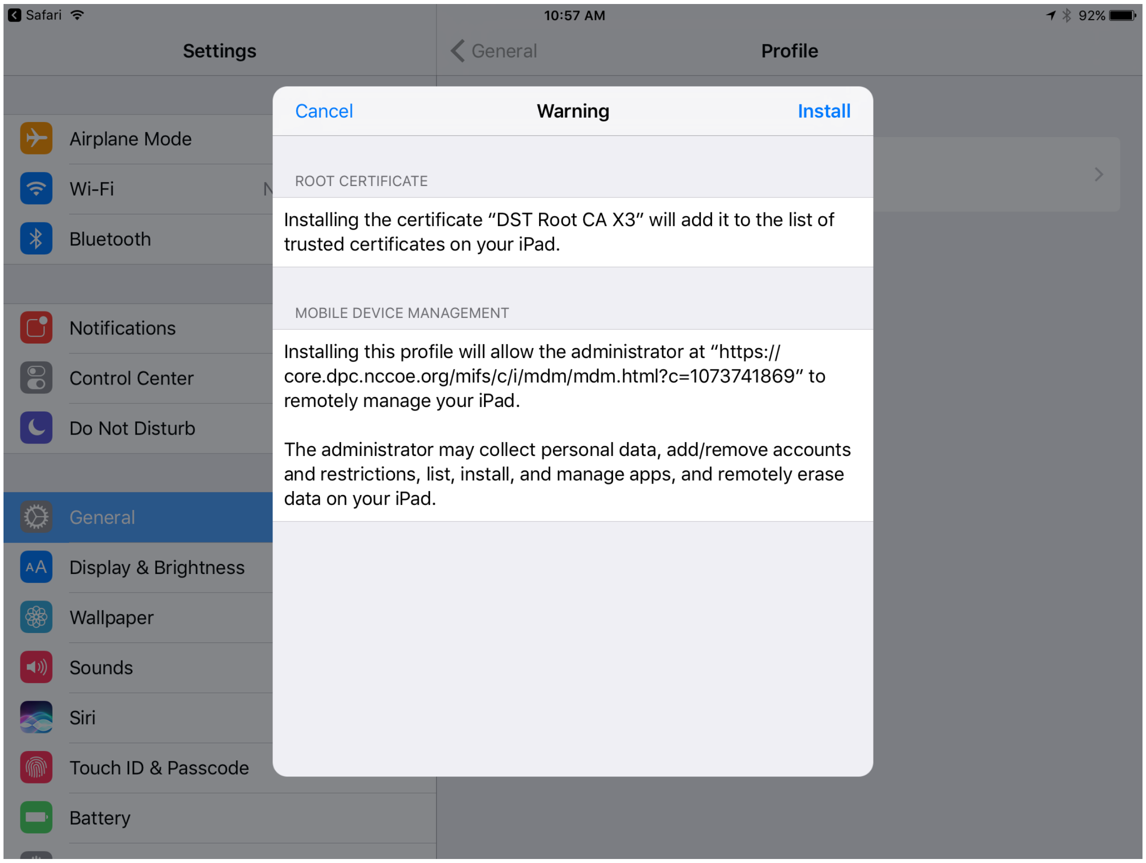
Contains Devi

More Details

Install Profile

Cancel Install

15. In the **Warning** dialogue, tap **Install**.



ROOT CERTIFICATE

Installing the certificate “DST Root CA X3” will add it to the list of trusted certificates on your iPad.

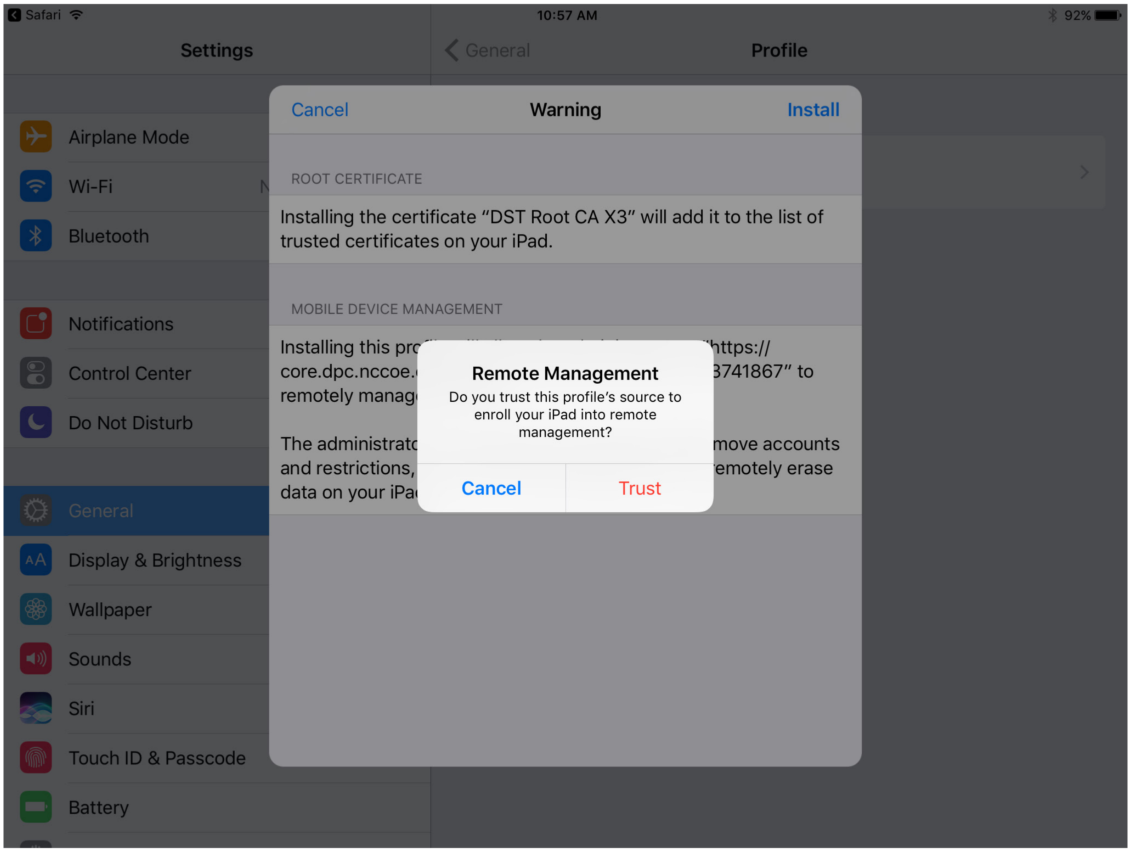
MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at “https://core.dpc.nccoe.org/mifs/c/i/mdm/mdm.html?c=1073741869” to remotely manage your iPad.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPad.

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 certificate authority.



Installing the certificate "DST Root CA X3" will add it to the list of trusted certificates on your iPad.

Installing this pro "https:// core.dpc.nccoe. 3741867" to remotely manag

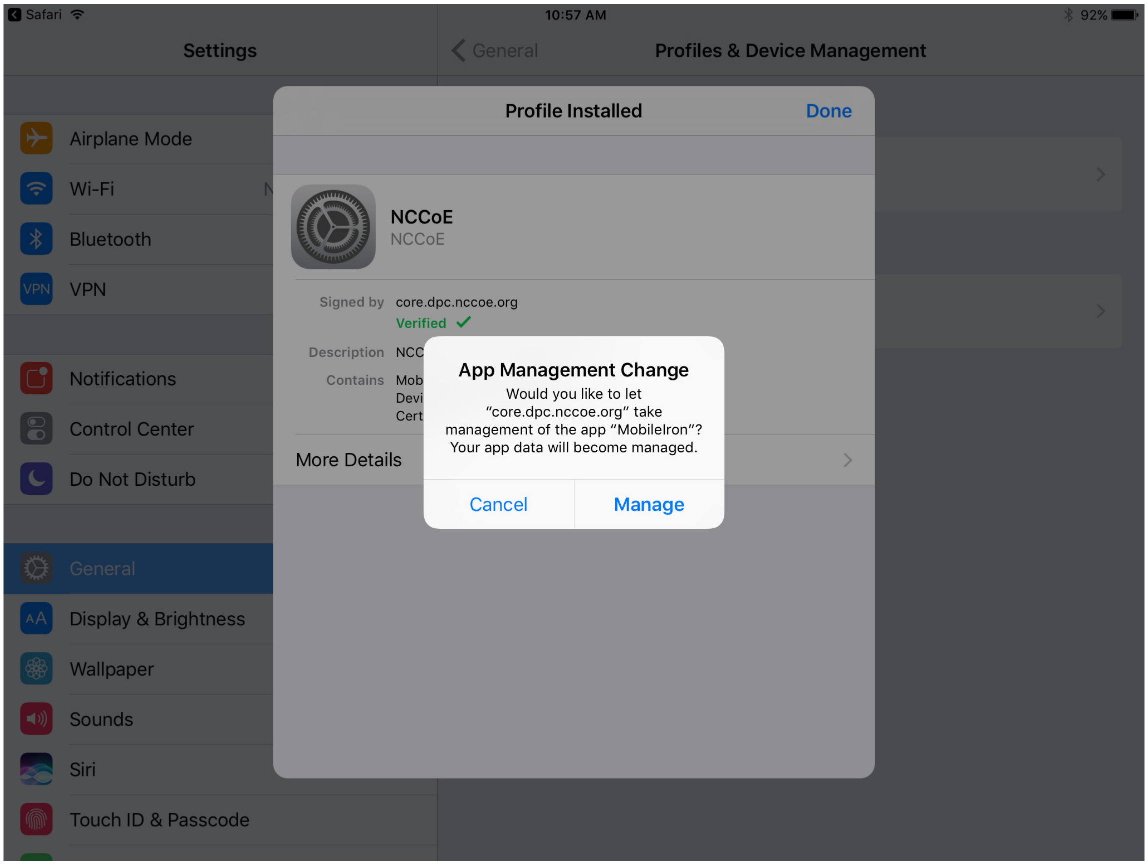
The administrat move accounts and restrictions, emotely erase data on your iPa

Remote Management

Do you trust this profile's source to enroll your iPad into remote management?

17. In the **Profile Installed** dialogue, tap **Done**.

18. In the **App Management Change** dialogue, tap **Manage**.



NCCoE
NCCoE

Signed by core.dpc.nccoe.org
Verified ✓

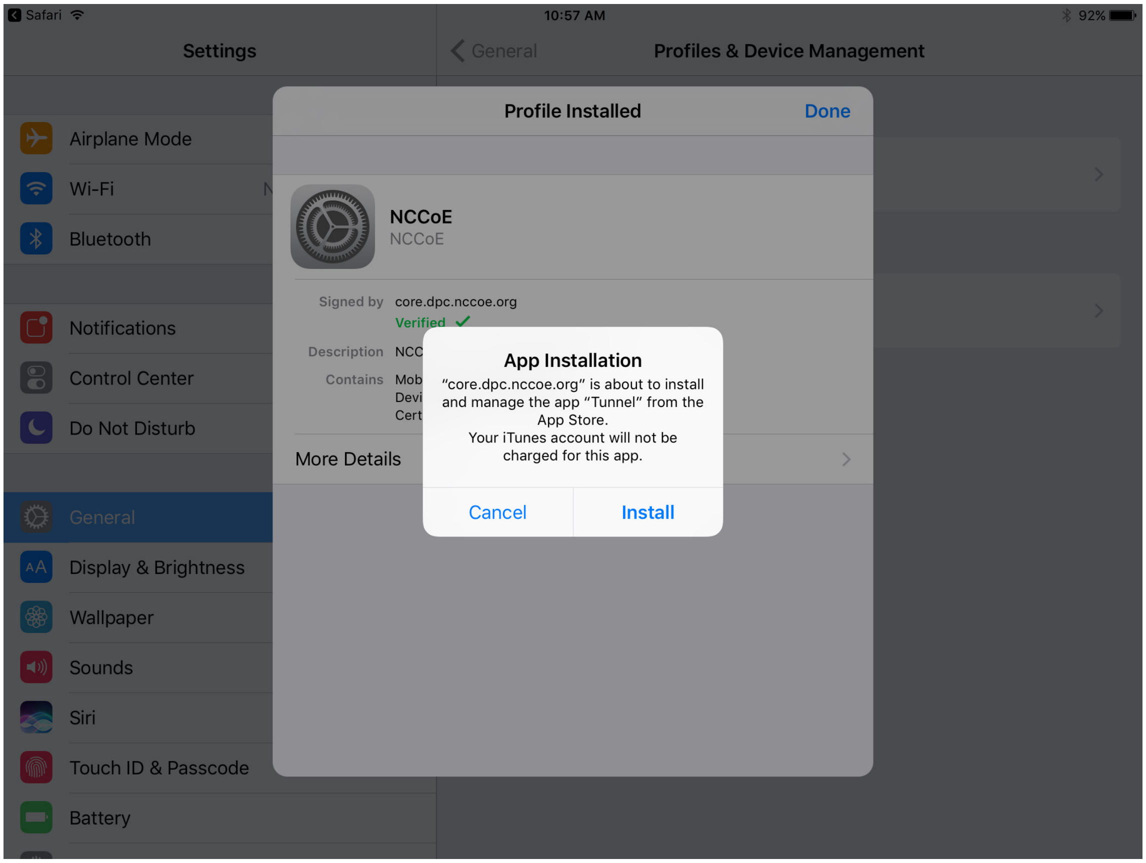
Description NCC

Contains Mob
Devi
Cert

App Management Change

Would you like to let "core.dpc.nccoe.org" take management of the app "MobileIron"? Your app data will become managed.

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**.



Profile Installed Done

NCCoE
NCCoE

Signed by core.dpc.nccoe.org
Verified ✓

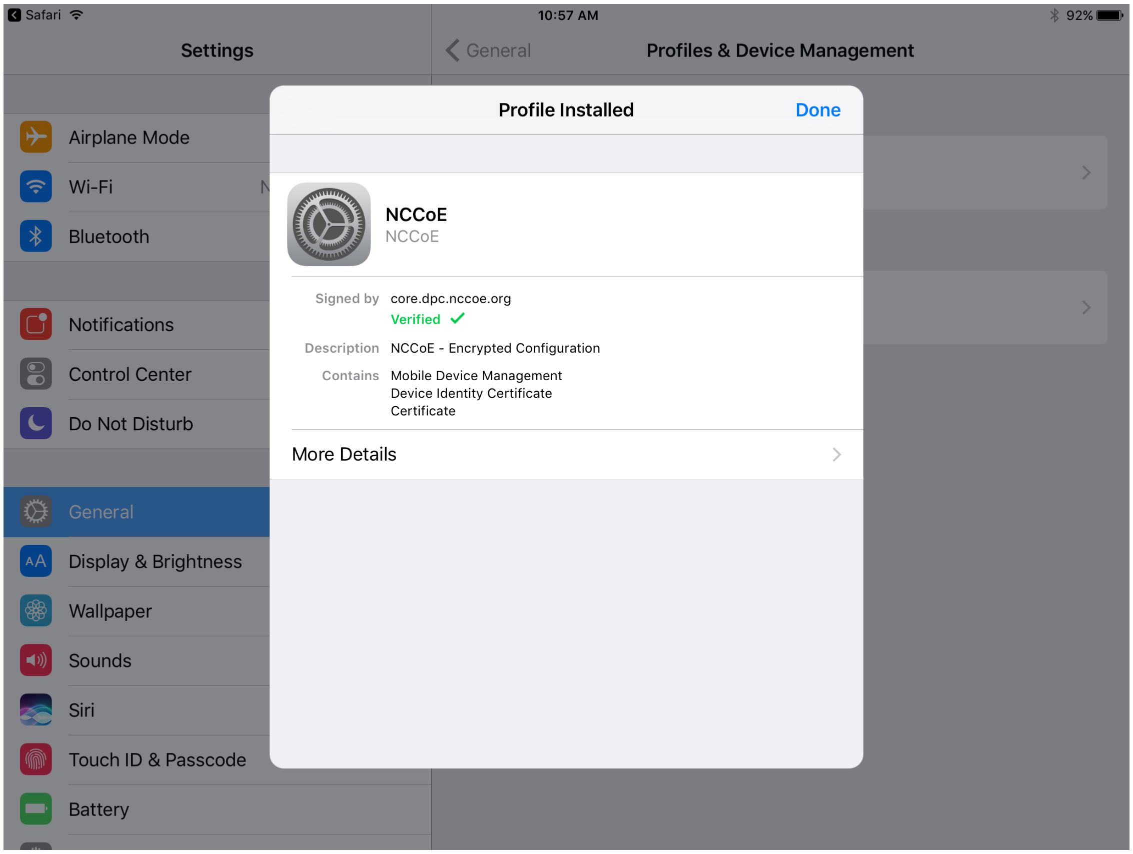
Description NCC

Contains Mob
Devi
Cert

App Installation

“core.dpc.nccoe.org” is about to install and manage the app “Tunnel” from the App Store.
Your iTunes account will not be charged for this app.

20. In the **Profile Installed** dialogue, tap **Done**.



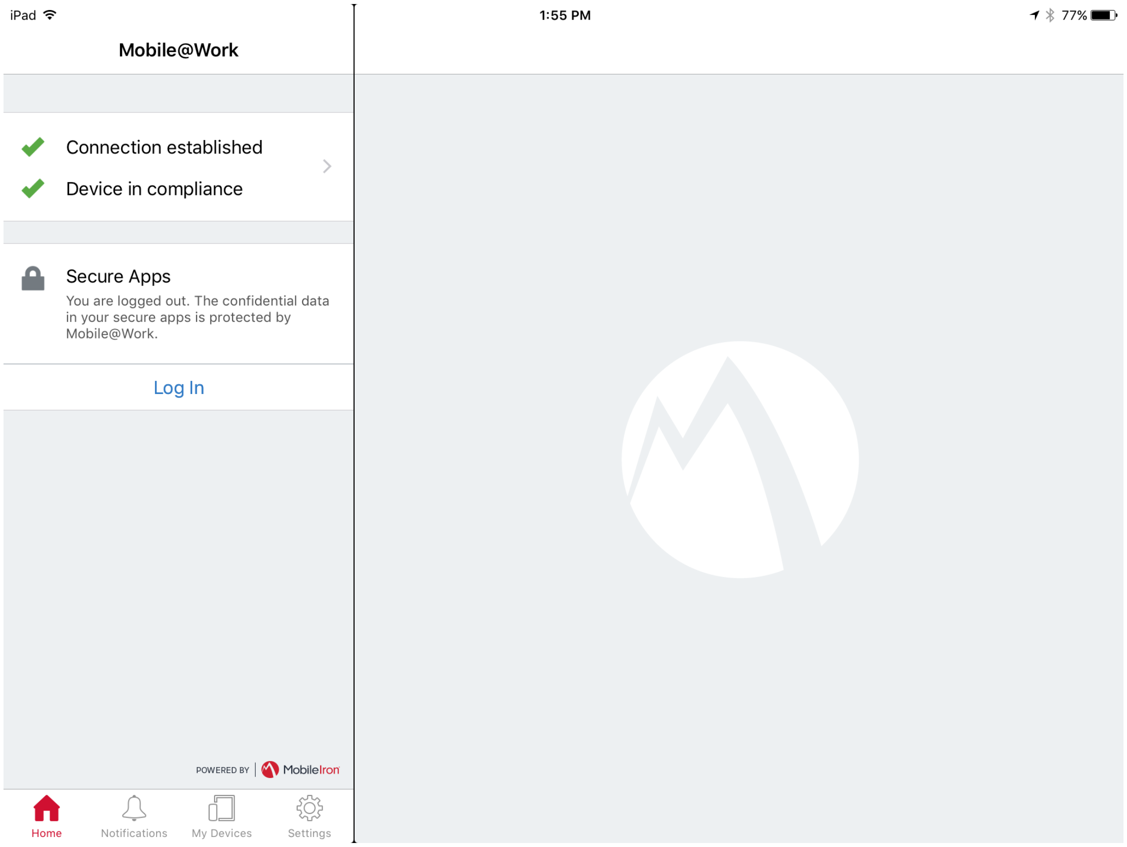
NCCoE
NCCoE

Signed by core.dpc.nccoe.org
Verified ✓

Description NCCoE - Encrypted Configuration

Contains Mobile Device Management
Device Identity Certificate
Certificate

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).



2.1.3.1.2 DPC Initial Issuance

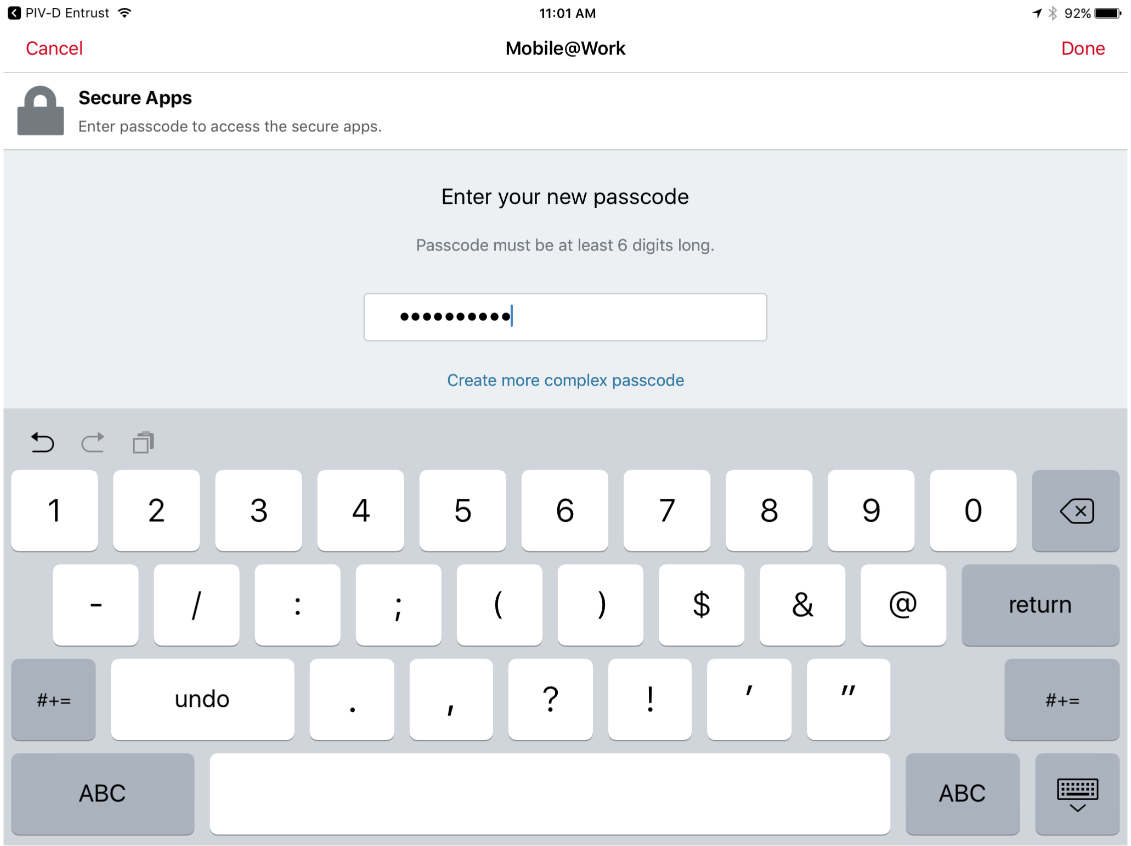
The following steps demonstrate how a DPC is issued to an applicant's mobile device. It assumes the target mobile device is registered with MobileIron (see Register Target Device with MobileIron) and the MobileIron PIV-D Entrust application is installed (see Implement MobileIron Guidance). These steps 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.


PIV-D Entrust 11:01 AM 92%

Cancel Mobile@Work Done

Secure Apps

Enter passcode to access the secure apps.

Enter your new passcode

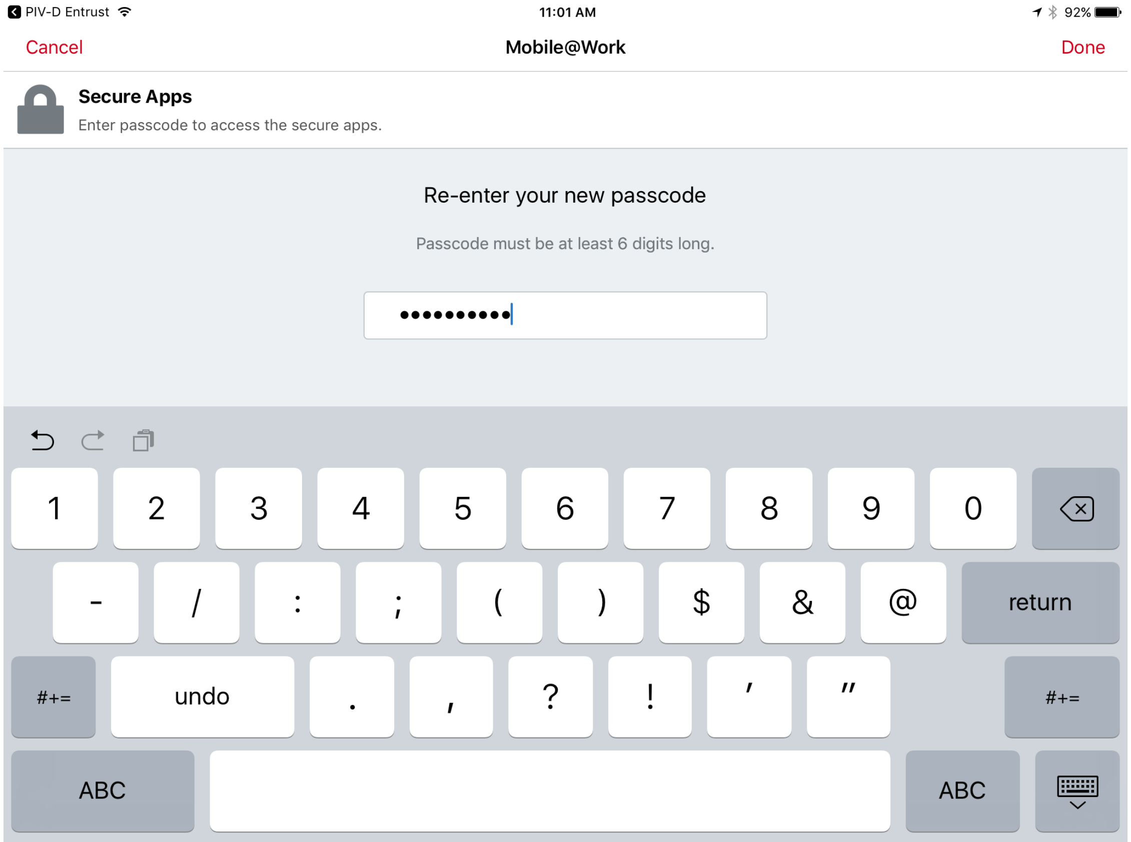
Passcode must be at least 6 digits long.

●●●●●●●●●●●

Create more complex passcode

b. In the **Re-enter your new passcode** field, re-enter the password you entered in Step 2b.

c. Tap **Done**.



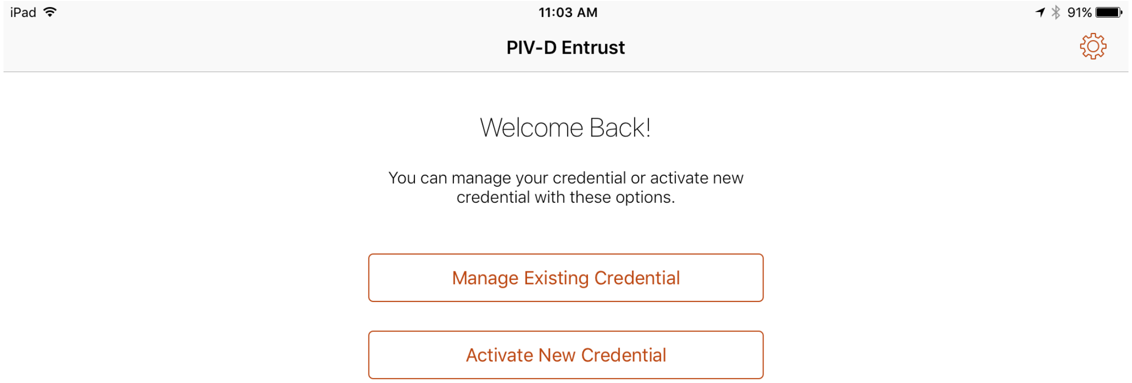
Secure Apps

Enter passcode to access the secure apps.

Re-enter your new passcode

Passcode must be at least 6 digits long.

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.



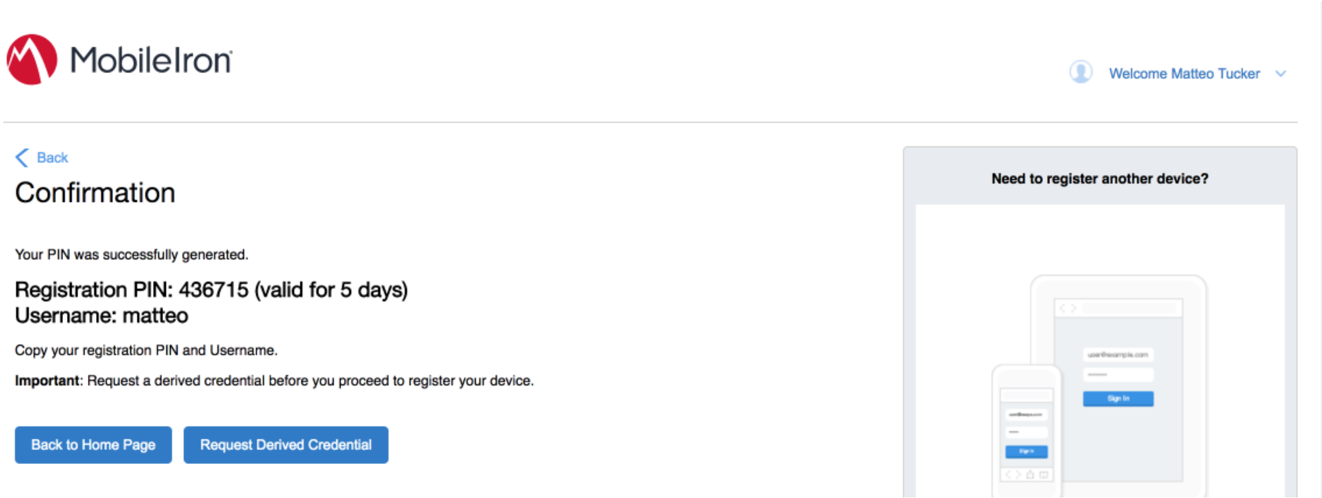
Welcome Back!

You can manage your credential or activate new credential with these options.

4. Insert your valid PIV Card into the reader attached to your laptop or computer workstation.

5. 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**.



Confirmation

Your PIN was successfully generated.

Registration PIN: 436715 (valid for 5 days)
Username: matteo

Copy your registration PIN and Username.

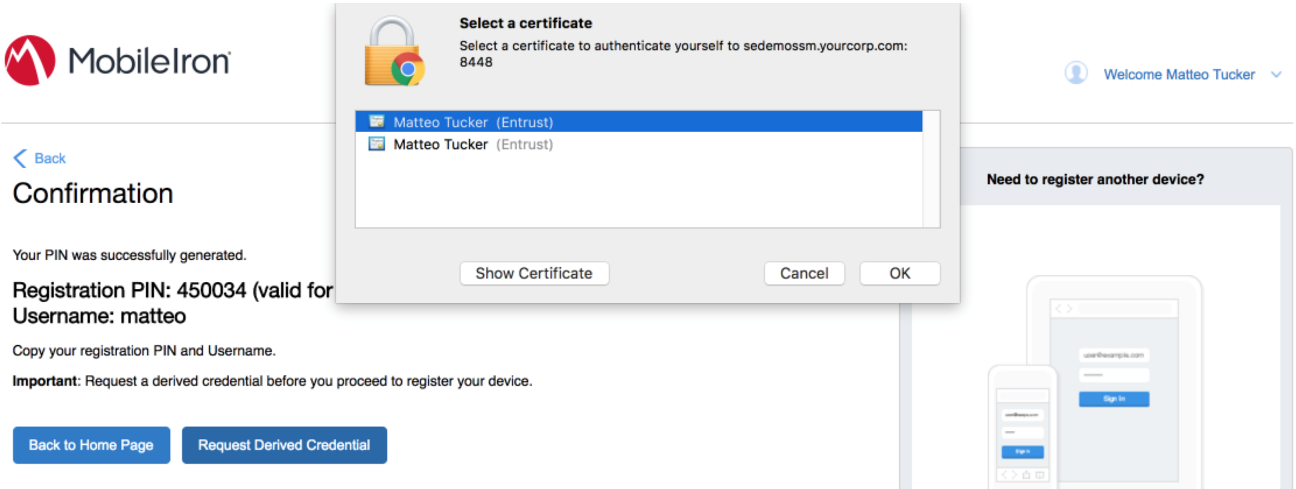
Important: Request a derived credential before you proceed to register your device.

   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.



Select a certificate

Select a certificate to authenticate yourself to sedemossm.yourcorp.com: 8448

Matteo Tucker (Entrust)

Matteo Tucker (Entrust)

Confirmation

Your PIN was successfully generated.

Registration PIN: 450034 (valid for

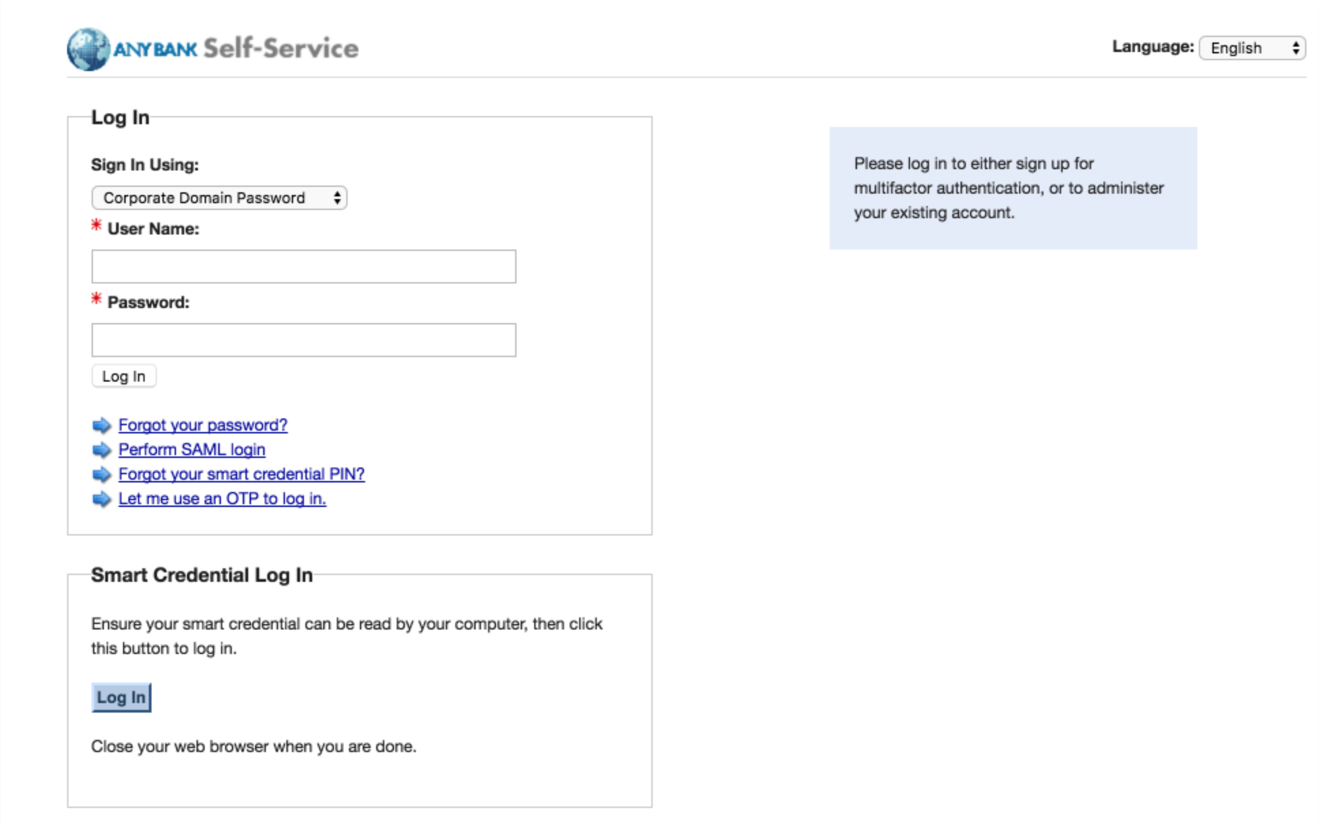
Username: matteo

Copy your registration PIN and Username.

Important: Request a derived credential before you proceed to register your device.

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.



ANYBANK Self-Service

Language: English

Log In

Sign In Using:

Corporate Domain Password

* User Name:

* Password:

Log In

- Forgot your password?
- Perform SAML login
- Forgot your smart credential PIN?
- Let me use an OTP to log in.

Please log in to either sign up for multifactor authentication, or to administer your existing account.

Smart Credential Log In

Ensure your smart credential can be read by your computer, then click this button to log in.

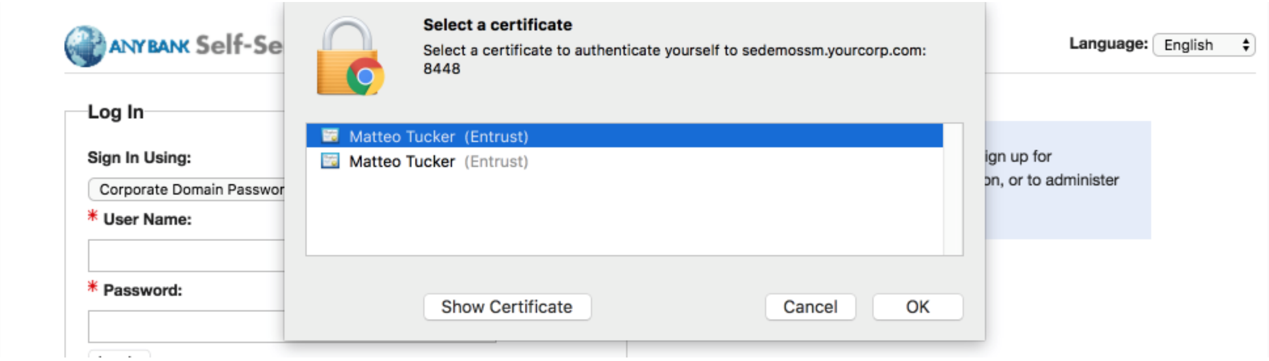
Log In

Close your web browser when you are done.

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**.



Select a certificate

Select a certificate to authenticate yourself to sedemossm.yourcorp.com: 8448

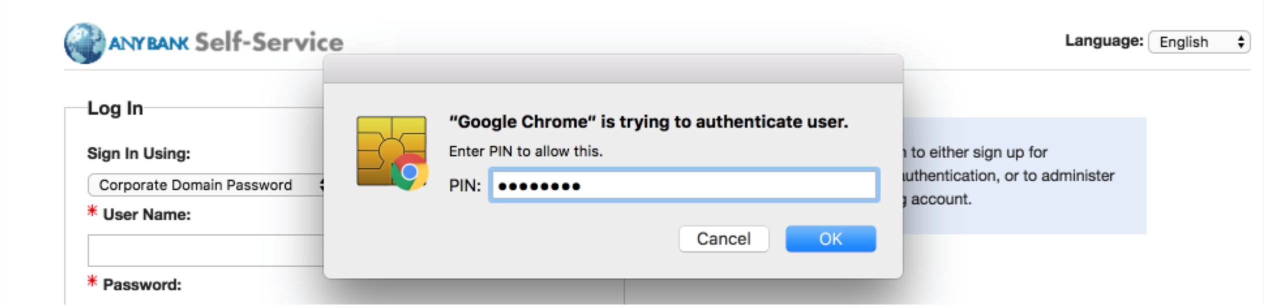
Matteo Tucker (Entrust)

Matteo Tucker (Entrust)

d. In the authentication dialogue:

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

   ii. Click **OK**.

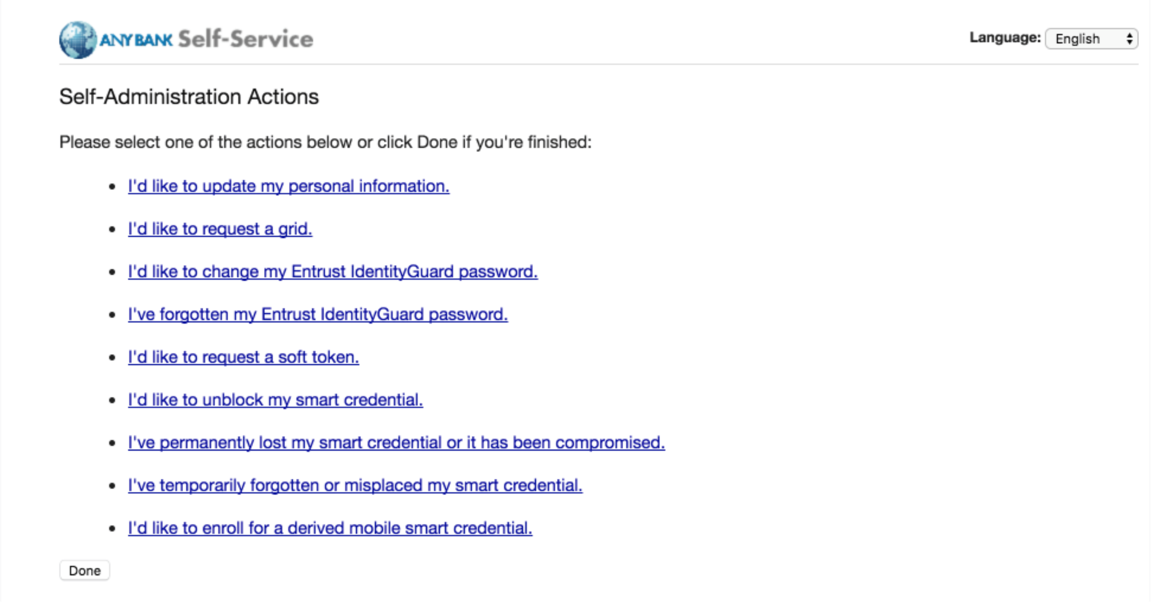


"Google Chrome" is trying to authenticate user.

Enter PIN to allow this.

PIN: •••••••••

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).



ANYBANK Self-Service

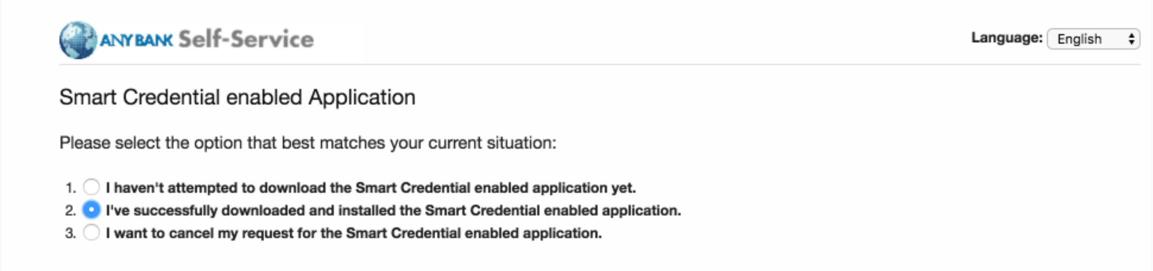
Language: English

Self-Administration Actions

Please select one of the actions below or click Done if you're finished:

- 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.

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



ANYBANK Self-Service

Language: English

Smart Credential enabled Application

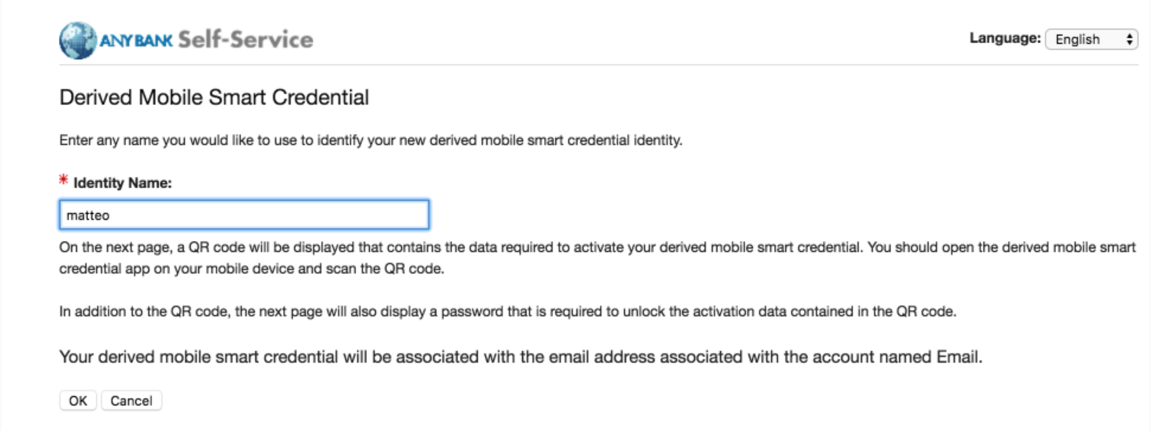
Please select the option that best matches your current situation:

1. ○ I haven't attempted to download the Smart Credential enabled application yet.
2. ● I've successfully downloaded and installed the Smart Credential enabled application.
3. ○ I want to cancel my request for 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**.



Derived Mobile Smart Credential

Enter any name you would like to use to identify your new derived mobile smart credential identity.

* Identity Name: matteo

On the next page, a QR code will be displayed that contains the data required to activate your derived mobile smart credential. You should open the derived mobile smart credential app on your mobile device and scan the QR code.

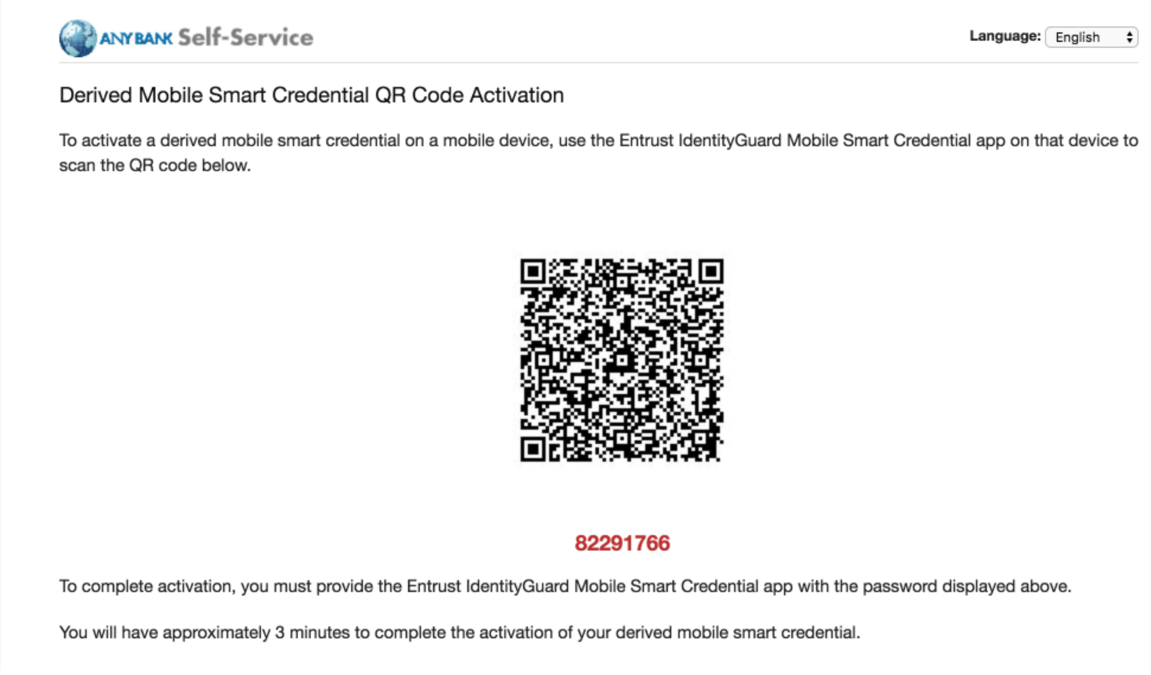
In addition to the QR code, the next page will also display a password that is required to unlock the activation data contained in the QR code.

Your derived mobile smart credential will be associated with the email address associated with the account named Email.

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.

Figure 2-3 Derived Mobile Smart Credential QR Code Activation Page



Derived Mobile Smart Credential QR Code Activation

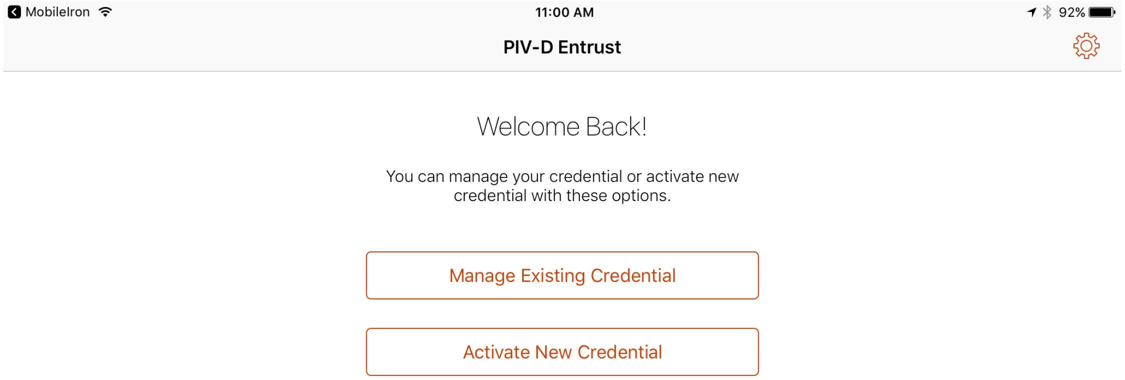
To activate a derived mobile smart credential on a mobile device, use the Entrust IdentityGuard Mobile Smart Credential app on that device to scan the QR code below.

82291766

To complete activation, you must provide the Entrust IdentityGuard Mobile Smart Credential app with the password displayed above.

You will have approximately 3 minutes to complete the activation of your derived mobile smart credential.

11. In the **PIV-D Entrust** application that is running on the target mobile device, tap **Activate New Credential**.



MobileIron 11:00 AM 92%

PIV-D Entrust

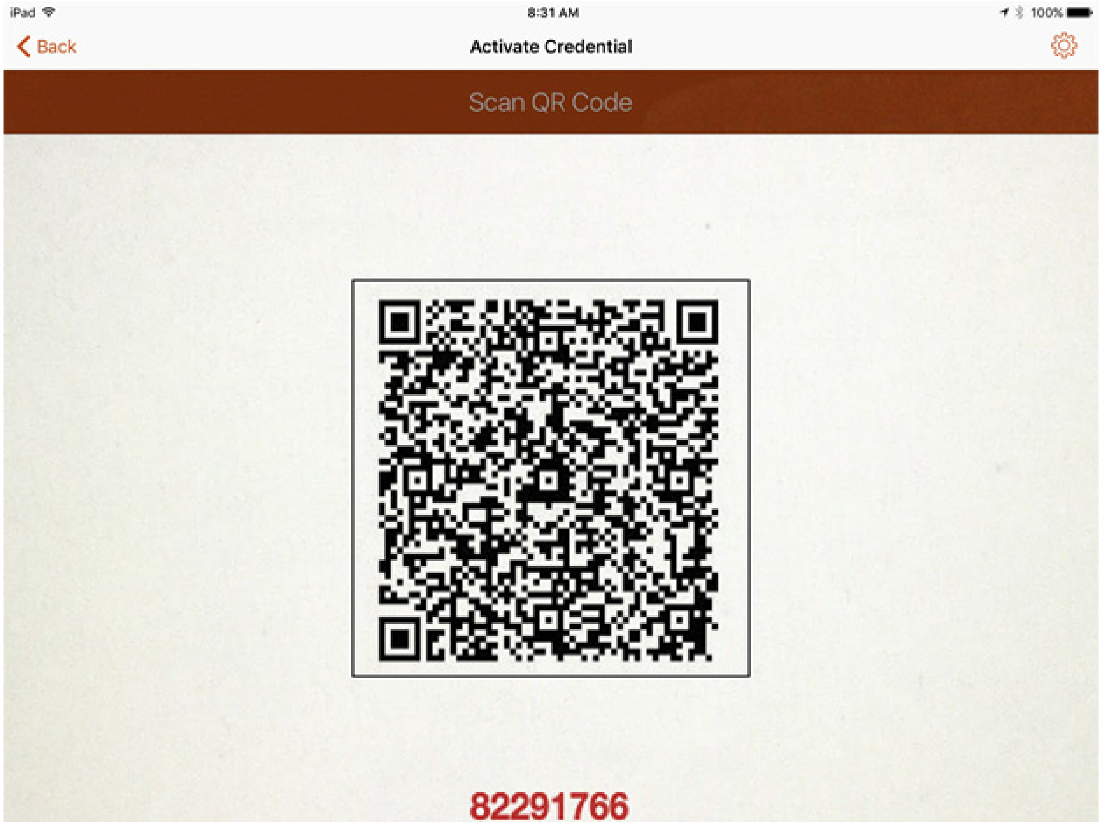
Welcome Back!

You can manage your credential or activate new credential with these options.

Manage Existing Credential

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.



iPad 8:31 AM 100%

Back

Activate Credential

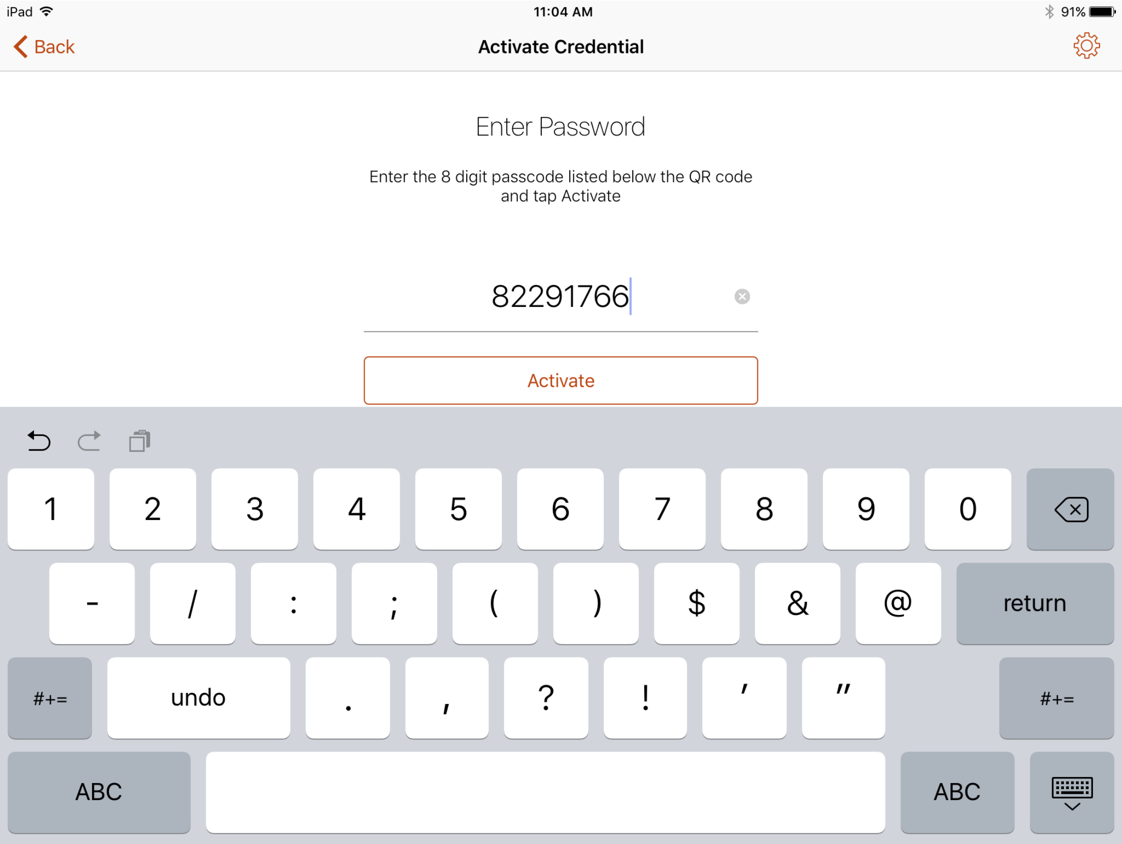
Scan QR Code

82291766

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**.



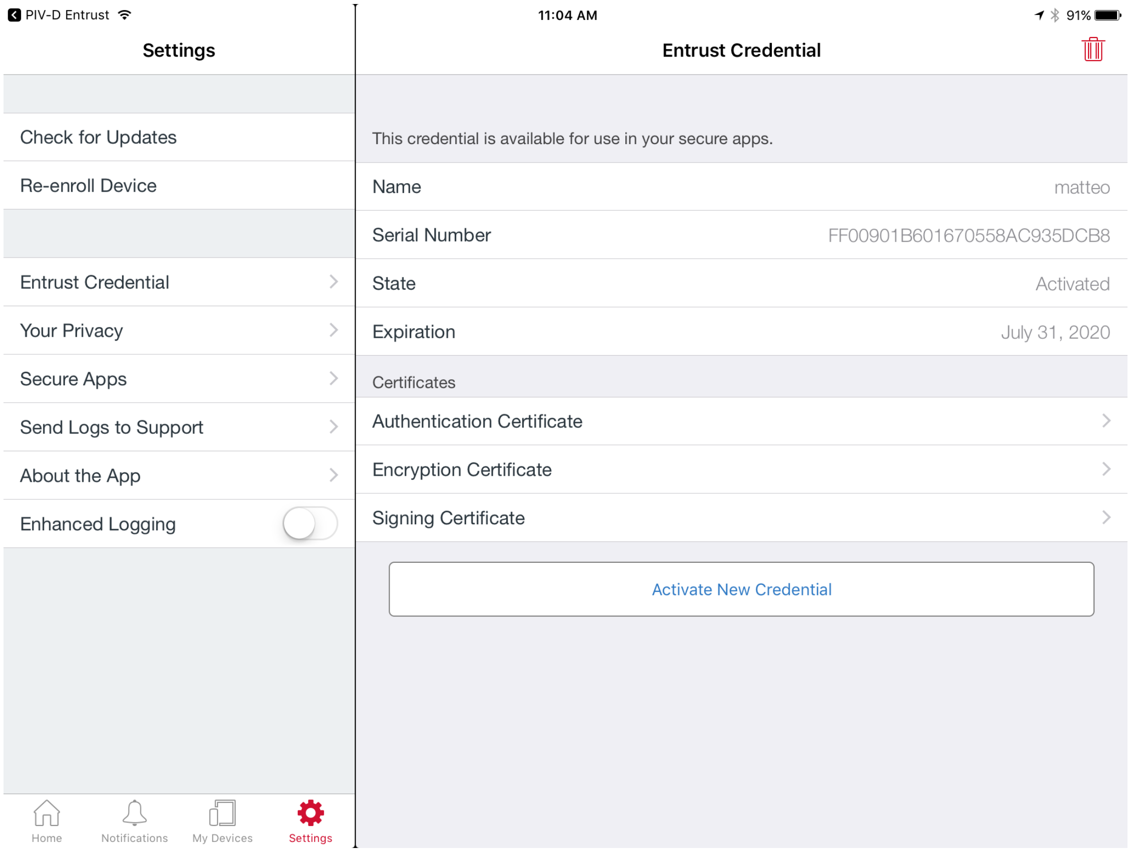
Activate Credential

Enter Password

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

82291766

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.



This credential is available for use in your secure apps.

Name matteo

Serial Number FF00901B601670558AC935DCB8

State Activated

Expiration July 31, 2020

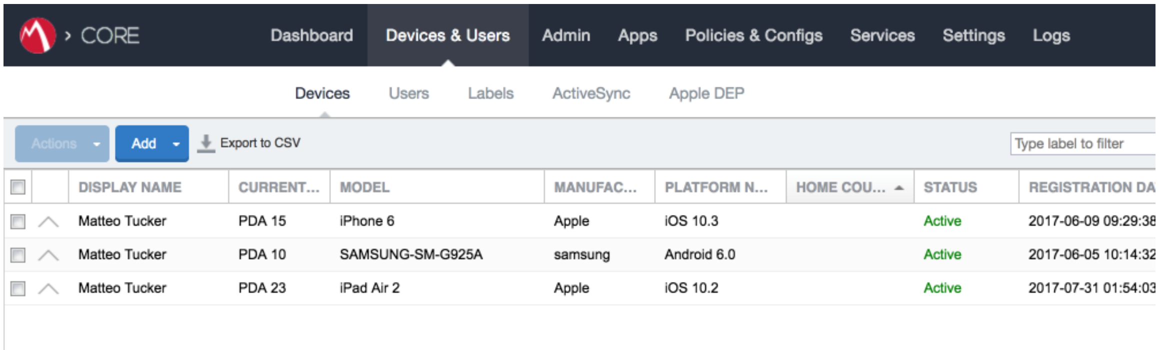
2.1.3.2 DPC Maintenance

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

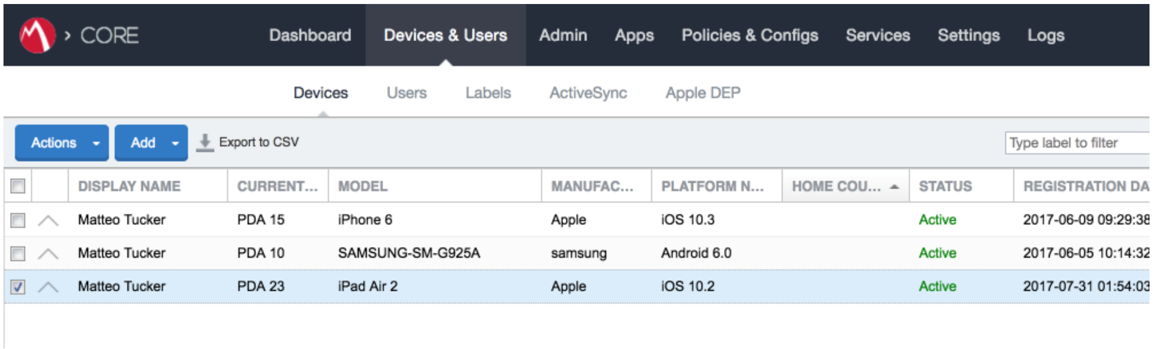
Termination of a DPC can be initiated from the MobileIron Admin Console. Upon completion of this workflow, the DPC stored in the MobileIron Apps@Work container will be cryptographically wiped (destroyed). These steps are performed by a MobileIron Core administrator.

1. In the MobileIron Admin Console, navigate to **Devices & Users > Devices**.



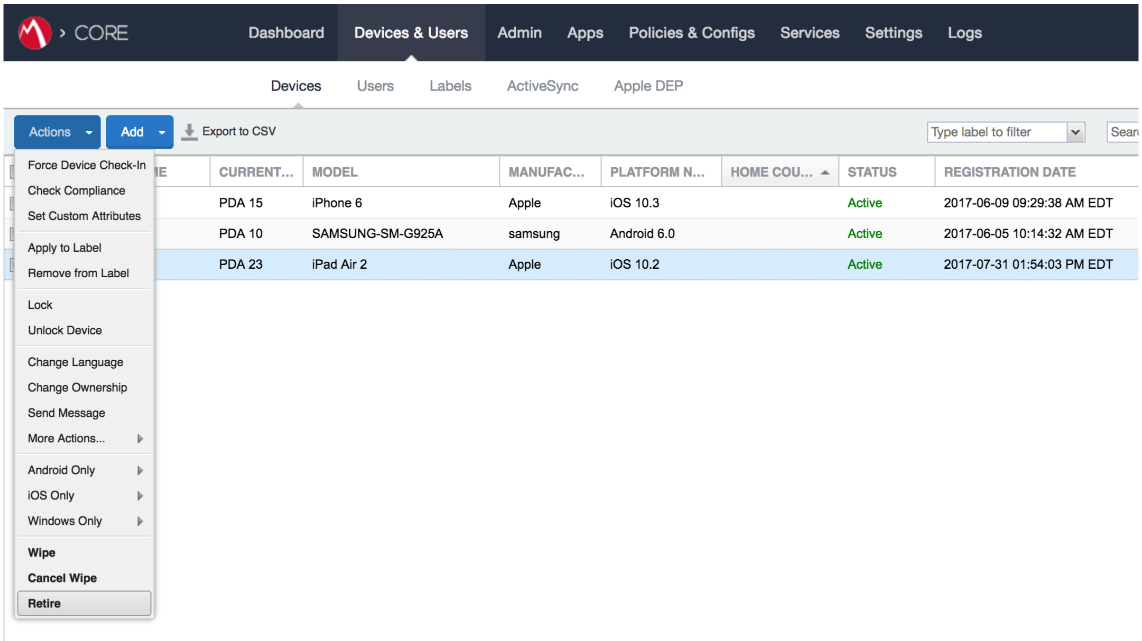
□		DISPLAY NAME	CURRENT...	MODEL	MANUFAC...	PLATFORM N...	HOME COU...	STATUS	REGISTRATION DA
□		Matteo Tucker	PDA 15	iPhone 6	Apple	iOS 10.3		Active	2017-06-09 09:29:38
□		Matteo Tucker	PDA 10	SAMSUNG-SM-G925A	samsung	Android 6.0		Active	2017-06-05 10:14:32
□		Matteo Tucker	PDA 23	iPad Air 2	Apple	iOS 10.2		Active	2017-07-31 01:54:03

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



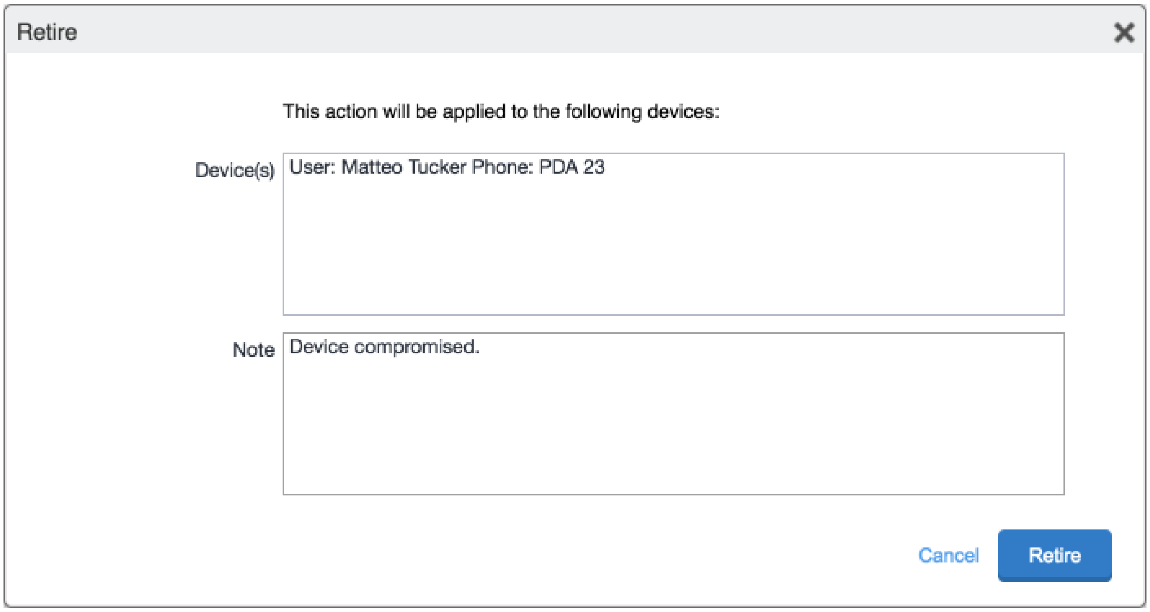
□		DISPLAY NAME	CURRENT...	MODEL	MANUFAC...	PLATFORM N...	HOME COU...	STATUS	REGISTRATION DA
□		Matteo Tucker	PDA 15	iPhone 6	Apple	iOS 10.3		Active	2017-06-09 09:29:38
□		Matteo Tucker	PDA 10	SAMSUNG-SM-G925A	samsung	Android 6.0		Active	2017-06-05 10:14:32
☑		Matteo Tucker	PDA 23	iPad Air 2	Apple	iOS 10.2		Active	2017-07-31 01:54:03

3. Select **Actions > Retire**.



E	CURRENT...	MODEL	MANUFAC...	PLATFORM N...	HOME COU...	STATUS	REGISTRATION DATE
	PDA 15	iPhone 6	Apple	iOS 10.3		Active	2017-06-09 09:29:38 AM EDT
	PDA 10	SAMSUNG-SM-G925A	samsung	Android 6.0		Active	2017-06-05 10:14:32 AM EDT
	PDA 23	iPad Air 2	Apple	iOS 10.2		Active	2017-07-31 01:54:03 PM EDT

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**.

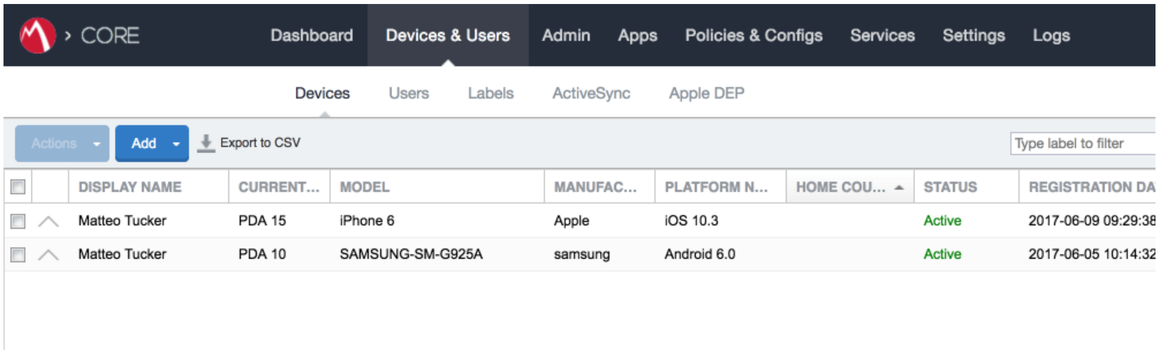


This action will be applied to the following devices:

Device(s): User: Matteo Tucker Phone: PDA 23

Note: Device compromised.

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



□		DISPLAY NAME	CURRENT...	MODEL	MANUFAC...	PLATFORM N...	HOME COU... ▲	STATUS	REGISTRATION DA
□	︿	Matteo Tucker	PDA 15	iPhone 6	Apple	iOS 10.3		Active	2017-06-09 09:29:38
□	︿	Matteo Tucker	PDA 10	SAMSUNG-SM-G925A	samsung	Android 6.0		Active	2017-06-05 10:14:32

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)

Figure 2-5 Mobile Device Hybrid Architecture for PIV Card and DPC Lifecycle Management (Intel Authenticate)

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 for specific installation procedures.

Table 2-3 SQL Server Components

Microsoft SQL Server Management Studio	11.0.5058.0
Microsoft Analysis Services Client Tools	11.0.5058.0
Microsoft Data Access Components (MDAC)	6.3.9600.17415
Microsoft Extensible Markup Language (MSXML)	3.0 6.0
Microsoft Internet Explorer	9.11.9600.18739
Microsoft .NET Framework	4.0.30319.42000
Operating System (OS)	6.3.9600

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:

Component	Comment
Java Runtime Environment 8.0	Download and install the latest update from the Oracle website. This build uses 8u121.
Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8	Download and install from the Oracle website.

2. Obtain the following configuration settings from your managed PKI instance:

Setting	Comment
Verizon SSP CA Path	Distinguished name to directory instance supplied by Verizon
Verizon SSP Enrollment Agent	Distinguished name for the Registration Authority supplied by Verizon
Verizon SSP Service Point	URI endpoint of the Verizon SSP web service supplied by Verizon
Verizon SSP Registration Authority Operator PKCS#12	Credentials are supplied by Verizon SSP
Verizon SSP Registration Authority Operator PKCS#12 Password	

3. Create a CA configuration by using the following procedures:

   a. In **MyID Desktop,** select the **Configuration** category.

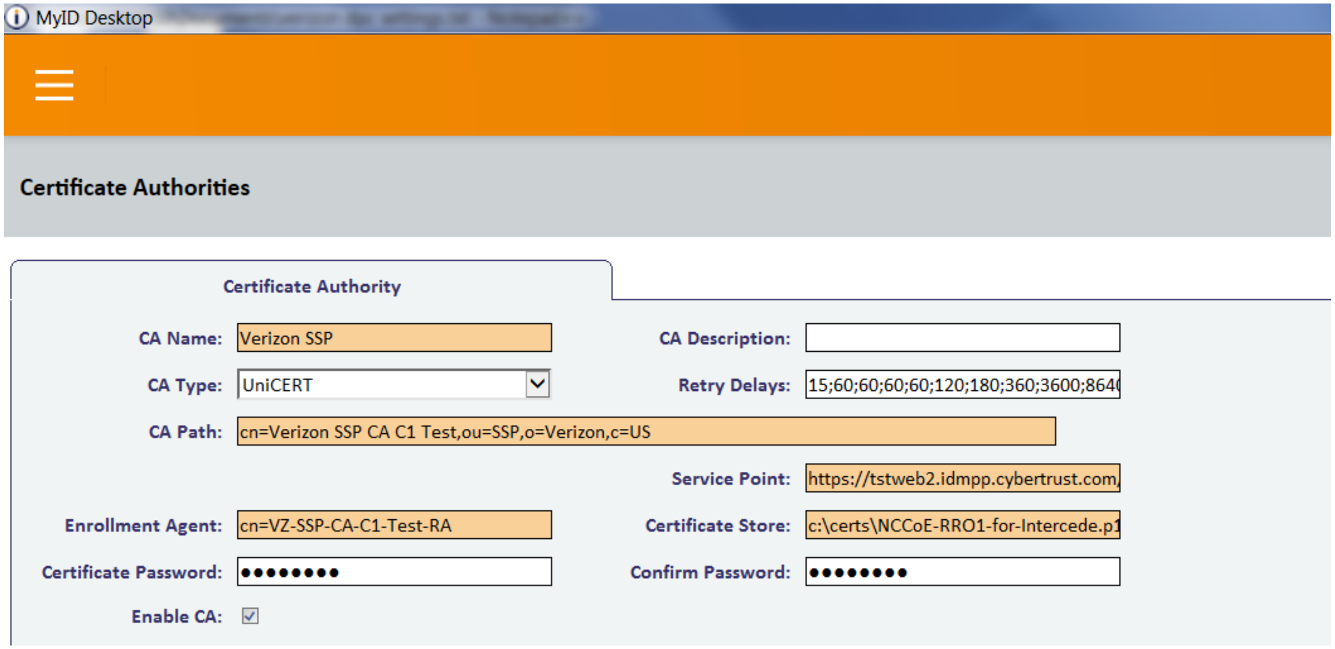
   b. Select **Certificate Authorities** from the **Configuration** menu.

   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:

CA Name	Enter a short name to identify the Verizon SSP
CA Description	Optional long description
CA Type	Leave this setting **UniCERT**
Retry Delays	Leave the defaults
CA Path	Retrieve setting from Step 2
Service Point	Retrieve setting from Step 2
Enrollment Agent	Retrieve setting from Step 2
Directory	Select the Entrust directory configured from Step **Error! Reference source not found.**
Certificate Store	Retrieve setting from Step 2 – enter fully qualified file path
Certificate Password	Retrieve setting from Step 2
Enable CA	Select this option



Certificate Authorities

Certificate Authority

CA Name:	Verizon SSP	CA Description:	
CA Type:	UniCERT	Retry Delays:	15;60;60;60;120;180;360;3600;864(
CA Path:	cn=Verizon SSP CA C1 Test,ou=SSP,o=Verizon,c=US		
		Service Point:	https://tstweb2.idmpp.cybertrust.com/
Enrollment Agent:	cn=VZ-SSP-CA-C1-Test-RA	Certificate Store:	c:\certs\NCCoE-RRO1-for-Intercede.p1
Certificate Password:	●●●●●●●●	Confirm Password:	●●●●●●●●
Enable CA:	☑		

   f. Click **Save**.

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.

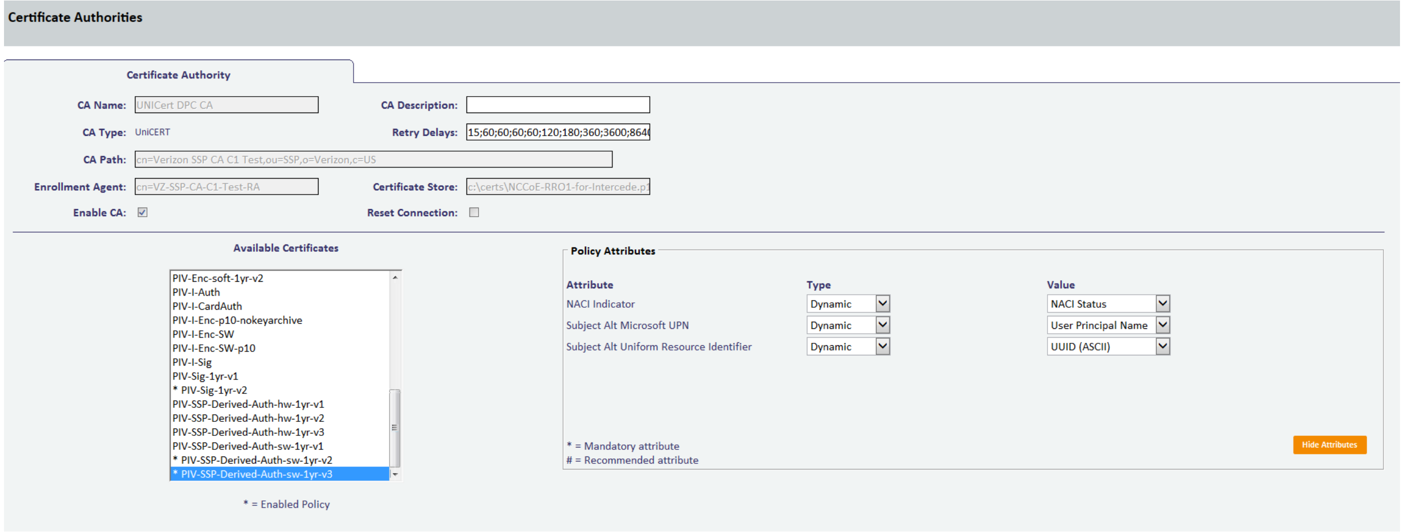
f. Set the following options for the policy.

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

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

Attribute	Type	Value
NACI Indicator	Dynamic	NACI Status
Subject Alt Microsoft UPN	Dynamic	User Principal Name
Subject Alt Uniform Resource Identifier	Dynamic	UUID

Figure 2-6 Certificate Profile Attributes



Certificate Authorities

Certificate Authority

CA Name:	UNICert DPC CA	CA Description:	
CA Type:	UniCERT	Retry Delays:	15;60;60;60;60;120;180;360;3600;864(
CA Path:	cn=Verizon SSP CA C1 Test,ou=SSP,o=Verizon,c=US		
Enrollment Agent:	cn=VZ-SSP-CA-C1-Test-RA	Certificate Store:	c:\certs\NCCoE-RRO1-for-Intercede.p1
Enable CA:	☑	Reset Connection:	□

Available Certificates

- PIV-Enc-soft-1yr-v2
- PIV-I-Auth
- PIV-I-CardAuth
- PIV-I-Enc-p10-nokeyarchive
- PIV-I-Enc-SW
- PIV-I-Enc-SW-p10
- PIV-I-Sig
- PIV-Sig-1yr-v1
- * PIV-Sig-1yr-v2
- PIV-SSP-Derived-Auth-hw-1yr-v1
- PIV-SSP-Derived-Auth-hw-1yr-v2
- PIV-SSP-Derived-Auth-hw-1yr-v3
- PIV-SSP-Derived-Auth-sw-1yr-v1
- * PIV-SSP-Derived-Auth-sw-1yr-v2
- * PIV-SSP-Derived-Auth-sw-1yr-v3

* = Enabled Policy

Policy Attributes

Attribute	Type	Value
NACI Indicator	Dynamic	NACI Status
Subject Alt Microsoft UPN	Dynamic	User Principal Name
Subject Alt Uniform Resource Identifier	Dynamic	UUID (ASCII)

* = Mandatory attribute
# = Recommended attribute

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:

Role	Permission
Mobile User	Console Logon, Request Derived Credentials (part 1), Mobile Certificate Recovery, Collect My Updates, Issue Device
Derived Credential Owner	Console Logon, Request Derived Credentials (part 2), Collect My Updates, Issue Device
PIV Applicant	Request Derived Credentials (part 2), Collect My Updates

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:

Setting	Value
Derived credential certificate OID	2.16.840.1.101.3.2.1.3.13

Derived credential signing certificate OID	2.16.840.1.101.3.2.1.3.6;
	2.16.840.1.101.3.2.1.3.7;
	2.16.840.1.101.3.2.1.3.16

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:

Setting	Value
Authentication Mode	PIN
Maximum PIN Length	12
Minimum PIN Length	6
Repeated Characters Allowed	1
Sequential Characters Allowed	1
Logon Attempts	5
PIN Inactivity Time	180
PIN History	0
Issue With	User specified PIN (default)
Email PIN	Unselect
Length	0

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

j. Click **Next.**

k. In the **Select Certificates** tab, check **PIV-SSP-Derived-Auth-sw-1yr-v3** along with **Signing** under **Certificate Policy Description.** Choose **Authentication Certificate** in the **Container** drop-down.

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 the 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

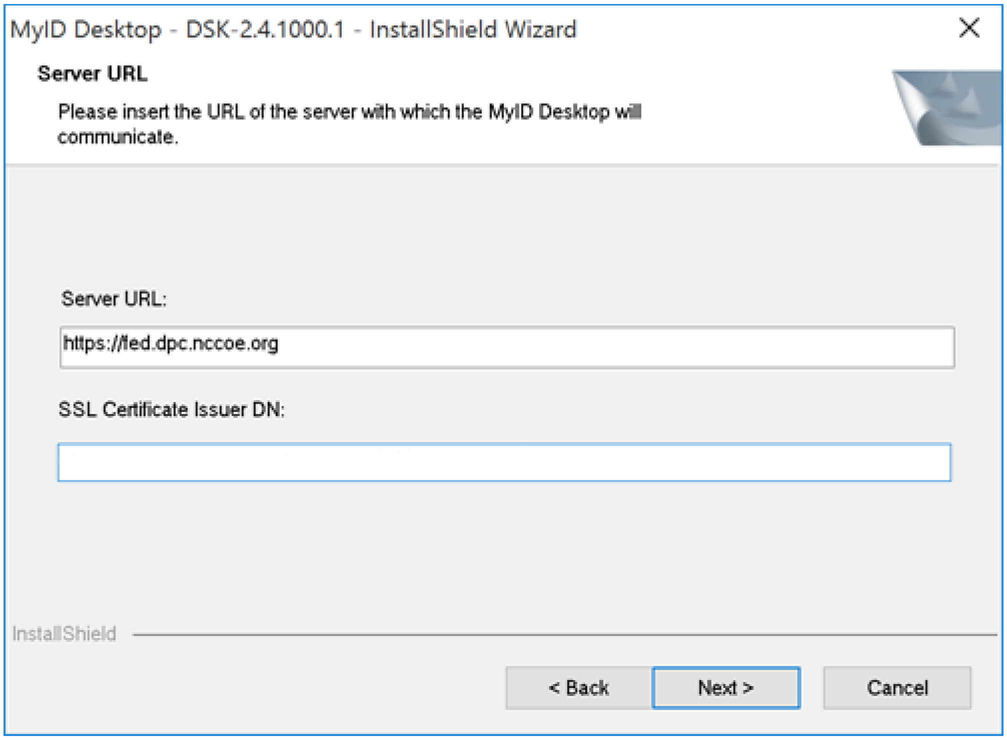
The Intercede Desktop component of this example solution serves as the main point of administration of the MyID CMS. It was installed on a Dell Latitude E6540 laptop running Windows 7. The procedures below are adapted from the *Installation and Configuration Guide Version 10.8,* Section 7.4.

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.**



MyID Desktop - DSK-2.4.1000.1 - InstallShield Wizard

Server URL

Please insert the URL of the server with which the MyID Desktop will communicate.

Server URL: https://fed.dpc.nccoe.org

SSL Certificate Issuer DN:

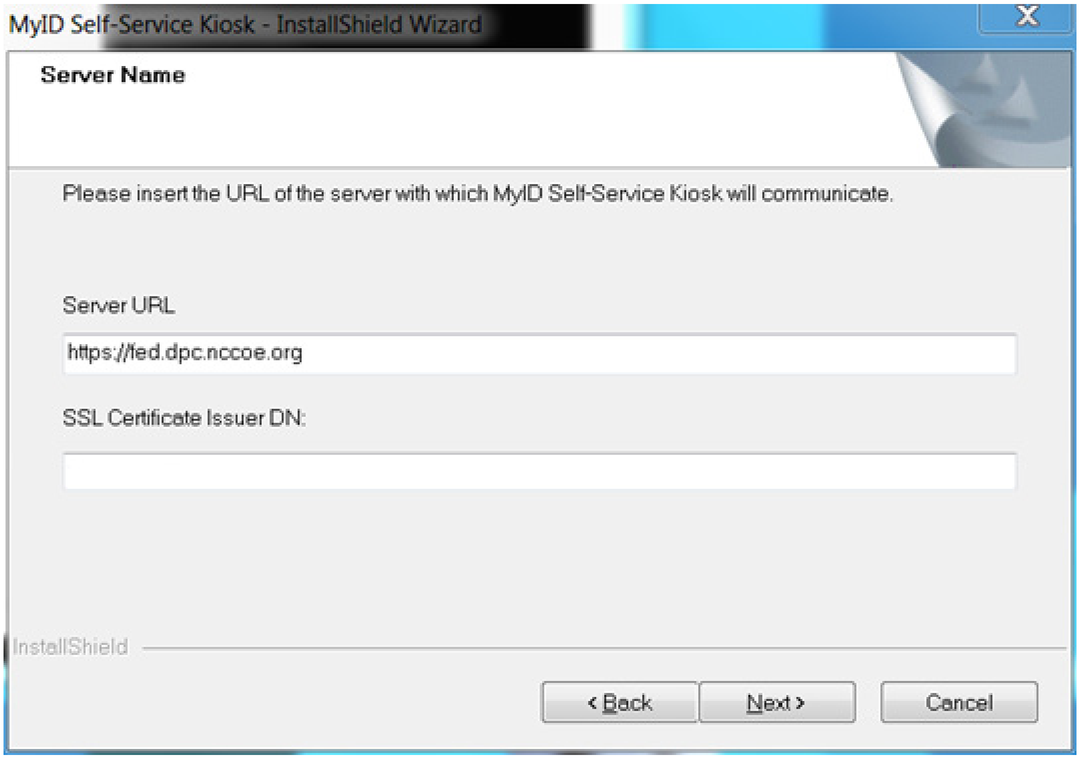
2.2.4 Intercede Self-Service Kiosk

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.**



MyID Self-Service Kiosk - InstallShield Wizard

Server Name

Please insert the URL of the server with which MyID Self-Service Kiosk will communicate.

Server URL

https://fed.dpc.nccoe.org

SSL Certificate Issuer DN:

2.2.4.2 Configuration

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

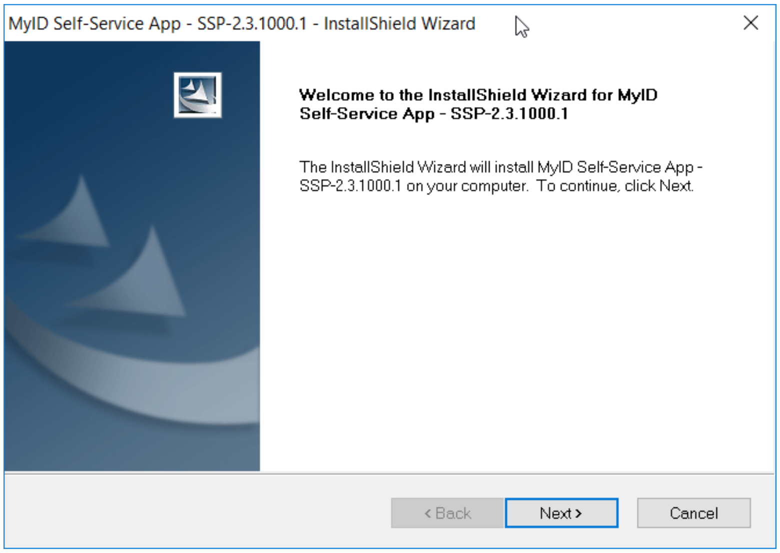
1. Set the timeout for the PIN entry screen by using the following procedures:
    a. Open C:\Program Files (x86)\Intercede\MyIDSelfServiceKiosk\MyIDKiosk.exe.config by using a text editor.
    b. Edit the **value** parameter in the following line:
    ```
    <add key="DerivedCredentialsPageTimeoutSeconds" value="120"/>
    ```
    c. Edit the **value** parameter in the following line with the MyID application server address:
    ```
    <add key="Server" value="http://myserver.example.com/"></add>
    ```
    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**.

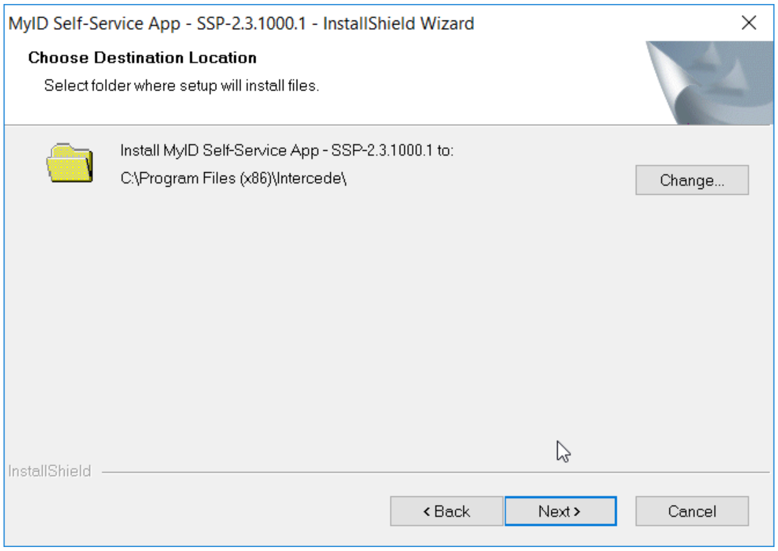


MyID Self-Service App - SSP-2.3.1000.1 - InstallShield Wizard

Welcome to the InstallShield Wizard for MyID Self-Service App - SSP-2.3.1000.1

The InstallShield Wizard will install MyID Self-Service App - SSP-2.3.1000.1 on your computer. To continue, click Next.

3. Click **Next**.



MyID Self-Service App - SSP-2.3.1000.1 - InstallShield Wizard

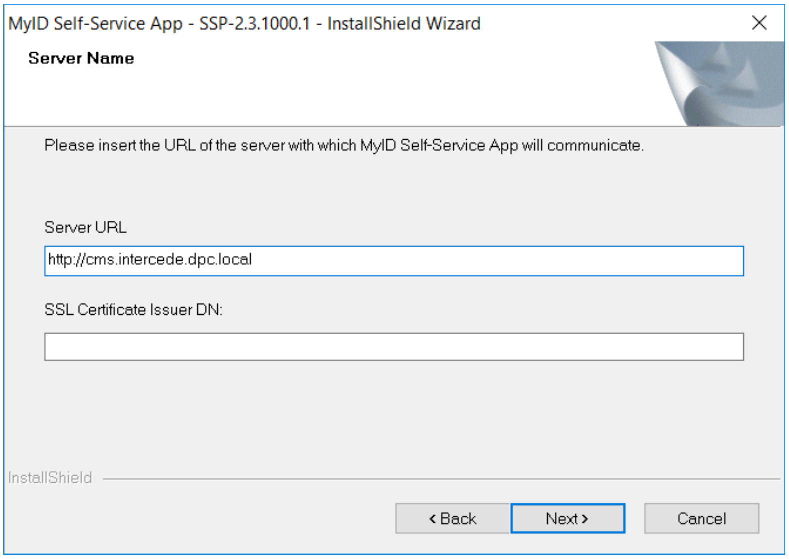
Choose Destination Location

Select folder where setup will install files.

Install MyID Self-Service App - SSP-2.3.1000.1 to:
C:\Program Files (x86)\Intercede\

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**.


MyID Self-Service App - SSP-2.3.1000.1 - InstallShield Wizard

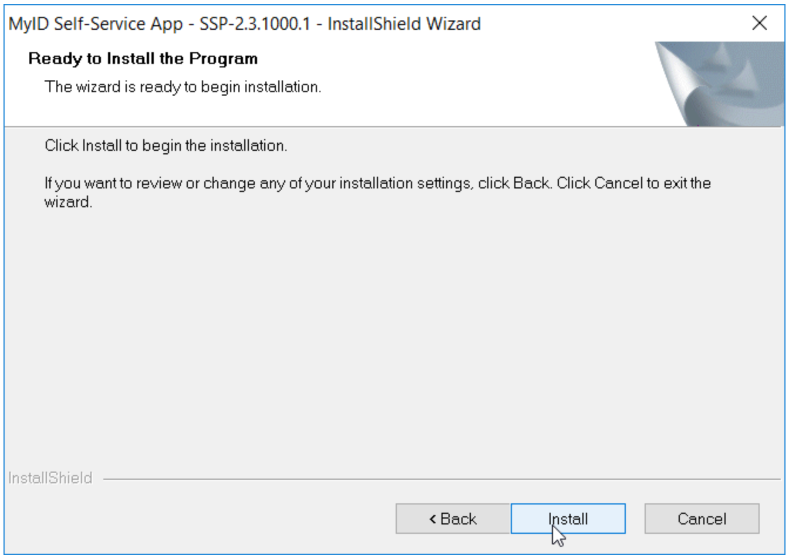
Server Name

Please insert the URL of the server with which MyID Self-Service App will communicate.

Server URL: http://cms.intercede.dpc.local

SSL Certificate Issuer DN:

6. Click **Install**.


MyID Self-Service App - SSP-2.3.1000.1 - InstallShield Wizard

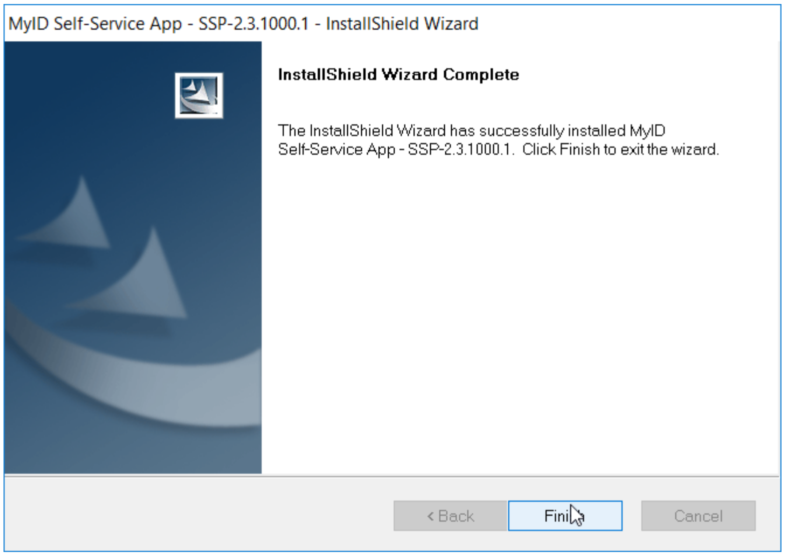
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

7. Click **Finish**.



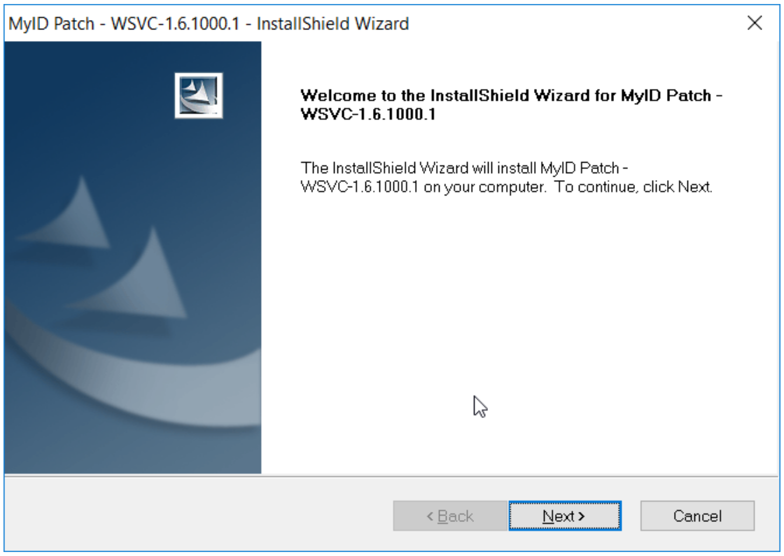
MyID Self-Service App - SSP-2.3.1000.1 - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed MyID Self-Service App - SSP-2.3.1000.1. Click Finish to exit the wizard.

2.2.5.2 Installing the WSVC Service

1. Run **WSVC-1.6.1000.1_B.msi.**
2. Click **Next.**

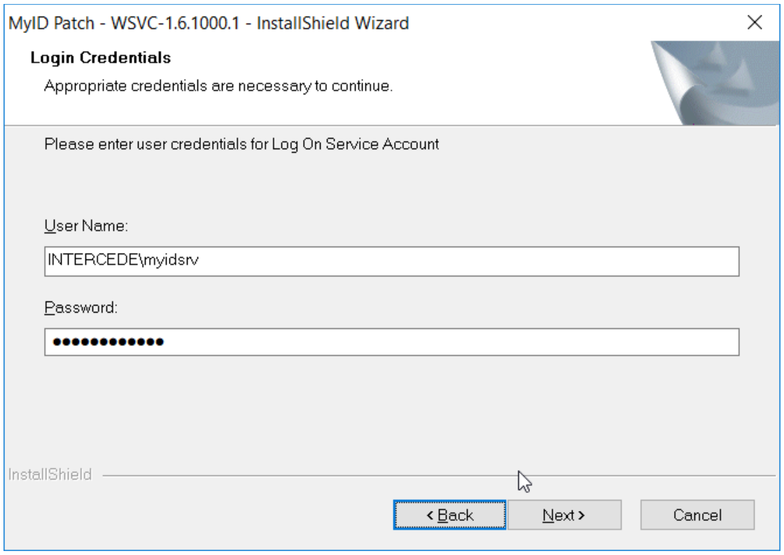


MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

Welcome to the InstallShield Wizard for MyID Patch - WSVC-1.6.1000.1

The InstallShield Wizard will install MyID Patch - WSVC-1.6.1000.1 on your computer. To continue, click Next.

3. Enter the username and password for the account that will install the service.
4. Click **Next.**


MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

Login Credentials

Appropriate credentials are necessary to continue.

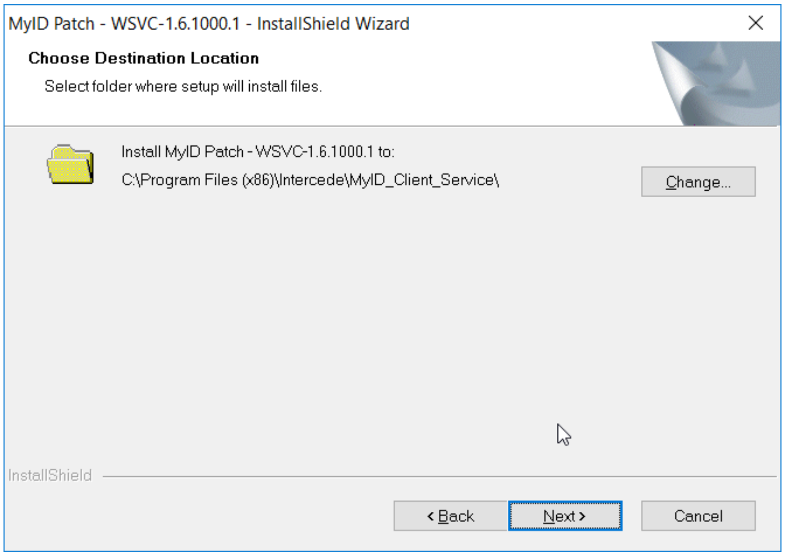
Please enter user credentials for Log On Service Account

User Name: INTERCEDE\myidsrv

Password: ●●●●●●●●●●●●●

710

711 5. Click **Next.**


MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

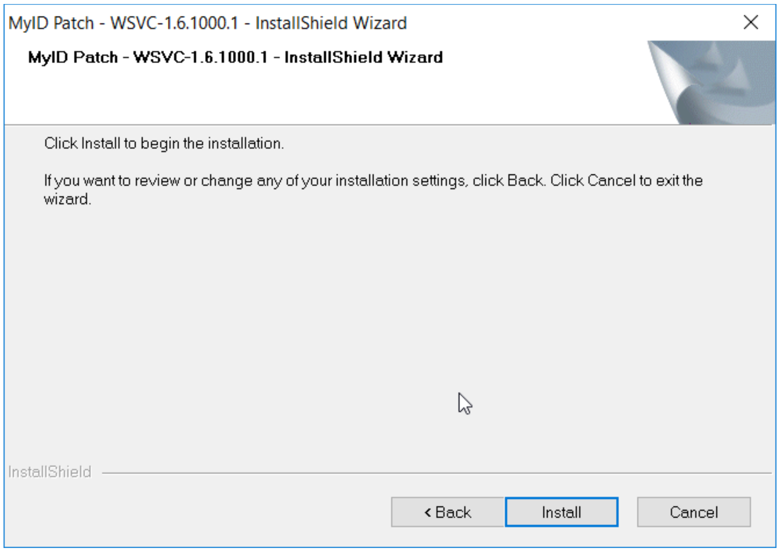
Choose Destination Location

Select folder where setup will install files.

Install MyID Patch - WSVC-1.6.1000.1 to:
C:\Program Files (x86)\Intercede\MyID_Client_Service\

712

713 6. Click **Install.**

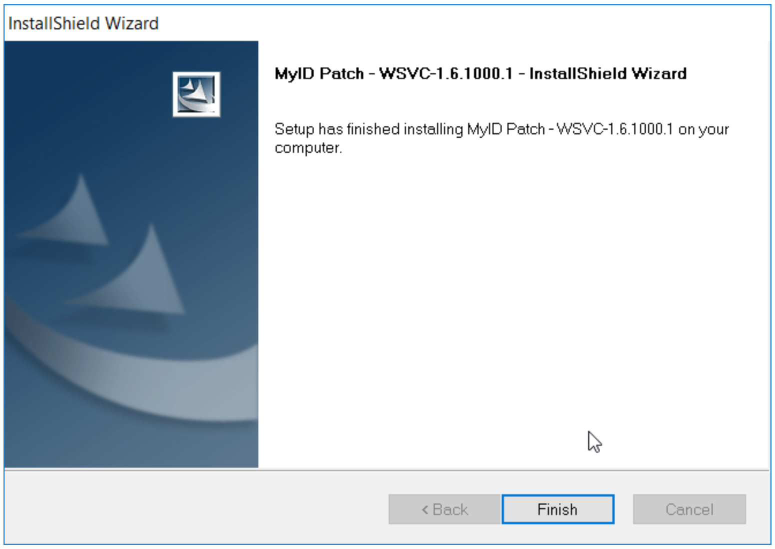

MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

7. Click **Finish.**


InstallShield Wizard

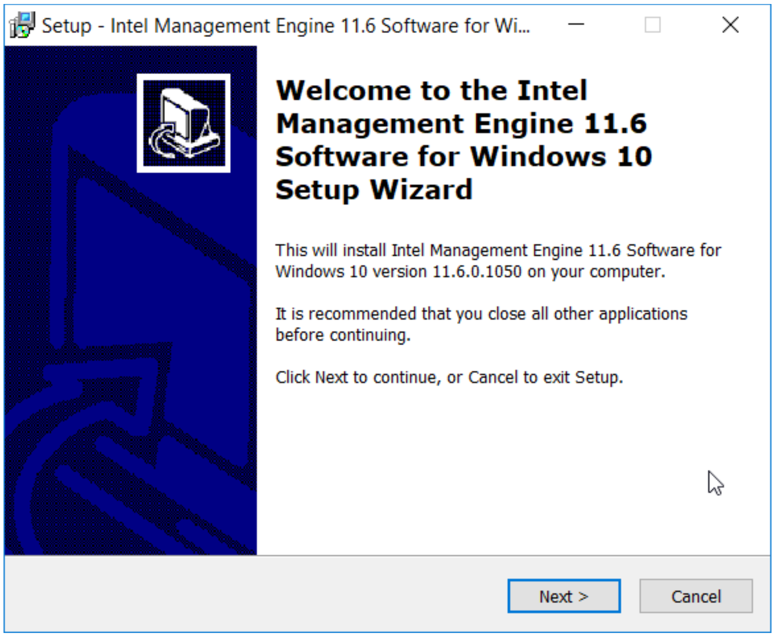
MyID Patch - WSVC-1.6.1000.1 - InstallShield Wizard

Setup has finished installing MyID Patch - WSVC-1.6.1000.1 on your computer.

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.**



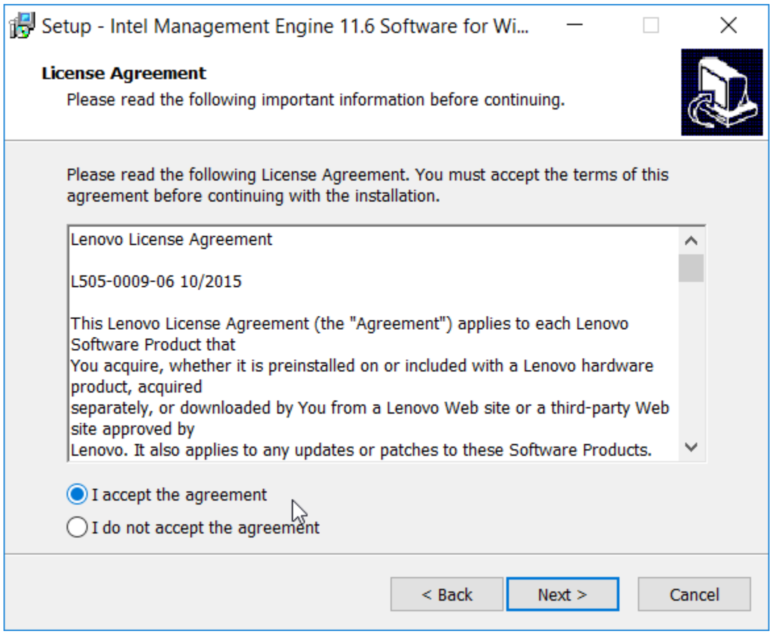
Welcome to the Intel Management Engine 11.6 Software for Windows 10 Setup Wizard

This will install Intel Management Engine 11.6 Software for Windows 10 version 11.6.0.1050 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

3. Select **I accept the agreement.**
4. Click **Next.**



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Lenovo License Agreement

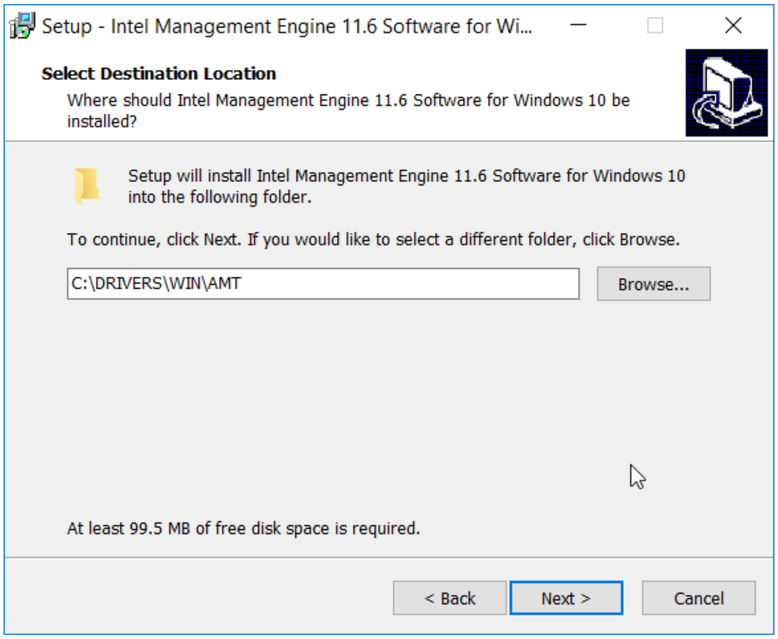
L505-0009-06 10/2015

This Lenovo License Agreement (the "Agreement") applies to each Lenovo Software Product that
You acquire, whether it is preinstalled on or included with a Lenovo hardware product, acquired
separately, or downloaded by You from a Lenovo Web site or a third-party Web site approved by
Lenovo. It also applies to any updates or patches to these Software Products.

● I accept the agreement

○ I do not accept the agreement

5. Click **Next.**



Select Destination Location

Where should Intel Management Engine 11.6 Software for Windows 10 be installed?

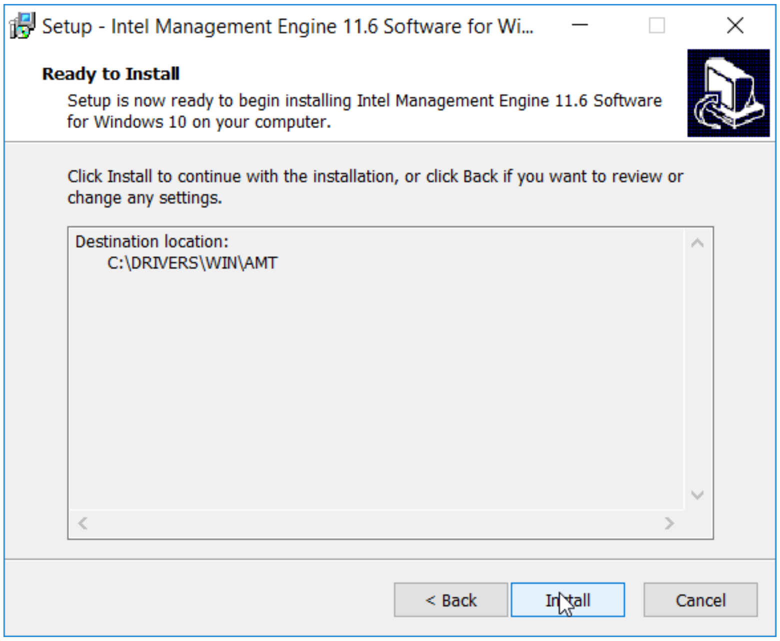
Setup will install Intel Management Engine 11.6 Software for Windows 10 into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\DRIVERS\WIN\AMT

At least 99.5 MB of free disk space is required.

6. Click **Install.**



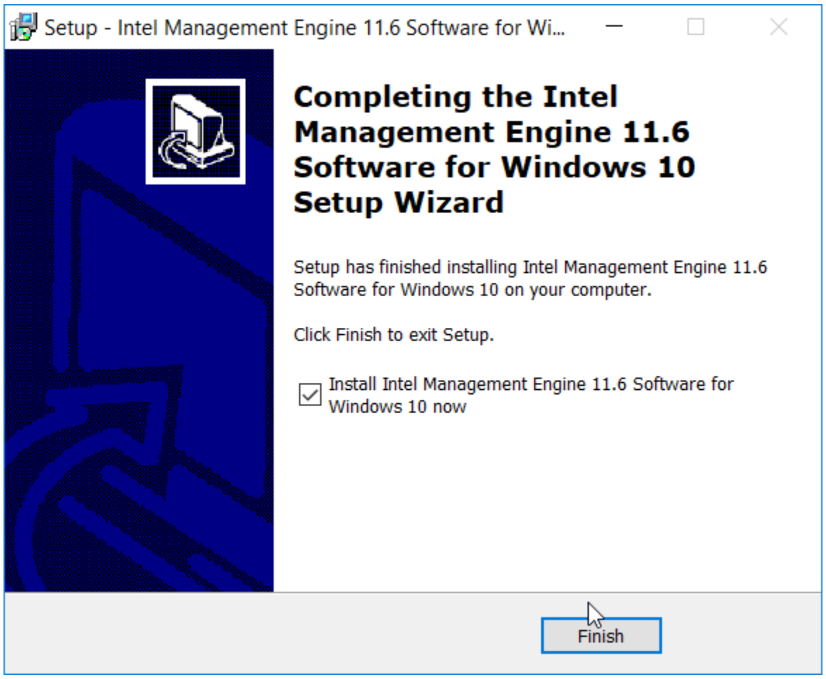
Ready to Install

Setup is now ready to begin installing Intel Management Engine 11.6 Software for Windows 10 on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\DRIVERS\WIN\AMT

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



Setup - Intel Management Engine 11.6 Software for Wi...

Completing the Intel Management Engine 11.6 Software for Windows 10 Setup Wizard

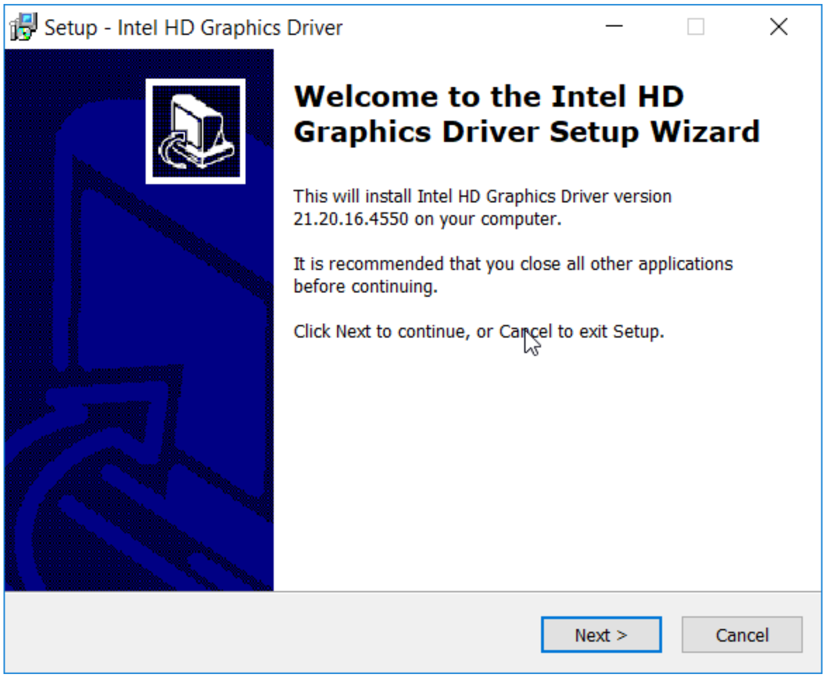
Setup has finished installing Intel Management Engine 11.6 Software for Windows 10 on your computer.

Click Finish to exit Setup.

☑ Install Intel Management Engine 11.6 Software for Windows 10 now

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

10. Click **Next.**



Setup - Intel HD Graphics Driver

Welcome to the Intel HD Graphics Driver Setup Wizard

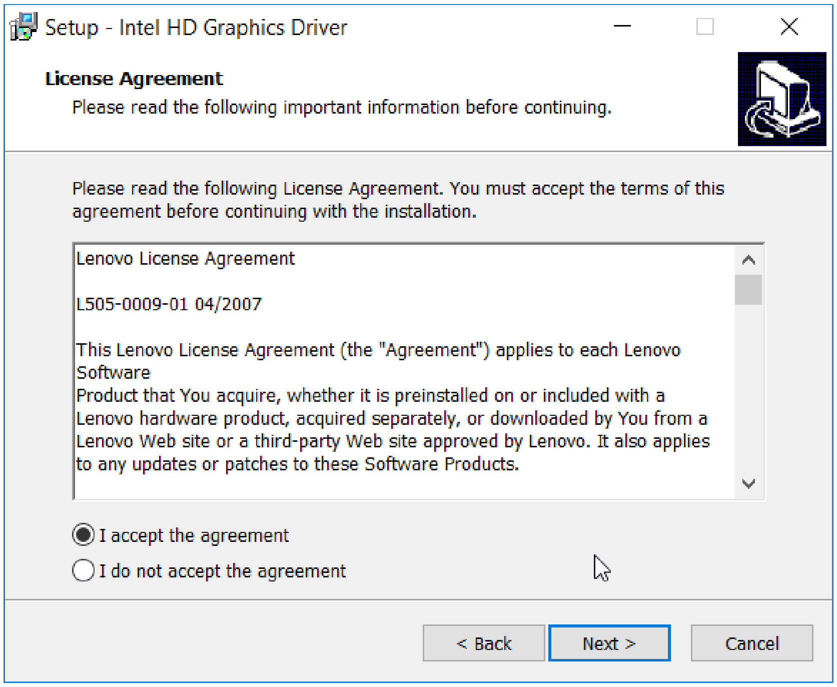
This will install Intel HD Graphics Driver version 21.20.16.4550 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

11. Select **I accept the agreement.**

12. Click **Next.**



Setup - Intel HD Graphics Driver

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Lenovo License Agreement

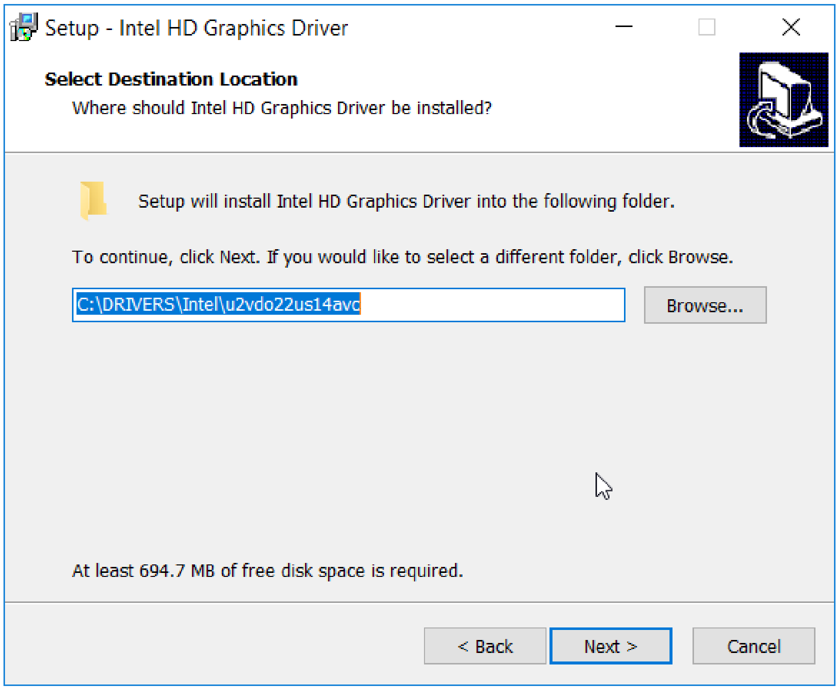
L505-0009-01 04/2007

This Lenovo License Agreement (the "Agreement") applies to each Lenovo Software
Product that You acquire, whether it is preinstalled on or included with a Lenovo hardware product, acquired separately, or downloaded by You from a Lenovo Web site or a third-party Web site approved by Lenovo. It also applies to any updates or patches to these Software Products.

● I accept the agreement

○ I do not accept the agreement

13. Click **Next.**



Setup - Intel HD Graphics Driver

Select Destination Location

Where should Intel HD Graphics Driver be installed?

Setup will install Intel HD Graphics Driver into the following folder.

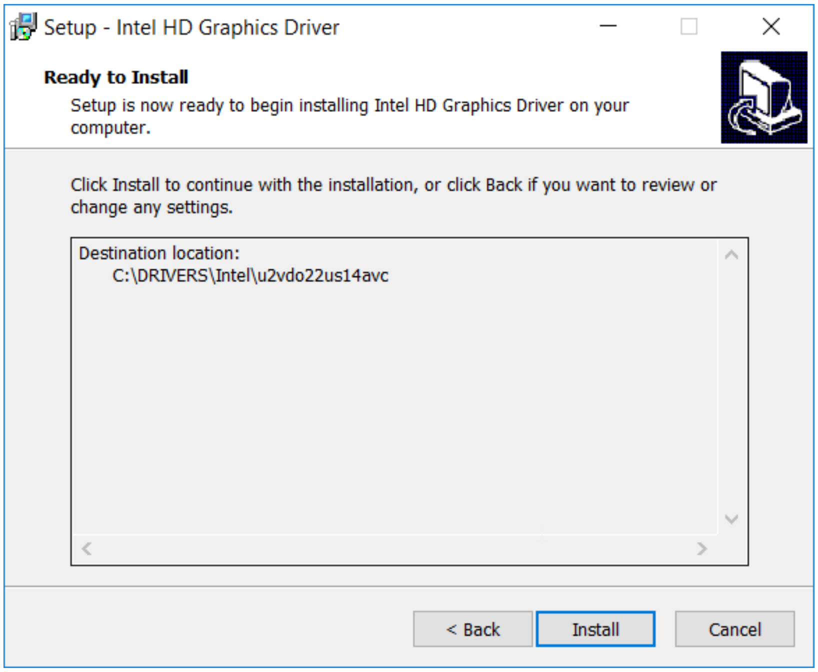
To continue, click Next. If you would like to select a different folder, click Browse.

C:\DRIVERS\Intel\u2vdo22us14avc

At least 694.7 MB of free disk space is required.

743

744 14. Click **Install.**



Setup - Intel HD Graphics Driver

Ready to Install

Setup is now ready to begin installing Intel HD Graphics Driver on your computer.

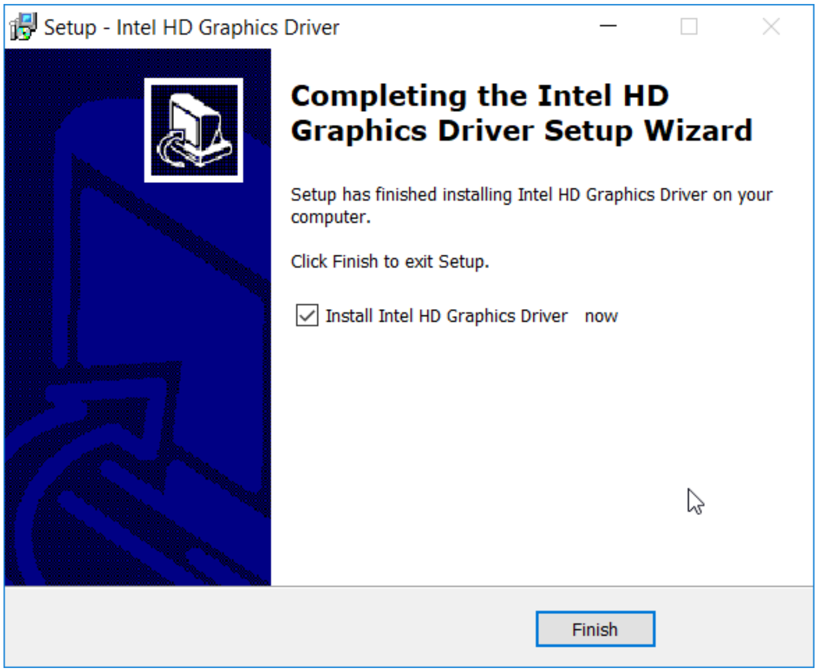
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\DRIVERS\Intel\u2vdo22us14avc

745

746 15. Check the box next to **Install Intel HD Graphics Driver now.**

16. Click **Finish.**



Completing the Intel HD Graphics Driver Setup Wizard

Setup has finished installing Intel HD Graphics Driver on your computer.

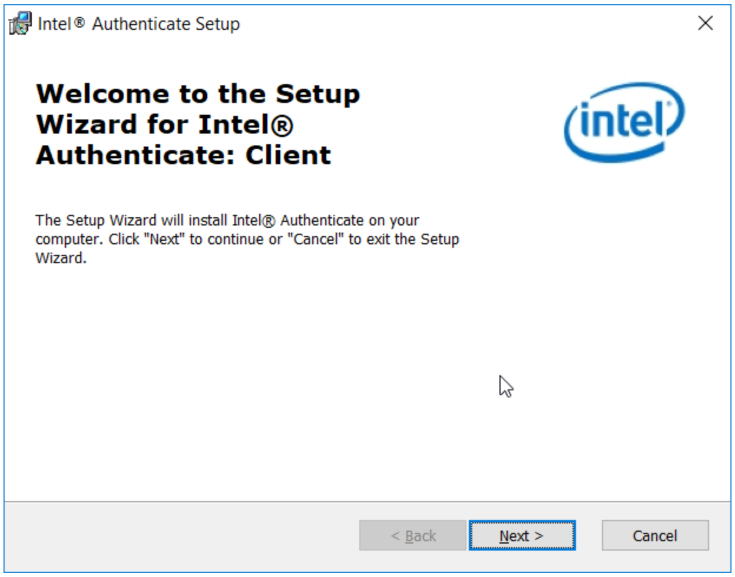
Click Finish to exit Setup.

☑ Install Intel HD Graphics Driver now

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.

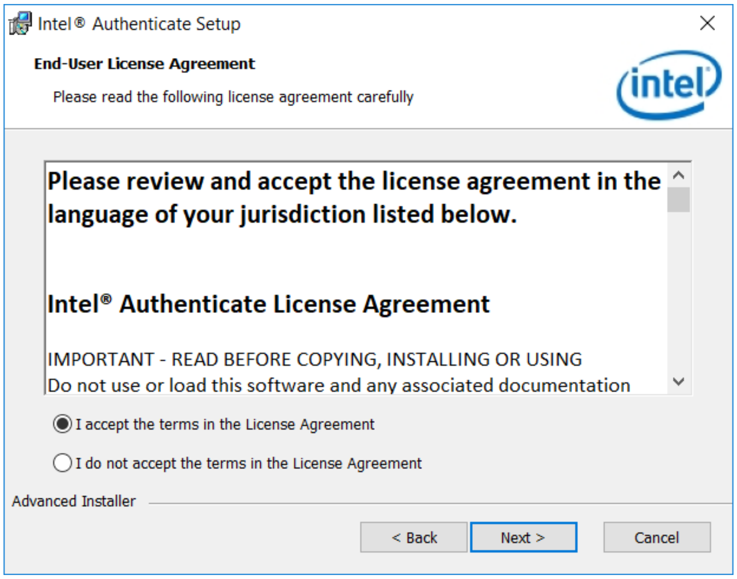
1. Run **IAx64-2.5.0.68.msi**.
2. Click **Next.**



Welcome to the Setup Wizard for Intel® Authenticate: Client

The Setup Wizard will install Intel® Authenticate on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

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



End-User License Agreement

Please read the following license agreement carefully

Please review and accept the license agreement in the language of your jurisdiction listed below.

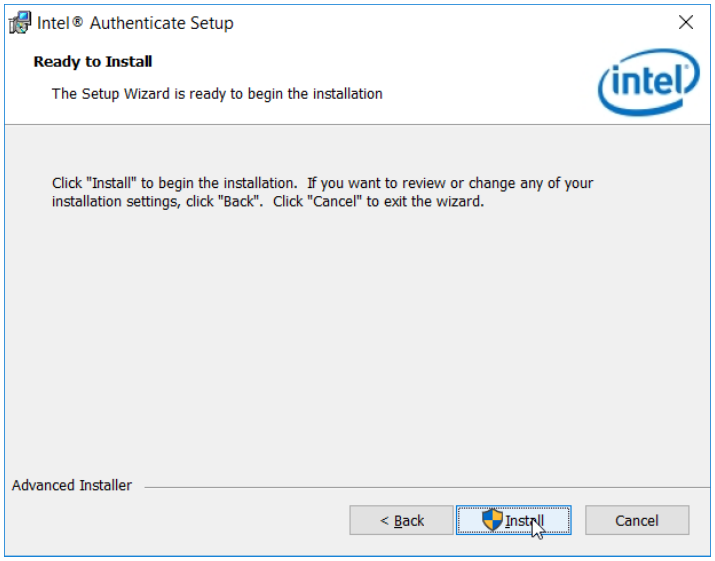
Intel® Authenticate License Agreement

IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING
Do not use or load this software and any associated documentation

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

5. Click **Install.**

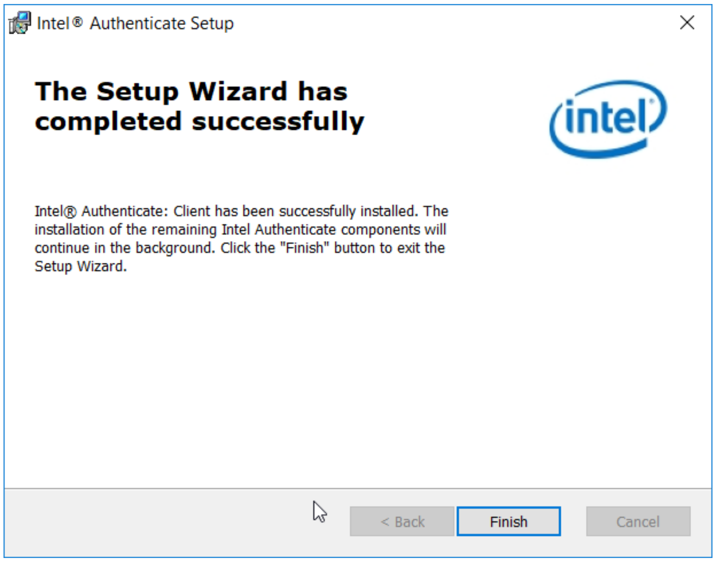

Intel® Authenticate Setup

Ready to Install

The Setup Wizard is ready to begin the installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

6. Click **Finish.**


Intel® Authenticate Setup

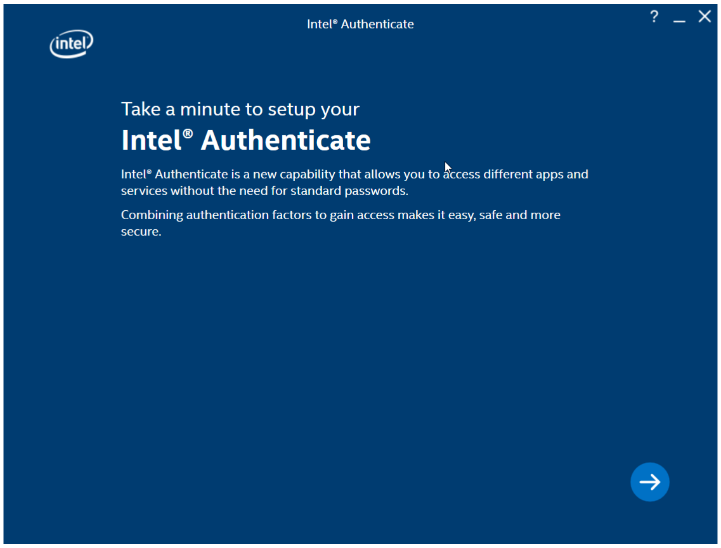
The Setup Wizard has completed successfully

Intel® Authenticate: Client has been successfully installed. The installation of the remaining Intel Authenticate components will continue in the background. Click the "Finish" button to exit the Setup Wizard.

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.**



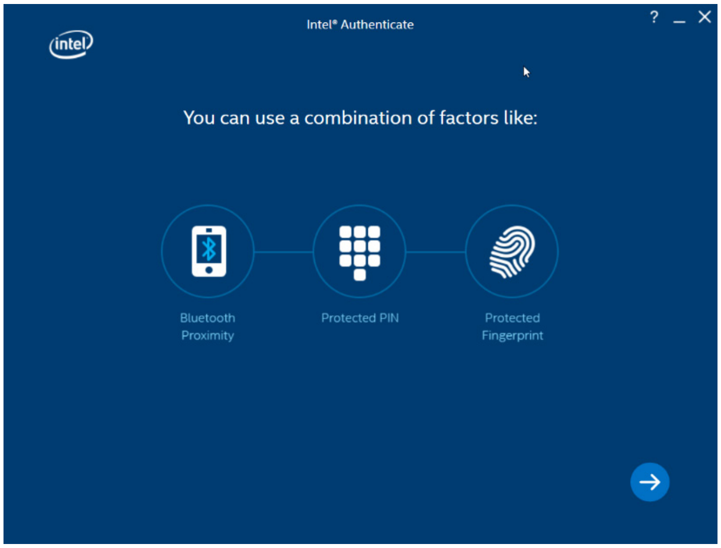
Take a minute to setup your

Intel® Authenticate

Intel® Authenticate is a new capability that allows you to access different apps and services without the need for standard passwords.

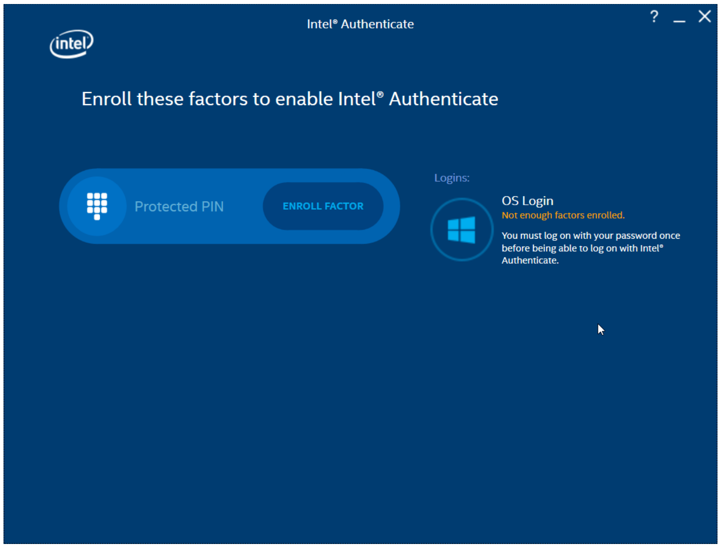
Combining authentication factors to gain access makes it easy, safe and more secure.

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



You can use a combination of factors like:

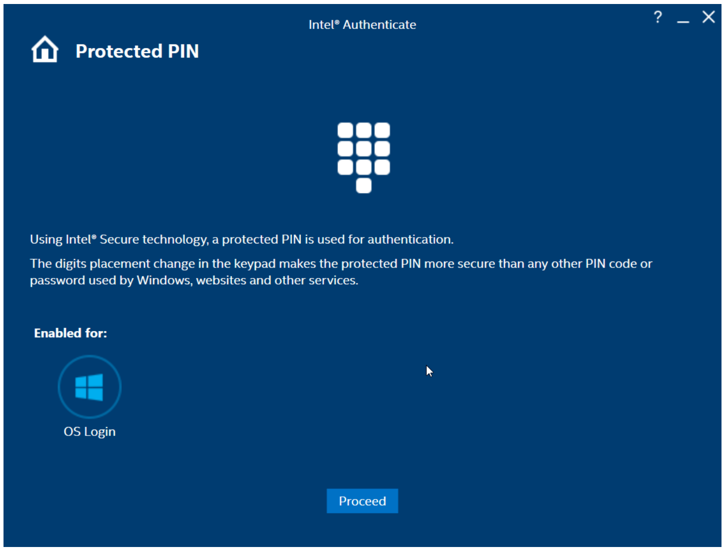
4. Click **Enroll Factor.**



Enroll these factors to enable Intel® Authenticate

OS Login
Not enough factors enrolled.
You must log on with your password once before being able to log on with Intel® Authenticate.

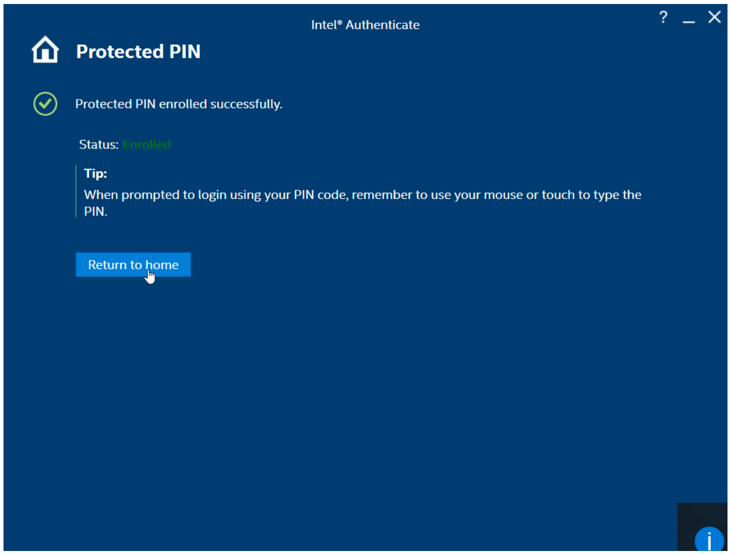
5. Click **Proceed.**



Using Intel® Secure technology, a protected PIN is used for authentication.

The digits placement change in the keypad makes the protected PIN more secure than any other PIN code or password used by Windows, websites and other services.

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.**

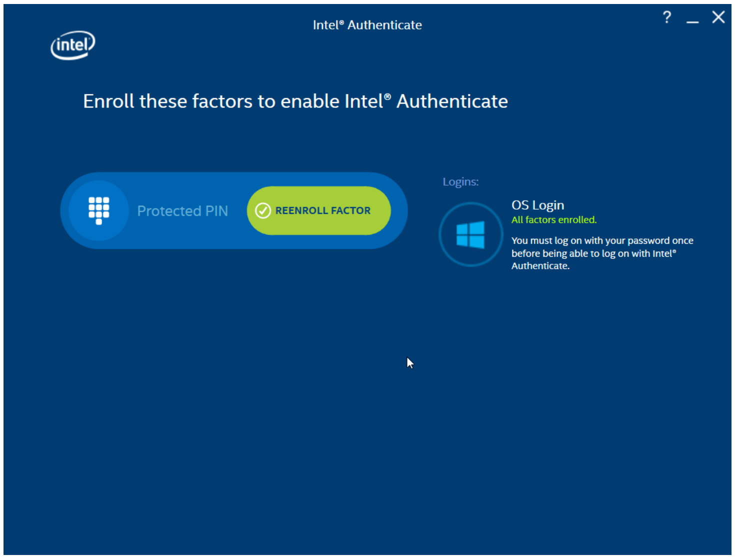


Protected PIN

Protected PIN enrolled successfully.

Status: Enrolled

Tip:
When prompted to login using your PIN code, remember to use your mouse or touch to type the PIN.



Enroll these factors to enable Intel® Authenticate

OS Login
All factors enrolled.
You must log on with your password once before being able to log on with Intel® Authenticate.

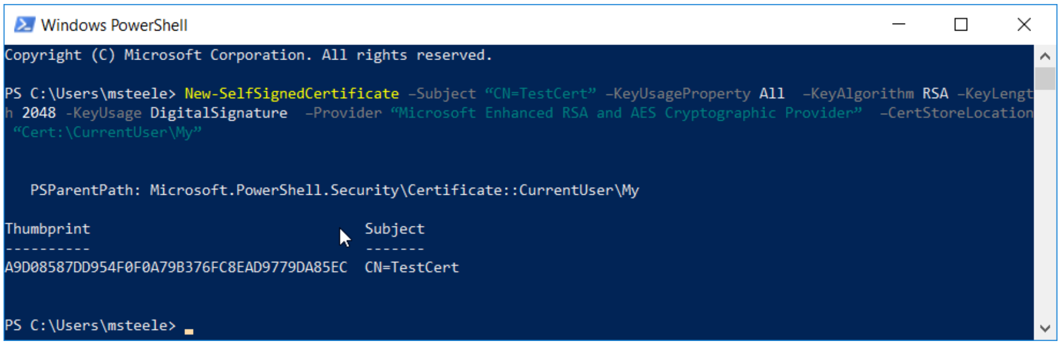
2.2.6 Intel Authenticate GPO

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

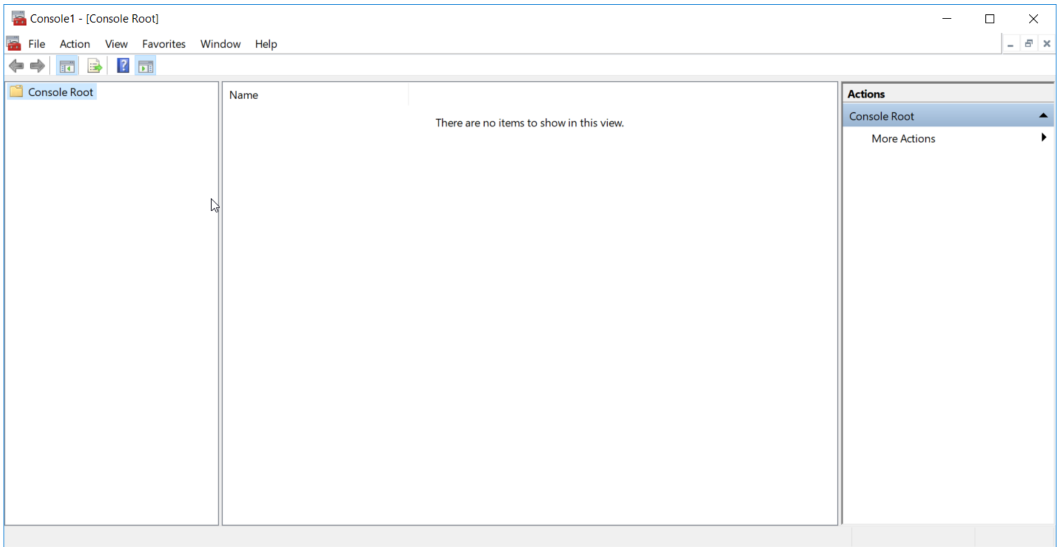
1. In a new PowerShell window, generate a new self-signed certificate to sign the Intel Policy. Enter the command:

```
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”
```



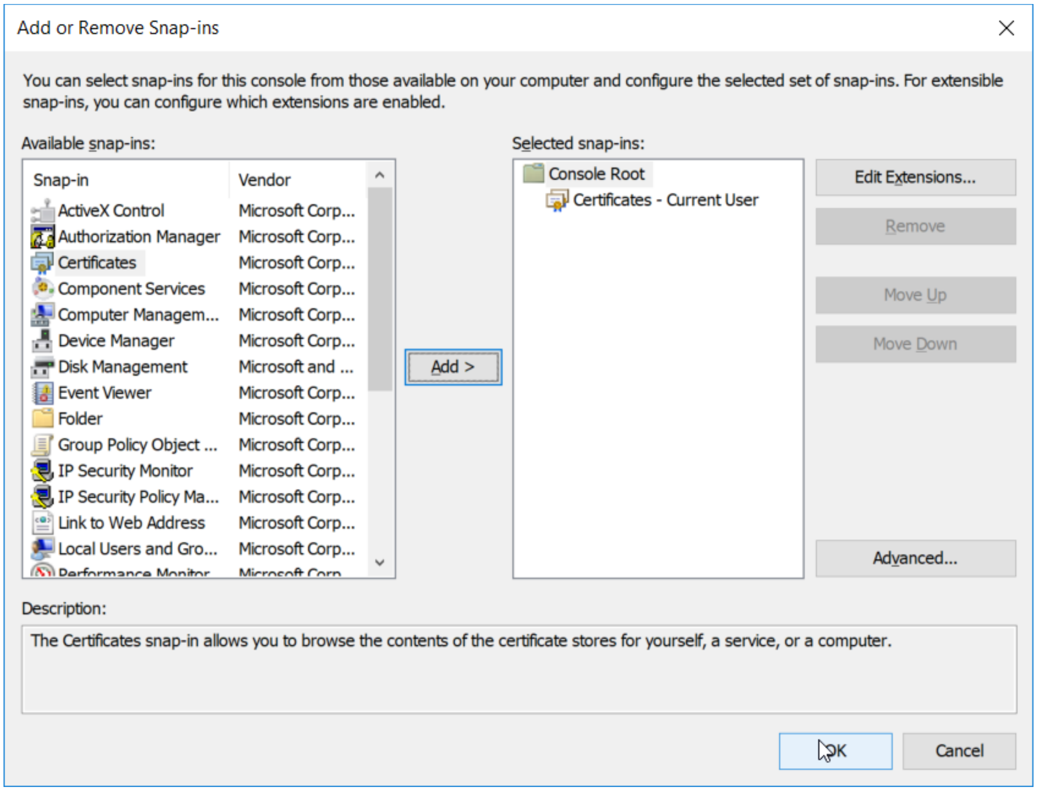
```
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\msteele> New-SelfSignedCertificate -Subject “CN=TestCert” -KeyUsageProperty All  -KeyAlgorithm RSA -KeyLengt
h 2048 -KeyUsage DigitalSignature  -Provider “Microsoft Enhanced RSA and AES Cryptographic Provider”  -CertStoreLocation
 “Cert:\CurrentUser\My”


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
A9D08587DD954F0F0A79B376FC8EAD9779DA85EC  CN=TestCert


PS C:\Users\msteele> _
```

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



There are no items to show in this view.

3. Select **File > Add/Remove Snap-In.** Add the **Certificates** snap-in.

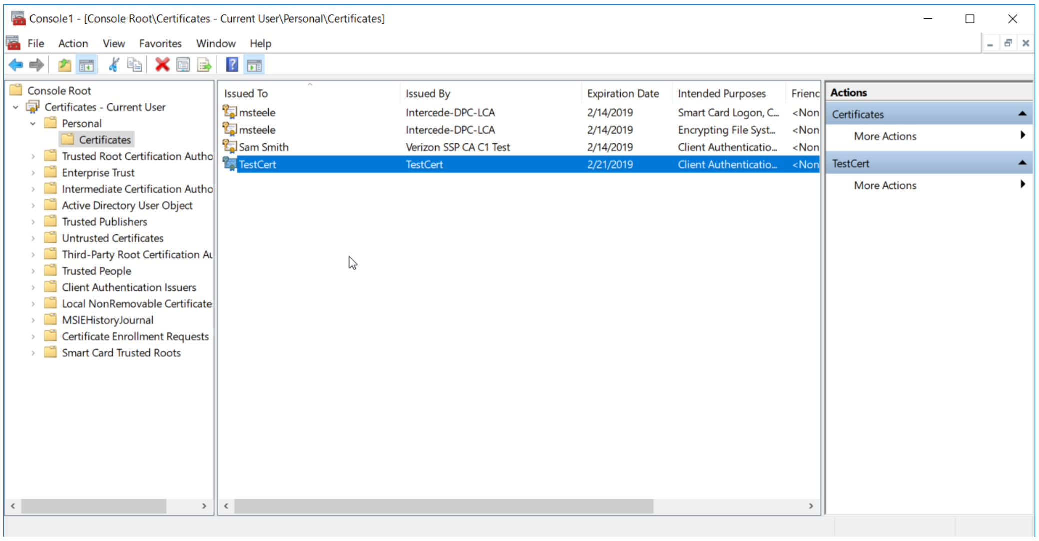


You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Corp...
Authorization Manager	Microsoft Corp...
Certificates	Microsoft Corp...
Component Services	Microsoft Corp...
Computer Managem...	Microsoft Corp...
Device Manager	Microsoft Corp...
Disk Management	Microsoft and ...
Event Viewer	Microsoft Corp...
Folder	Microsoft Corp...
Group Policy Object ...	Microsoft Corp...
IP Security Monitor	Microsoft Corp...
IP Security Policy Ma...	Microsoft Corp...
Link to Web Address	Microsoft Corp...
Local Users and Gro...	Microsoft Corp...
Performance Monitor	Microsoft Corp

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. The newly created certificate should be in the **Certificates – Current User > Personal > Certificates** store.

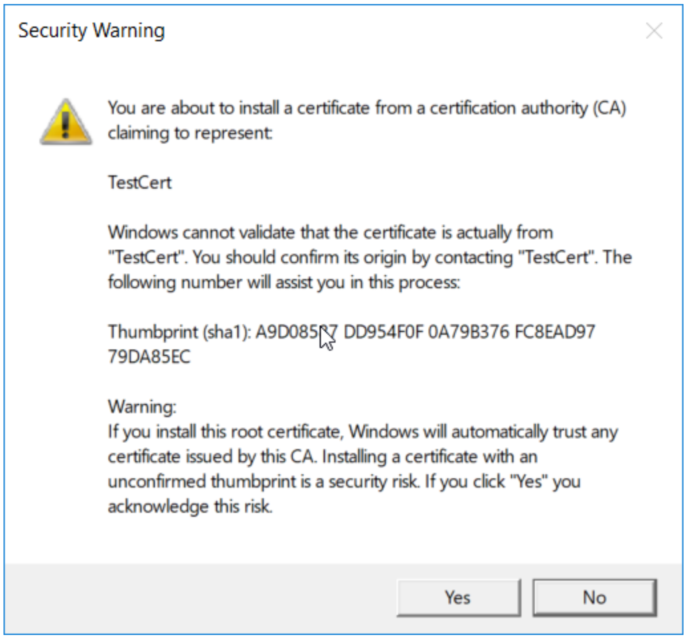

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Client Authentication Issuers
Local NonRemovable Certificate
MSIEHistoryJournal
Certificate Enrollment Requests
Smart Card Trusted Roots
Actions
Certificates
More Actions
TestCert
More Actions

Issued To	Issued By	Expiration Date	Intended Purposes	Frienc
msteele	Intercede-DPC-LCA	2/14/2019	Smart Card Logon, C...	<Non
msteele	Intercede-DPC-LCA	2/14/2019	Encrypting File Syst...	<Non
Sam Smith	Verizon SSP CA C1 Test	2/14/2019	Client Authenticatio...	<Non
TestCert	TestCert	2/21/2019	Client Authenticatio...	<Non

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.



Security Warning

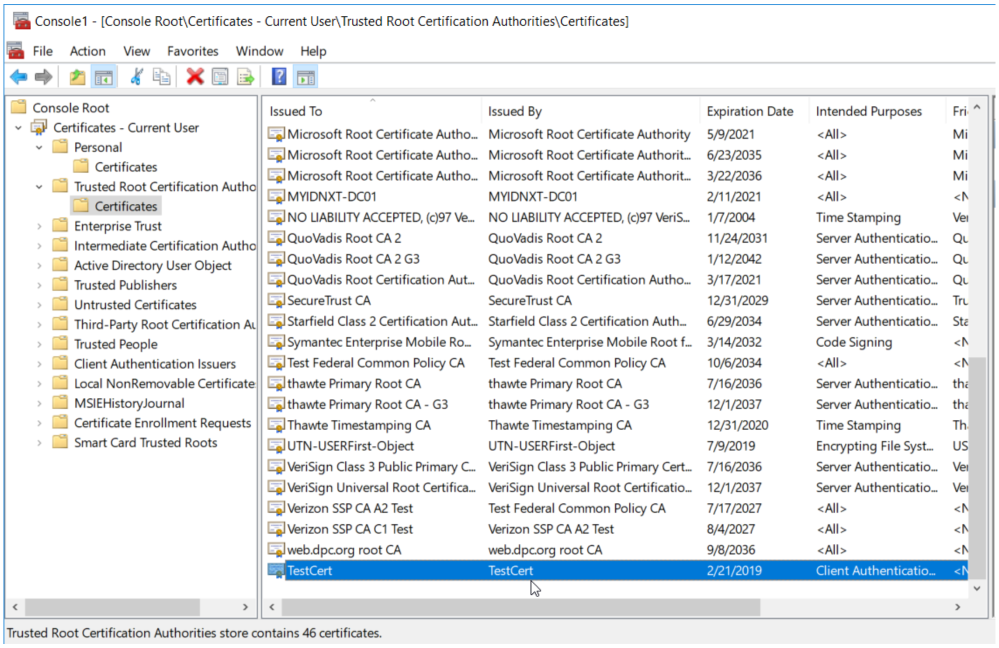
You are about to install a certificate from a certification authority (CA) claiming to represent:

TestCert

Windows cannot validate that the certificate is actually from "TestCert". You should confirm its origin by contacting "TestCert". The following number will assist you in this process:

Thumbprint (sha1): A9D085?7 DD954F0F 0A79B376 FC8EAD97 79DA85EC

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.



Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

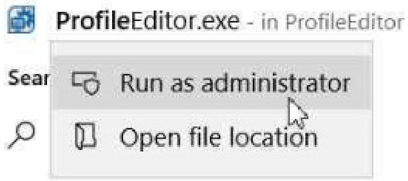
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Autho
Certificates
Enterprise Trust
Intermediate Certification Autho
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Client Authentication Issuers
Local NonRemovable Certificate
MSIEHistoryJournal
Certificate Enrollment Requests
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Fri
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	5/9/2021	<All>	Mi
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	6/23/2035	<All>	Mi
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	3/22/2036	<All>	Mi
MYIDNXT-DC01	MYIDNXT-DC01	2/11/2021	<All>	<N
NO LIABILITY ACCEPTED, (c)97 Ve...	NO LIABILITY ACCEPTED, (c)97 VeriS...	1/7/2004	Time Stamping	Ve
QuoVadis Root CA 2	QuoVadis Root CA 2	11/24/2031	Server Authenticatio...	Qu
QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	1/12/2042	Server Authenticatio...	Qu
QuoVadis Root Certification Aut...	QuoVadis Root Certification Autho...	3/17/2021	Server Authenticatio...	Qu
SecureTrust CA	SecureTrust CA	12/31/2029	Server Authenticatio...	Tru
Starfield Class 2 Certification Aut...	Starfield Class 2 Certification Auth...	6/29/2034	Server Authenticatio...	Sta
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root f...	3/14/2032	Code Signing	<N
Test Federal Common Policy CA	Test Federal Common Policy CA	10/6/2034	<All>	<N
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Server Authenticatio...	tha
thawte Primary Root CA - G3	thawte Primary Root CA - G3	12/1/2037	Server Authenticatio...	tha
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Th
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst...	US
VeriSign Class 3 Public Primary C...	VeriSign Class 3 Public Primary Cert...	7/16/2036	Server Authenticatio...	Ve
VeriSign Universal Root Certifica...	VeriSign Universal Root Certificatio...	12/1/2037	Server Authenticatio...	Ve
Verizon SSP CA A2 Test	Test Federal Common Policy CA	7/17/2027	<All>	<N
Verizon SSP CA C1 Test	Verizon SSP CA A2 Test	8/4/2027	<All>	<N
web.dpc.org root CA	web.dpc.org root CA	9/8/2036	<All>	<N
TestCert	TestCert	2/21/2019	Client Authenticatio...	<N

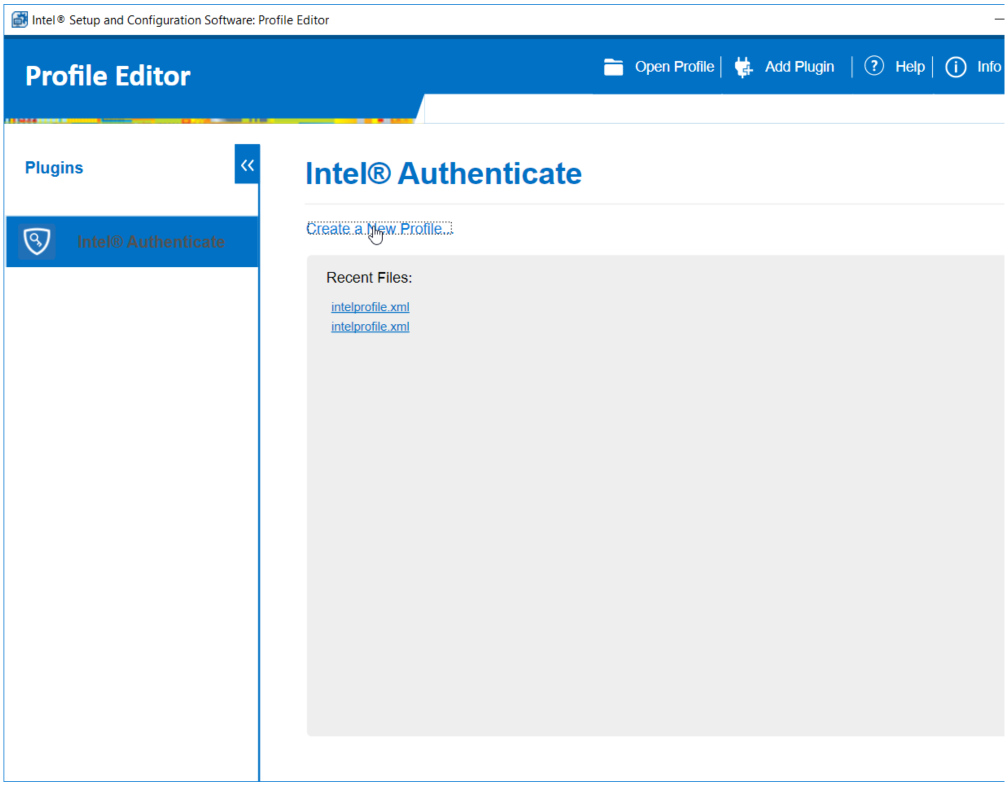
Trusted Root Certification Authorities store contains 46 certificates.

2.2.6.2 Creating a Profile

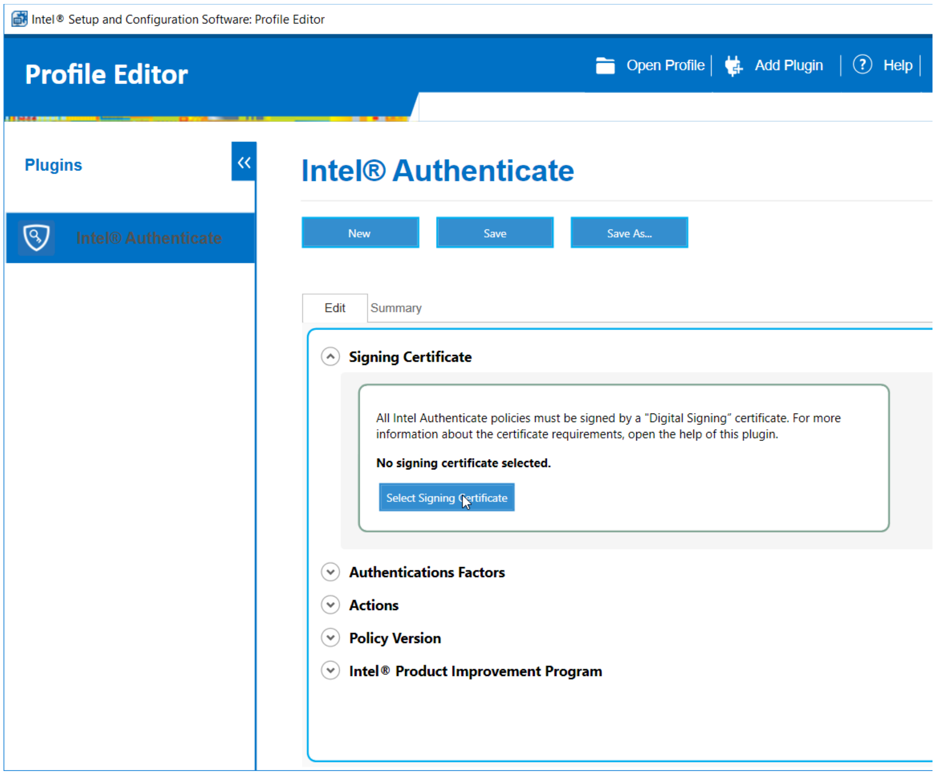
1. Run the **ProfileEditor.exe** file as an administrator.



2. Click **Create a New Profile…**.



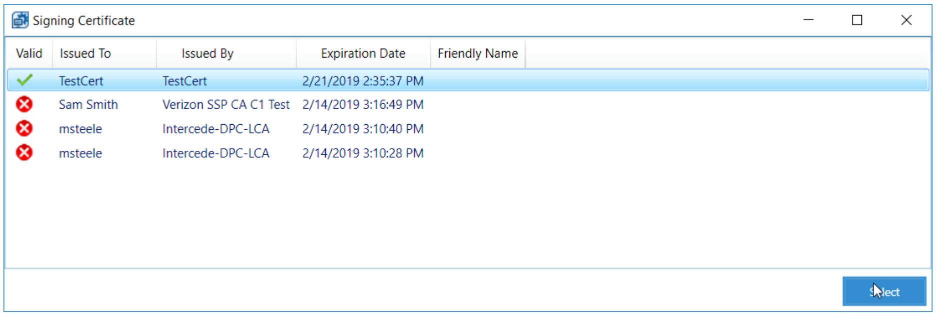
3. Click **Select Signing Certificate**.



All Intel Authenticate policies must be signed by a "Digital Signing" certificate. For more information about the certificate requirements, open the help of this plugin.

No signing certificate selected.

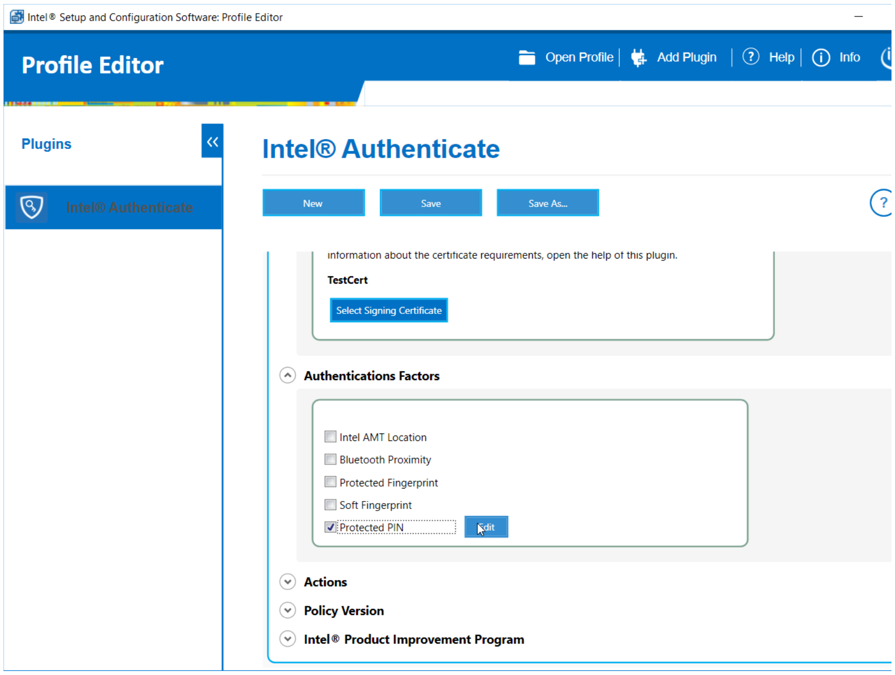
4. Select the newly created certificate and click **Select**.



Valid	Issued To	Issued By	Expiration Date	Friendly Name
✓	TestCert	TestCert	2/21/2019 2:35:37 PM	
☒	Sam Smith	Verizon SSP CA C1 Test	2/14/2019 3:16:49 PM	
☒	msteele	Intercede-DPC-LCA	2/14/2019 3:10:40 PM	
☒	msteele	Intercede-DPC-LCA	2/14/2019 3:10:28 PM	

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

6. Click the **Edit** button.


Intel® Setup and Configuration Software: Profile Editor
Profile Editor
Open Profile
Add Plugin
Help
Info
Plugins
Intel® Authenticate
New
Save
Save As...
Select Signing Certificate
Actions
Policy Version
Intel® Product Improvement Program
Edit

Intel® Authenticate

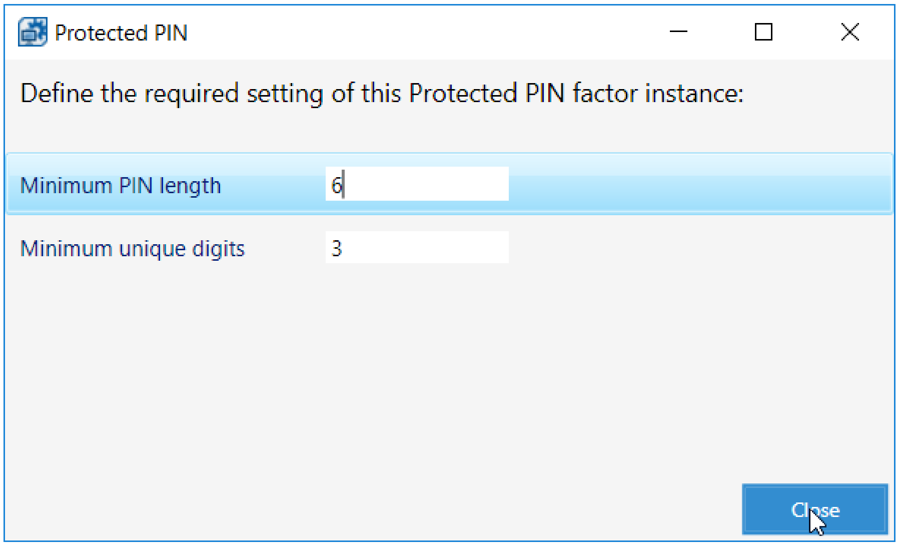
information about the certificate requirements, open the help of this plugin.

TestCert

Authentications Factors

- □ Intel AMT Location
- □ Bluetooth Proximity
- □ Protected Fingerprint
- □ Soft Fingerprint
- ☑ Protected PIN

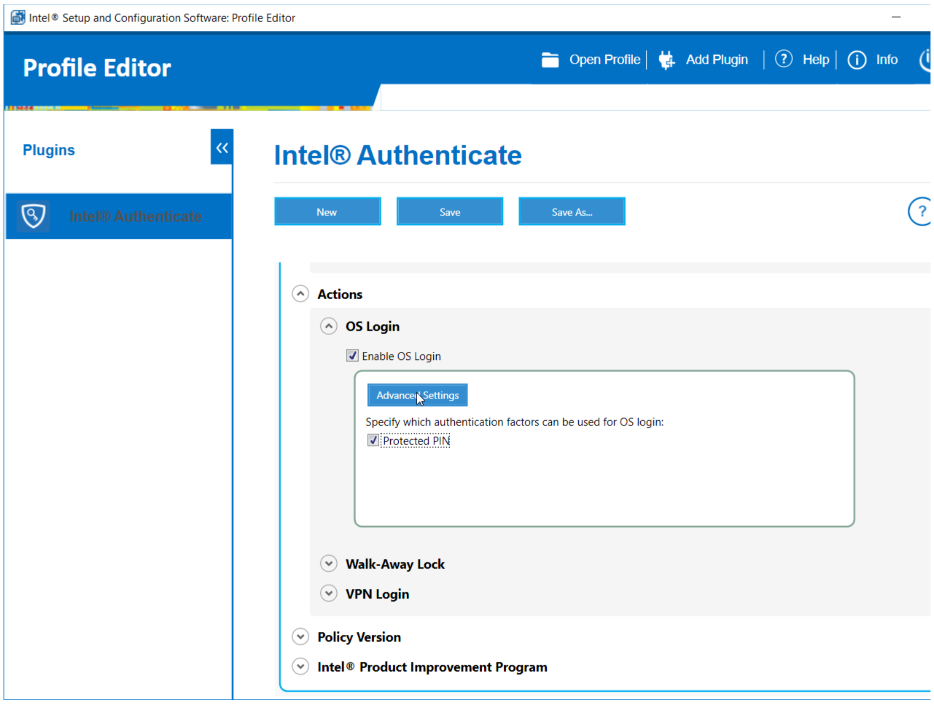
7. Set the PIN length and the minimum number of unique digits.
8. Click **Close**.



Define the required setting of this Protected PIN factor instance:

Minimum PIN length	6
Minimum unique digits	3

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**.



Intel® Authenticate

Actions

OS Login

☑ Enable OS Login

Specify which authentication factors can be used for OS login:

☑ Protected PIN

Walk-Away Lock

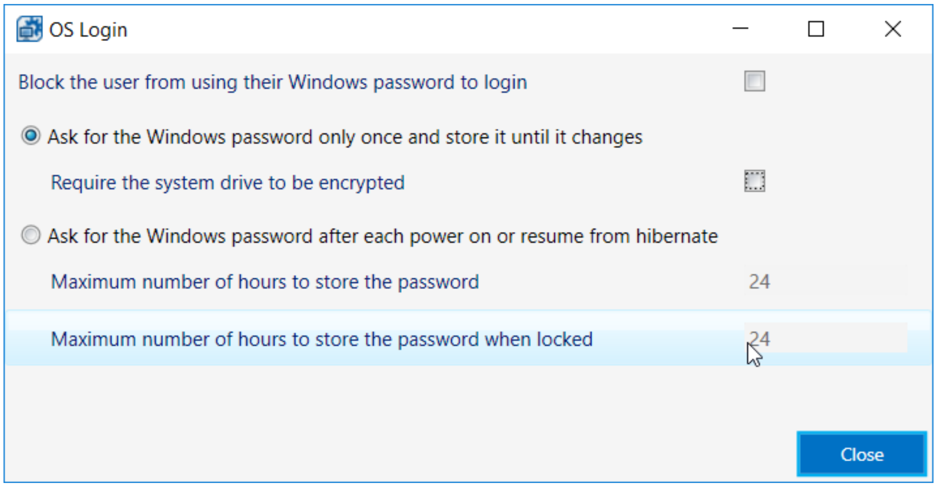
VPN Login

Policy Version

Intel® Product Improvement Program

12. Uncheck the box next to **Require the system drive to be encrypted**.

13. Click **Close**.



Block the user from using their Windows password to login □

● Ask for the Windows password only once and store it until it changes

Require the system drive to be encrypted □

○ Ask for the Windows password after each power on or resume from hibernate

Maximum number of hours to store the password 24

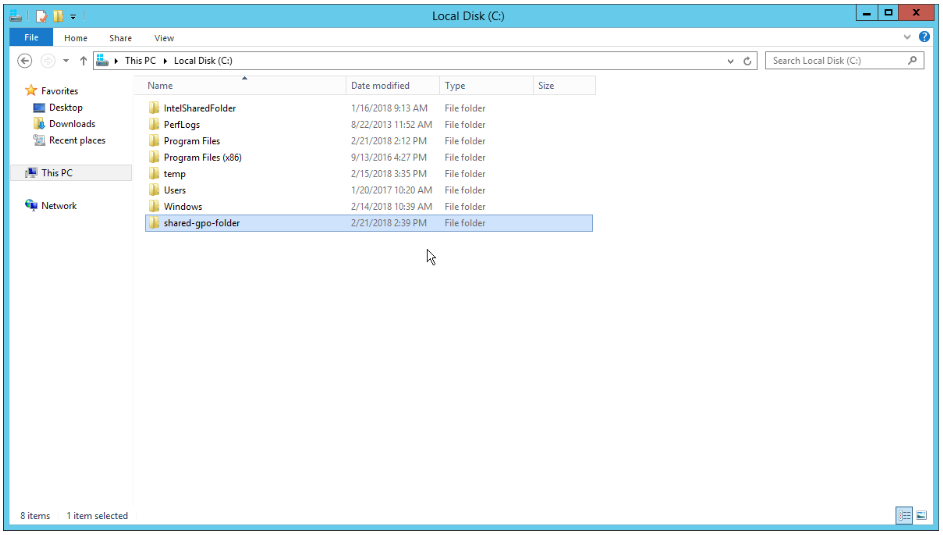
Maximum number of hours to store the password when locked 24

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*.

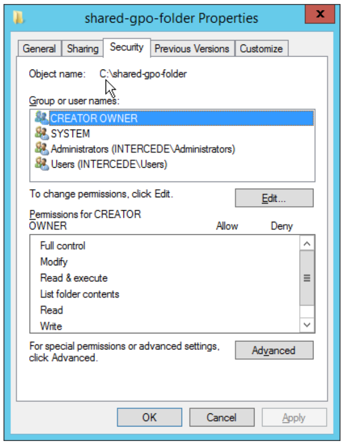


Name	Date modified	Type	Size
IntelSharedFolder	1/16/2018 9:13 AM	File folder	
PerfLogs	8/22/2013 11:52 AM	File folder	
Program Files	2/21/2018 2:12 PM	File folder	
Program Files (x86)	9/13/2016 4:27 PM	File folder	
temp	2/15/2018 3:35 PM	File folder	
Users	1/20/2017 10:20 AM	File folder	
Windows	2/14/2018 10:39 AM	File folder	
shared-gpo-folder	2/21/2018 2:39 PM	File folder	

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

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

5. Click **Edit**.



Object name: C:\shared-gpo-folder

Group or user names:

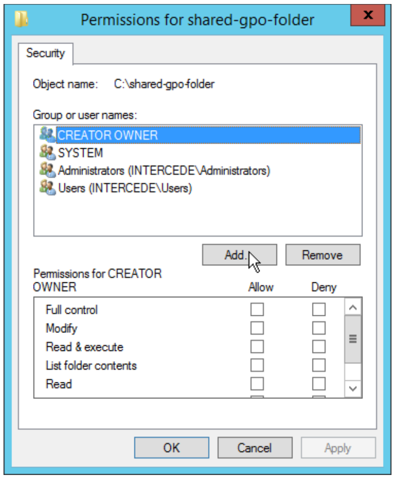
- CREATOR OWNER
- SYSTEM
- Administrators (INTERCEDE\Administrators)
- Users (INTERCEDE\Users)

To change permissions, click Edit.

Permissions for CREATOR OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		

For special permissions or advanced settings, click Advanced.

6. Click **Add**.



Object name: C:\shared-gpo-folder

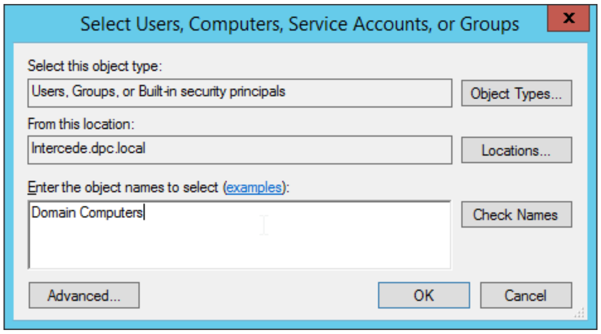
Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (INTERCEDE\Administrators)
- Users (INTERCEDE\Users)

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□

7. Enter **Domain Computers** in the text box.

8. Click **OK**.



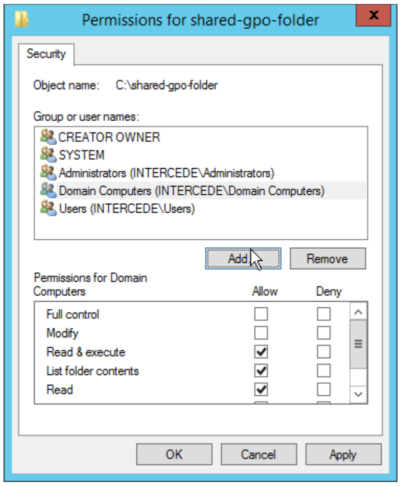
Select this object type: Users, Groups, or Built-in security principals

From this location: Intercede.dpc.local

Enter the object names to select (examples): Domain Computers

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

10. Click **OK.**



Object name: C:\shared-gpo-folder

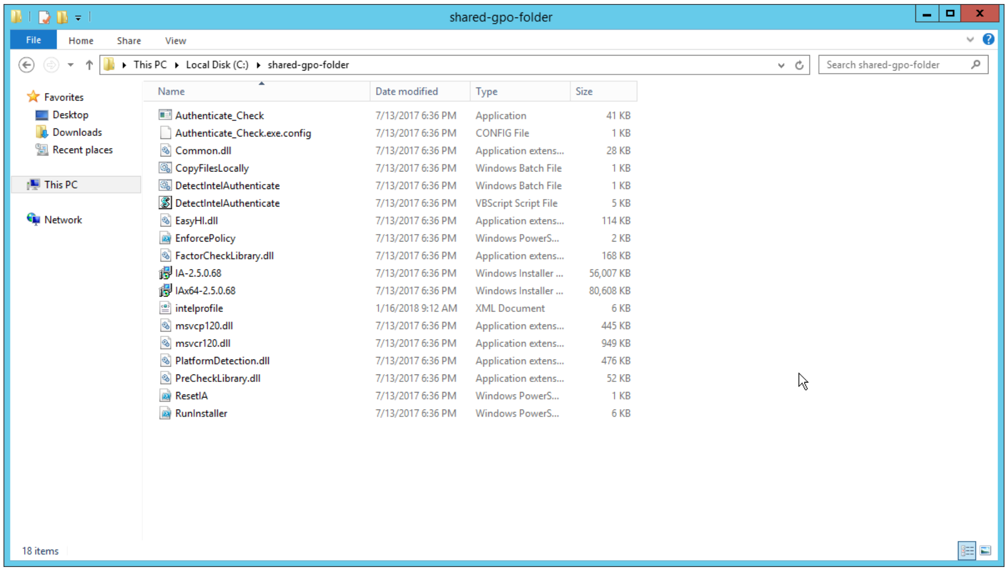
Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (INTERCEDE\Administrators)
- Domain Computers (INTERCEDE\Domain Computers)
- Users (INTERCEDE\Users)

Permissions for Domain Computers	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

11. Click **OK.**

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



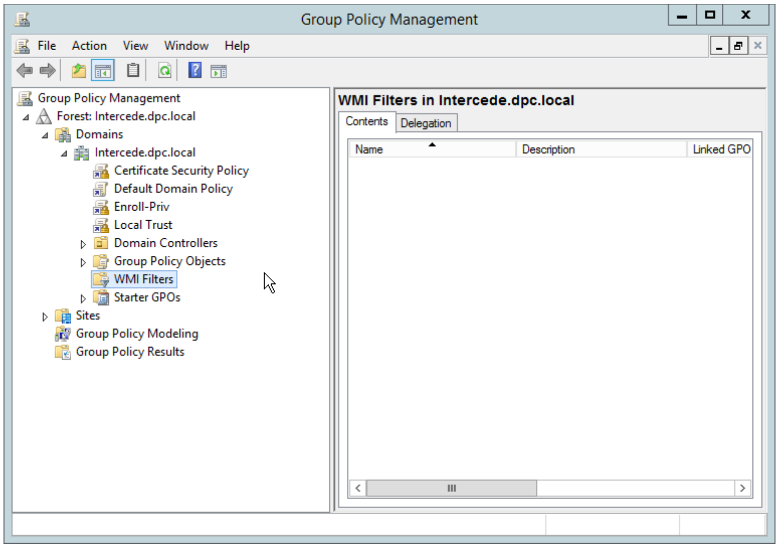
Name	Date modified	Type	Size
Authenticate_Check	7/13/2017 6:36 PM	Application	41 KB
Authenticate_Check.exe.config	7/13/2017 6:36 PM	CONFIG File	1 KB
Common.dll	7/13/2017 6:36 PM	Application extens...	28 KB
CopyFilesLocally	7/13/2017 6:36 PM	Windows Batch File	1 KB
DetectIntelAuthenticate	7/13/2017 6:36 PM	Windows Batch File	1 KB
DetectIntelAuthenticate	7/13/2017 6:36 PM	VBScript Script File	5 KB
EasyHI.dll	7/13/2017 6:36 PM	Application extens...	114 KB
EnforcePolicy	7/13/2017 6:36 PM	Windows PowerS...	2 KB
FactorCheckLibrary.dll	7/13/2017 6:36 PM	Application extens...	168 KB
IA-2.5.0.68	7/13/2017 6:36 PM	Windows Installer ...	56,007 KB
IAx64-2.5.0.68	7/13/2017 6:36 PM	Windows Installer ...	80,608 KB
intelprofile	1/16/2018 9:12 AM	XML Document	6 KB
msvcp120.dll	7/13/2017 6:36 PM	Application extens...	445 KB
msvcr120.dll	7/13/2017 6:36 PM	Application extens...	949 KB
PlatformDetection.dll	7/13/2017 6:36 PM	Application extens...	476 KB
PreCheckLibrary.dll	7/13/2017 6:36 PM	Application extens...	52 KB
ResetIA	7/13/2017 6:36 PM	Windows PowerS...	1 KB
RunInstaller	7/13/2017 6:36 PM	Windows PowerS...	6 KB

18 items

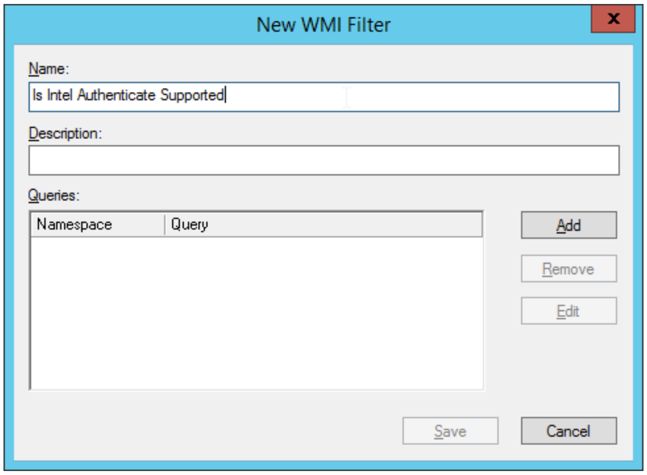
2.2.6.4 Creating WMI Filters for the GPOs

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

2. Right-click **WMI Filters** and select **New….**



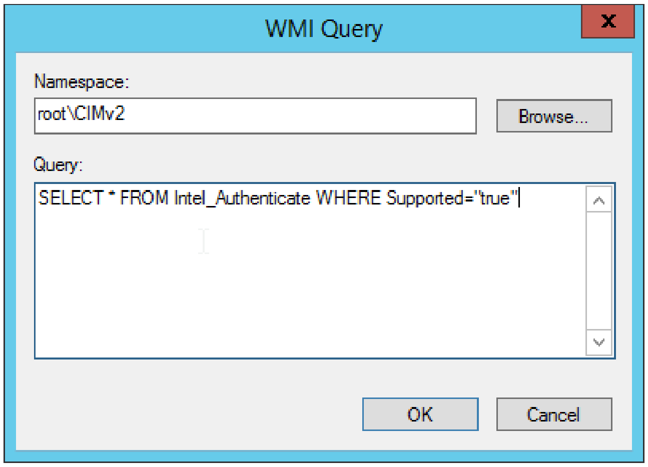
3. Enter a name such as *Is Intel Authenticate Supported* and click **Add**.



Name: Is Intel Authenticate Supported

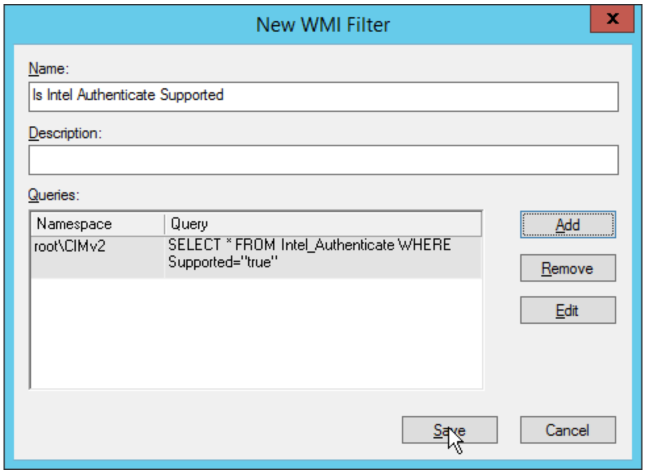
4. In the **Query** field, enter *SELECT * FROM Intel_Authenticate WHERE Supported="true"*.

5. Click **OK**.



SELECT * FROM Intel_Authenticate WHERE Supported="true"

6. Click **Save**.

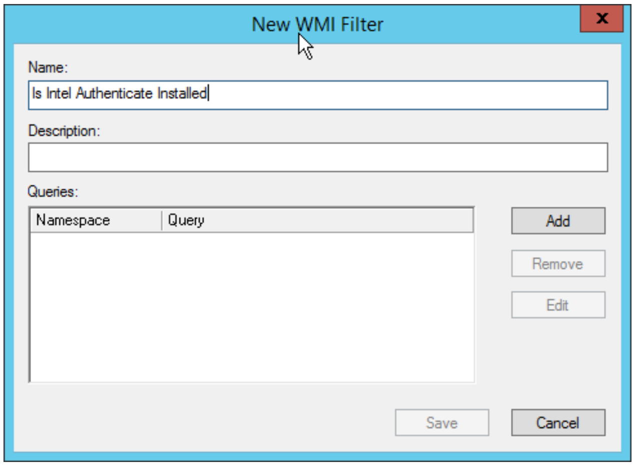


Name: Is Intel Authenticate Supported

Namespace	Query
root\CIMv2	SELECT * FROM Intel_Authenticate WHERE Supported="true"

7. Right-click **WMI Filters** and select **New…**.

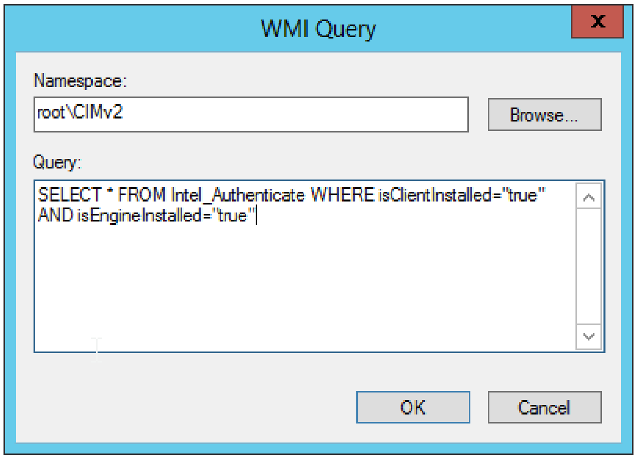
8. Enter a name such as *Is Intel Authenticate Installed* and click **Add**.



Name: Is Intel Authenticate Installed

9. In the **Query** field, enter *SELECT * FROM Intel_Authenticate WHERE isClientInstalled="true" AND isEngineInstalled="true"*.

10. Click **OK**.

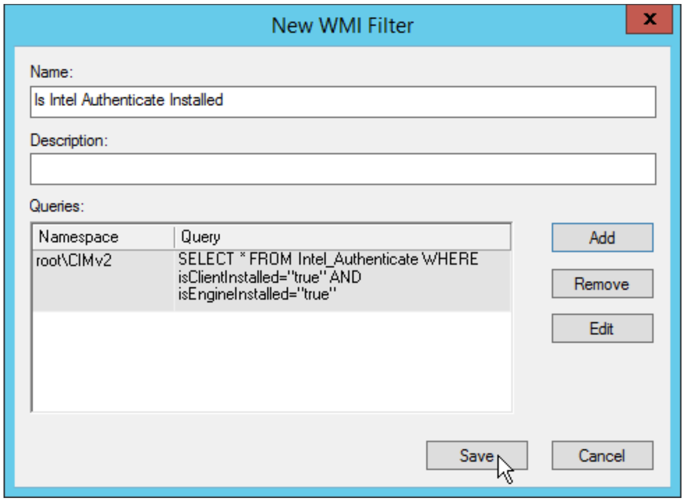


Namespace: root\CIMv2

Query:

```
SELECT * FROM Intel_Authenticate WHERE isClientInstalled="true"
AND isEngineInstalled="true"
```

11. Click **Save**.

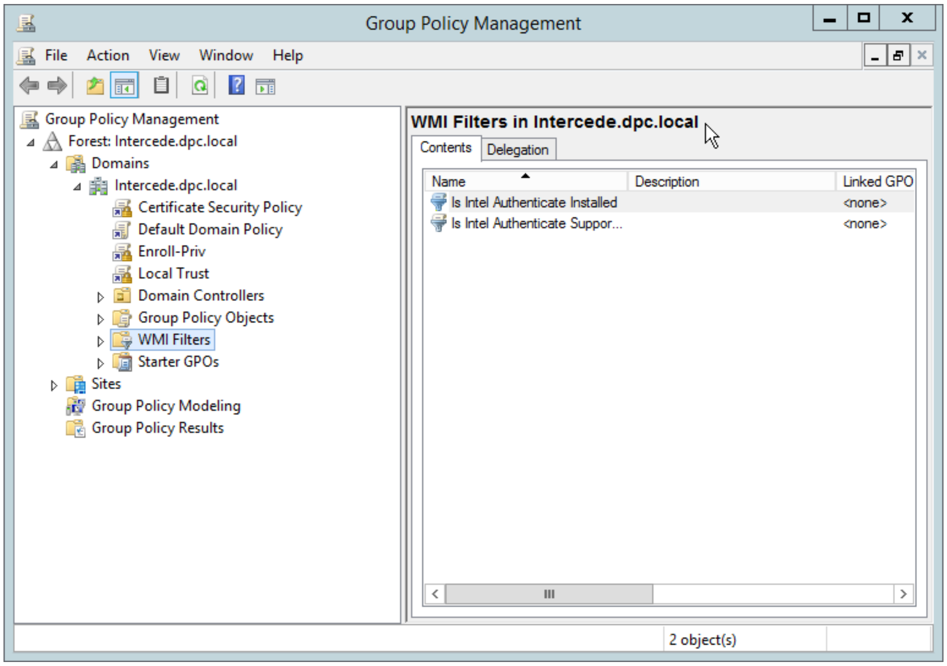


Name: Is Intel Authenticate Installed

Description:

Queries:

Namespace	Query
root\CIMv2	SELECT * FROM Intel_Authenticate WHERE isClientInstalled="true" AND isEngineInstalled="true"



WMI Filters in Intercede.dpc.local

Name	Description	Linked GPO
Is Intel Authenticate Installed		<none>
Is Intel Authenticate Suppor...		<none>

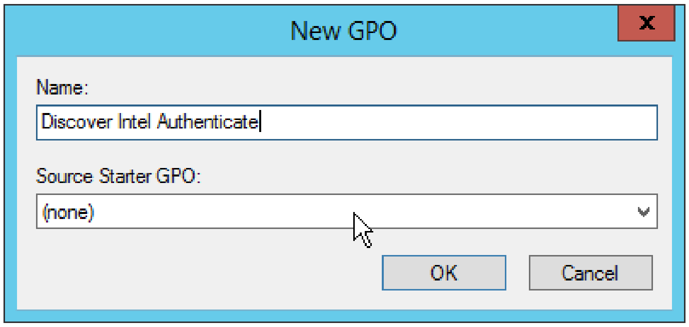
2 object(s)

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.

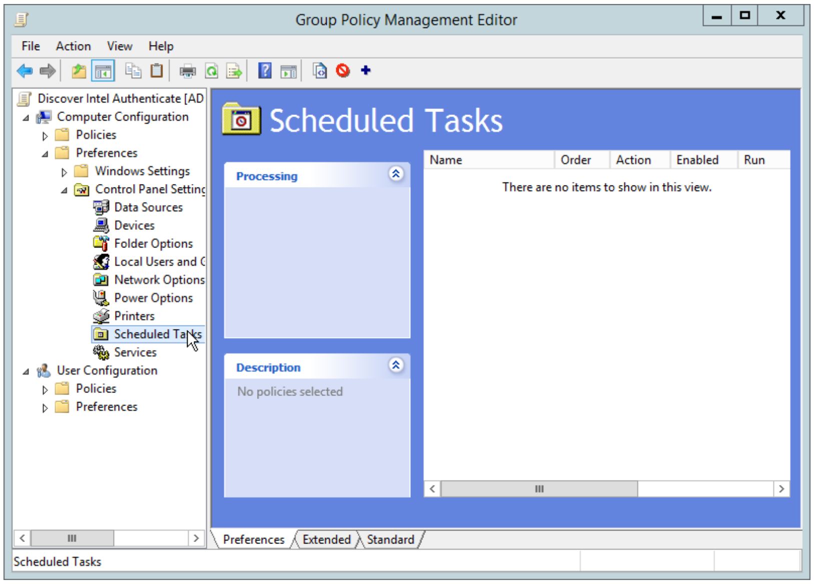


Name: Discover Intel Authenticate

Source Starter GPO: (none)

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)**.

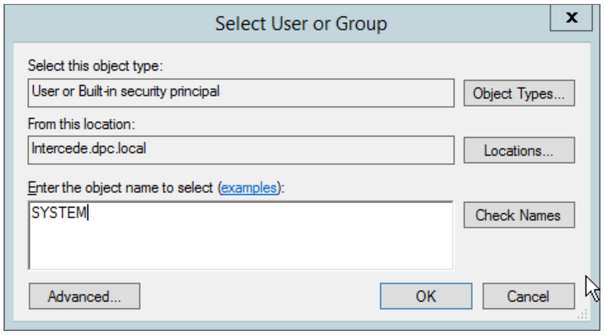


6. Select **Replace** from the drop-down list for **Action**.

7. Enter a descriptive name.

8. Click **Change User or Group**.

9. Enter *SYSTEM* and click **OK**.



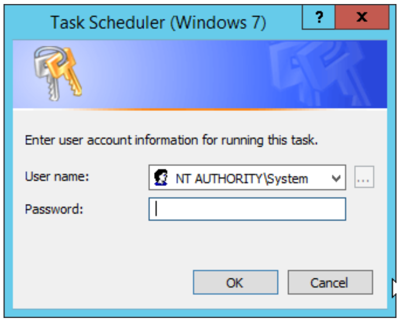
Select User or Group

Select this object type: User or Built-in security principal

From this location: Intercede.dpc.local

Enter the object name to select (examples): SYSTEM

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**.



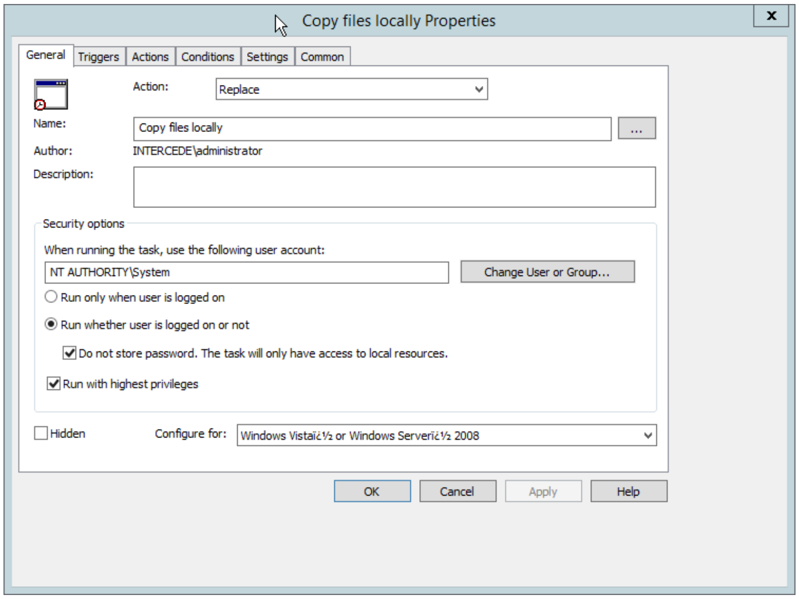
Task Scheduler (Windows 7)

Enter user account information for running this task.

User name: NT AUTHORITY\System

Password:

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**.



Copy files locally Properties

Action: Replace

Name: Copy files locally

Author: INTERCEDE\administrator

Description:

Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources.

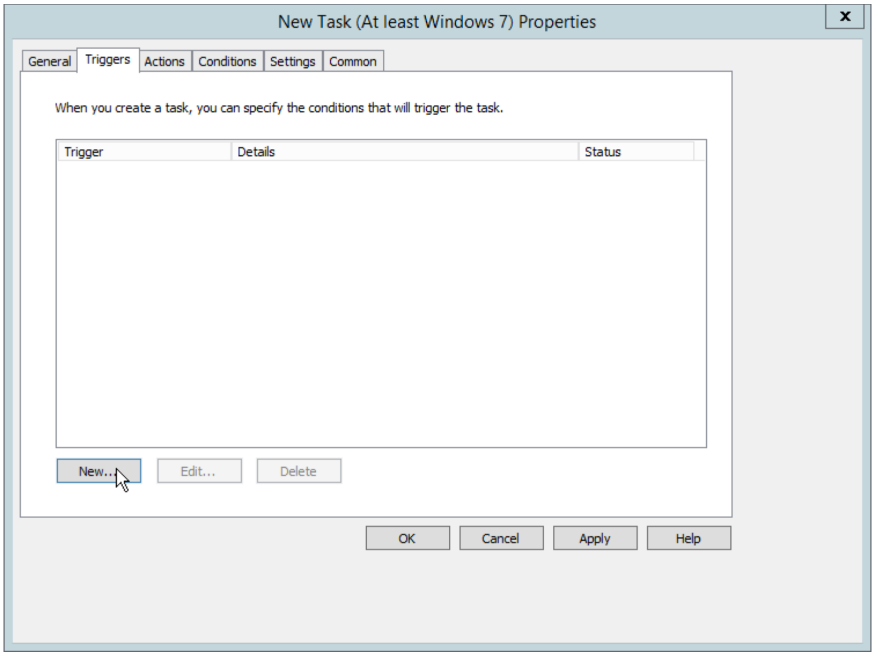
☑ Run with highest privileges

□ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

14. Select the **Triggers** tab.

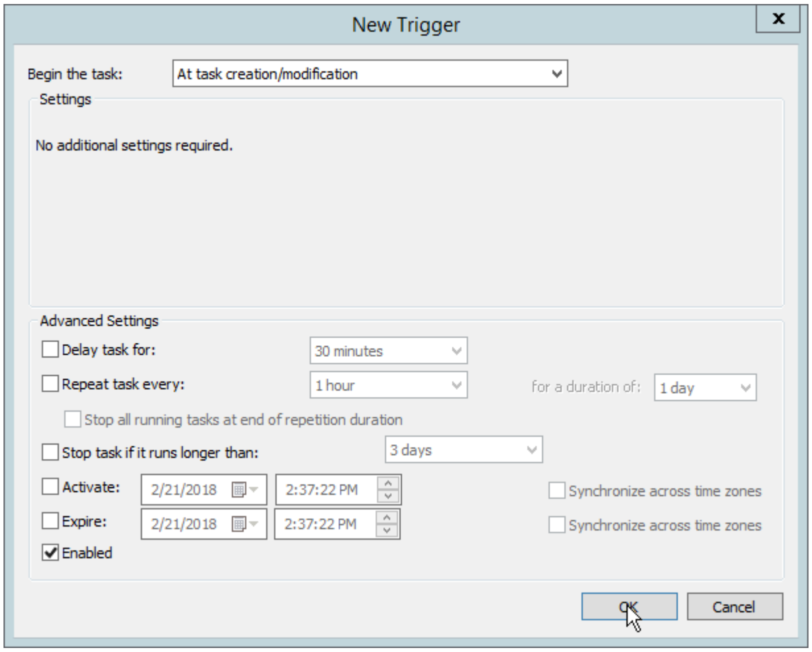
15. Click **New…**.



When you create a task, you can specify the conditions that will trigger the task.

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

17. Click **OK**.



Begin the task: At task creation/modification

Settings

No additional settings required.

Advanced Settings

□ Delay task for: 30 minutes

□ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

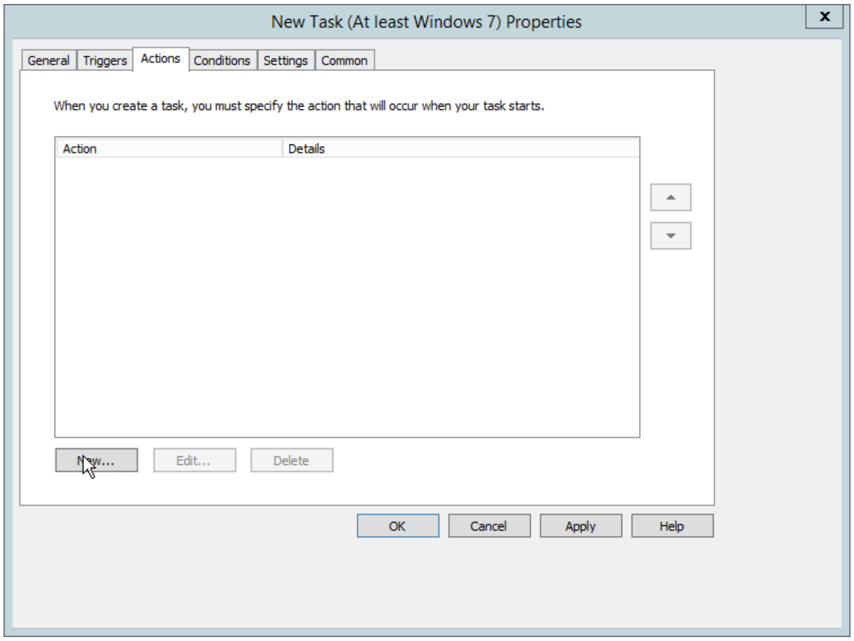
□ Activate: 2/21/2018 2:37:22 PM □ Synchronize across time zones

□ Expire: 2/21/2018 2:37:22 PM □ Synchronize across time zones

☑ Enabled

18. Select the **Actions** tab.

19. Click **New…**.



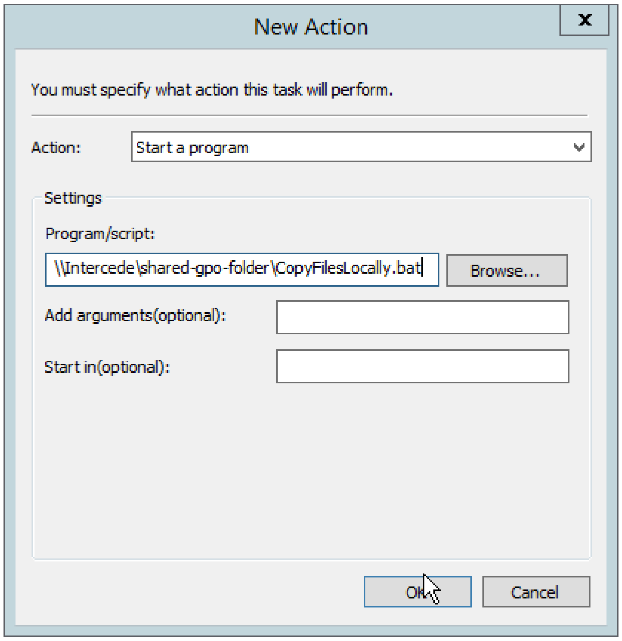
When you create a task, you must specify the action that will occur when your task starts.

Action	Details

20. Select **Start a program**.

21. For **Program/script,** enter the network location of the **CopyFilesLocally.bat** file.

22. Click **OK**.



Action: Start a program

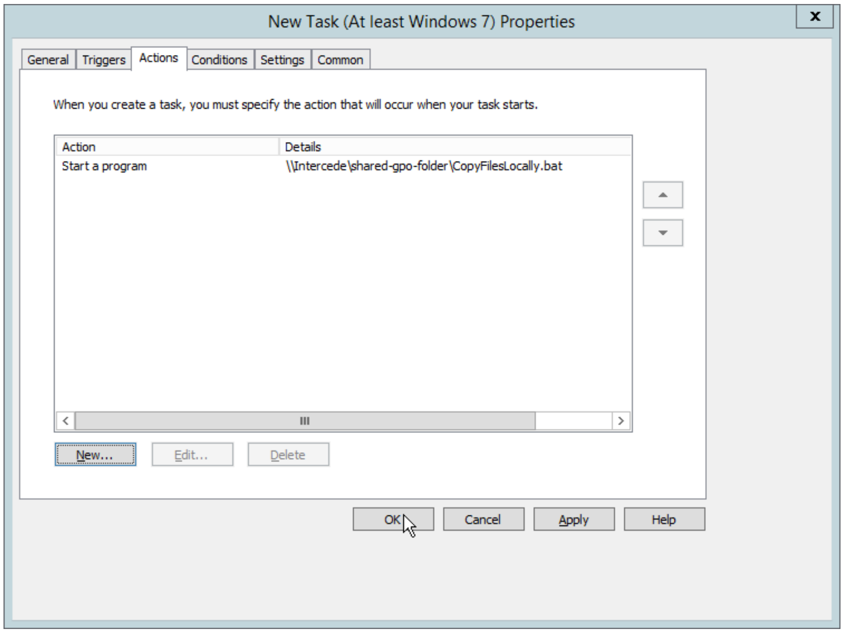
Settings

Program/script: \\Intercede\shared-gpo-folder\CopyFilesLocally.bat

Add arguments(optional):

Start in(optional):

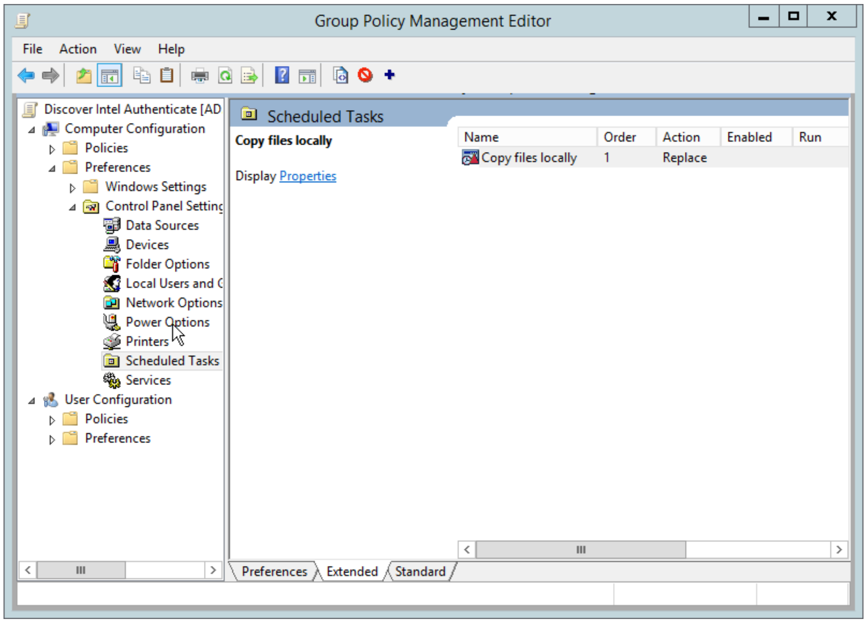
23. Click **OK**.



New Task (At least Windows 7) Properties
General
Triggers
Actions
Conditions
Settings
Common
When you create a task, you must specify the action that will occur when your task starts.
New...
Edit...
Delete
OK
Cancel
Apply
Help

Action	Details
Start a program	\\Intercede\shared-gpo-folder\CopyFilesLocally.bat

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



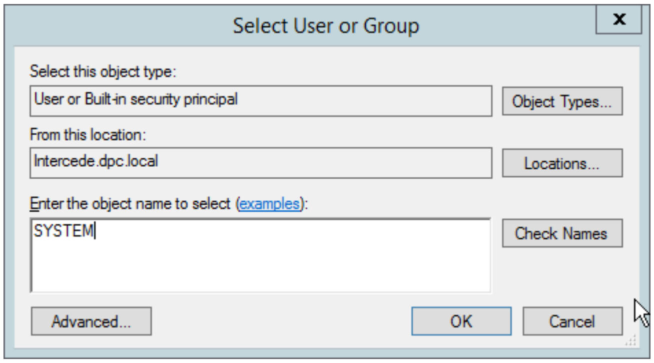
Name	Order	Action	Enabled	Run
Copy files locally	1	Replace		

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**.



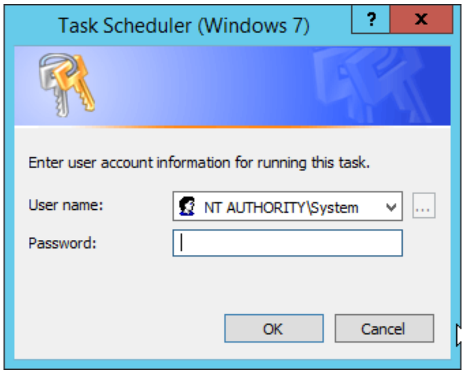
Select this object type:
User or Built-in security principal

From this location:
Intercede.dpc.local

Enter the object name to select (examples):
SYSTEM

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**.



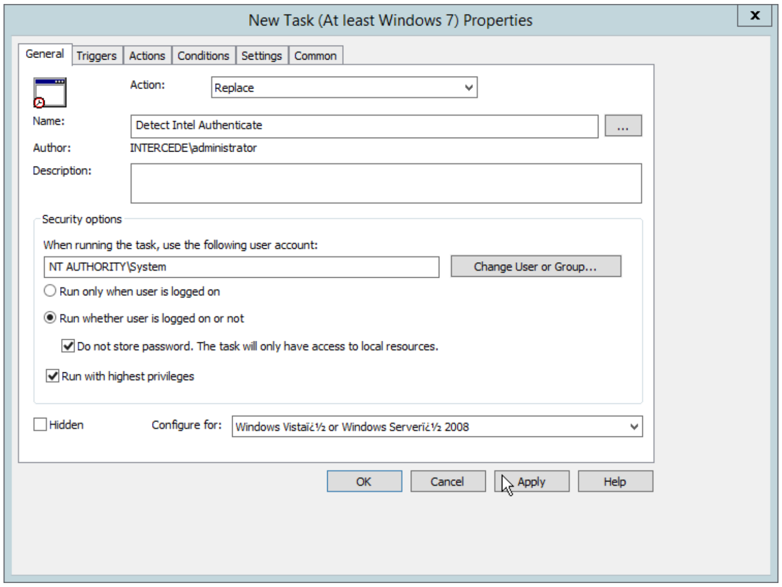
Enter user account information for running this task.

User name: NT AUTHORITY\System

Password:

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**.



Action: Replace

Name: Detect Intel Authenticate

Author: INTERCEDE\administrator

Description:

Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources.

☑ Run with highest privileges

□ Hidden

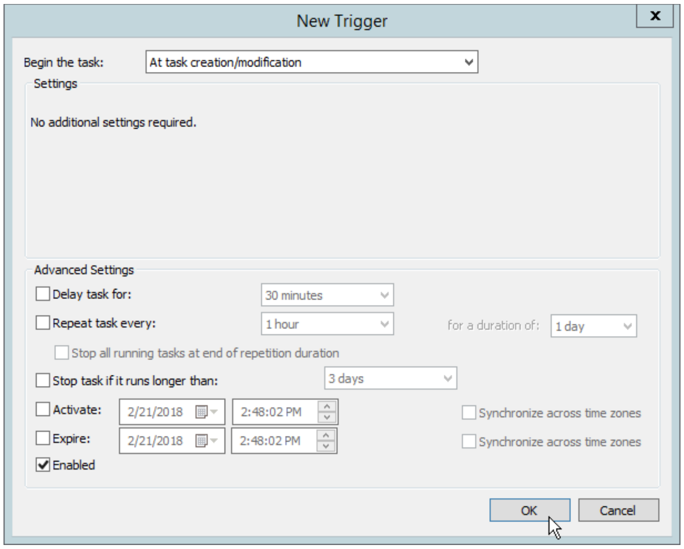
Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

33. Select the **Triggers** tab.

34. Click **New…**.

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

36. Click **OK**.



New Trigger

Begin the task: At task creation/modification

Settings

No additional settings required.

Advanced Settings

☐ Delay task for: 30 minutes

☐ Repeat task every: 1 hour for a duration of: 1 day

☐ Stop all running tasks at end of repetition duration

☐ Stop task if it runs longer than: 3 days

☐ Activate: 2/21/2018 2:48:02 PM ☐ Synchronize across time zones

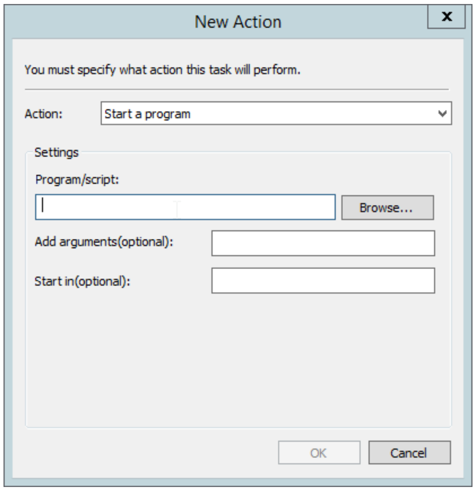
☐ Expire: 2/21/2018 2:48:02 PM ☐ Synchronize across time zones

☑ Enabled

37. Select the **Actions** tab.

38. Click **New…**.

39. Select **Start a program**.



New Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script:

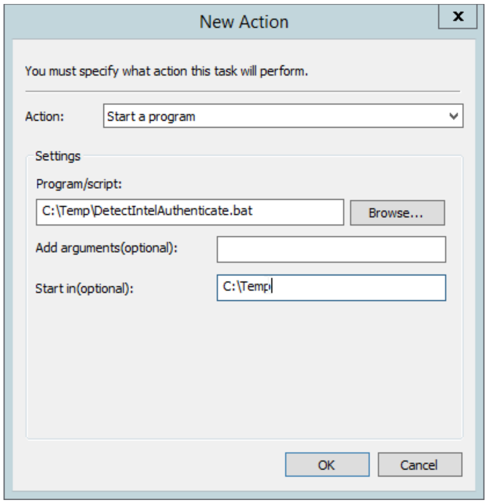
Add arguments(optional):

Start in(optional):

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

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

42. Click **OK**.



Action: Start a program

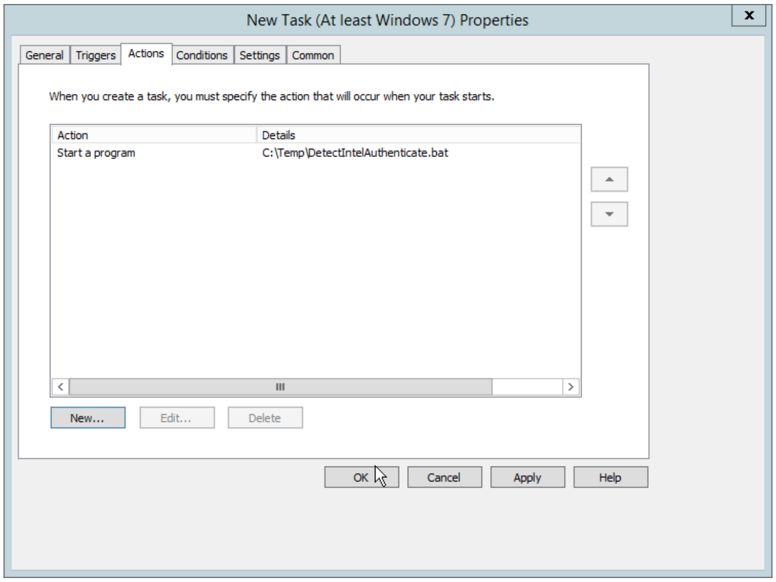
Program/script: C:\Temp\DetectIntelAuthenticate.bat

Add arguments(optional):

Start in(optional): C:\Temp

930

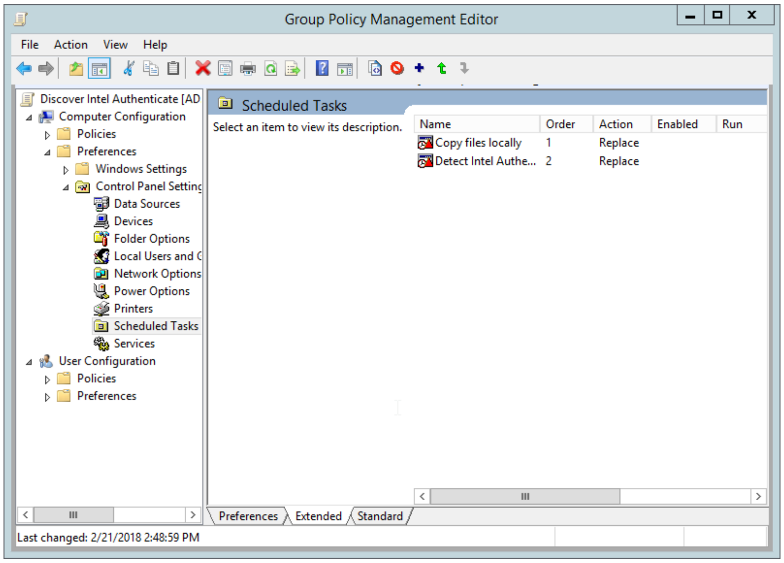
931 43. Click **OK**.



When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Temp\DetectIntelAuthenticate.bat

932

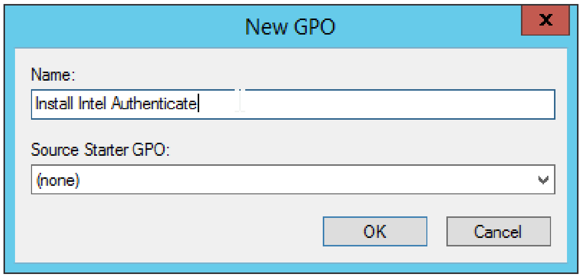


Name	Order	Action	Enabled	Run
Copy files locally	1	Replace		
Detect Intel Authe...	2	Replace		

Last changed: 2/21/2018 2:48:59 PM

2.2.6.6 Creating a GPO to Install Intel Authenticate

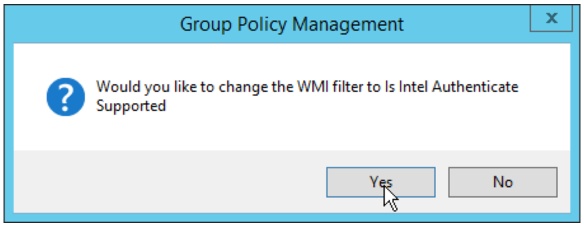
1. Open **Group Policy Management**.
2. In the Group Policy Management tree, right-click the domain and select **Create a GPO in the domain and Link it here**.
3. Enter a **name** for this GPO.
4. Click **OK**.



Name: Install Intel Authenticate

Source Starter GPO: (none)

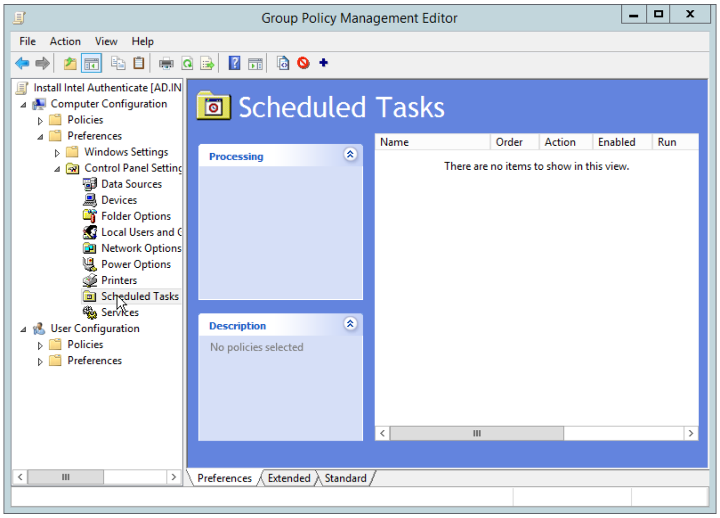
5. Select the GPO you just created and select **Is Intel Authenticate Supported** in the **WMI Filtering** section.
6. Click **Yes**.



Group Policy Management

Would you like to change the WMI filter to Is Intel Authenticate Supported

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



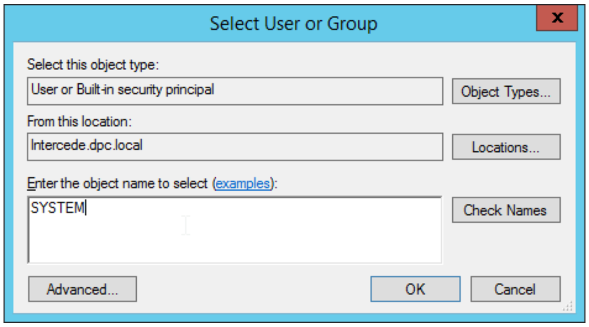
8. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.

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**.



Select User or Group

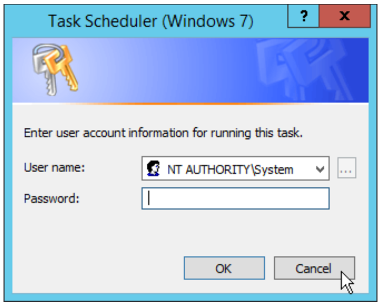
Select this object type:
User or Built-in security principal

From this location:
Intercede.dpc.local

Enter the object name to select (examples):
SYSTEM

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**.



Task Scheduler (Windows 7)

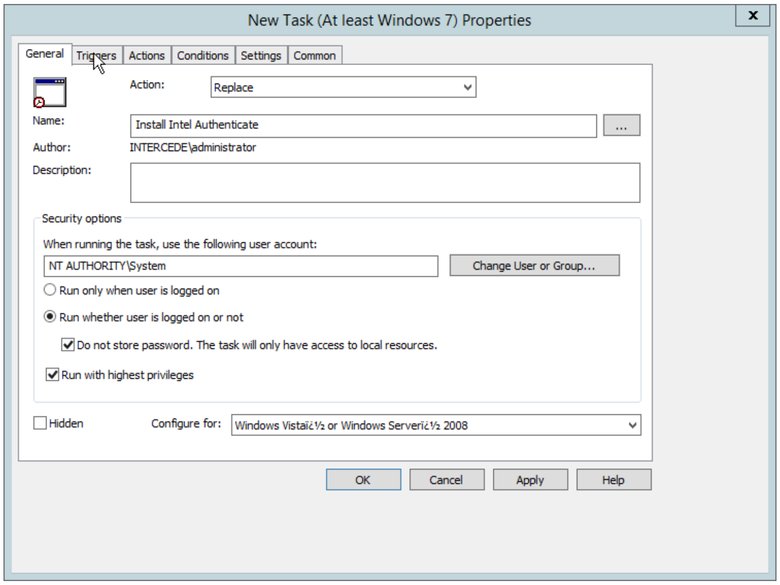
Enter user account information for running this task.

User name: NT AUTHORITY\System

Password:

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**.



New Task (At least Windows 7) Properties

Action: Replace

Name: Install Intel Authenticate

Author: INTERCEDE\administrator

Description:

Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

17. Select the **Triggers** tab.

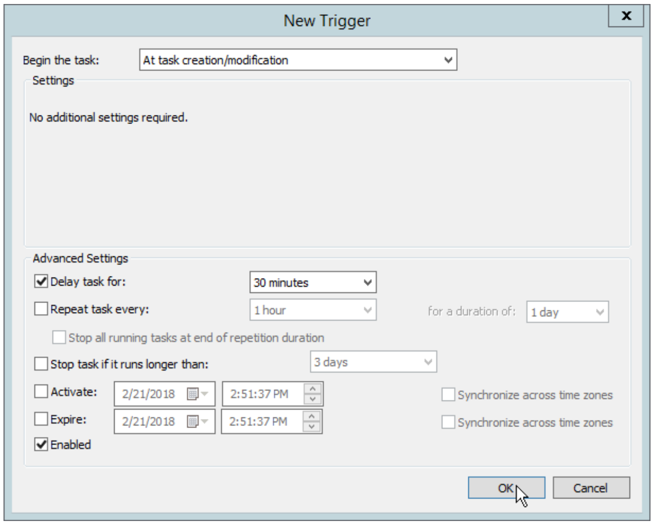
18. Click **New…**.

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**.



New Trigger

Begin the task: At task creation/modification

Settings

No additional settings required.

Advanced Settings

☑ Delay task for: 30 minutes

□ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

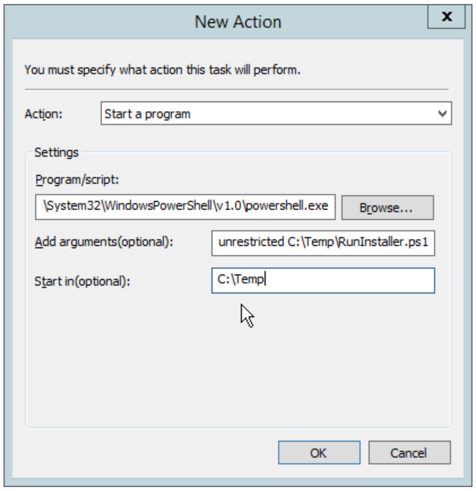
□ Stop task if it runs longer than: 3 days

□ Activate: 2/21/2018 2:51:37 PM □ Synchronize across time zones

□ Expire: 2/21/2018 2:51:37 PM □ Synchronize across time zones

☑ Enabled

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**.



New Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: \System32\WindowsPowerShell\v1.0\powershell.exe

Add arguments(optional): unrestricted C:\Temp\RunInstaller.ps1

Start in(optional): C:\Temp

30. Click **OK**.

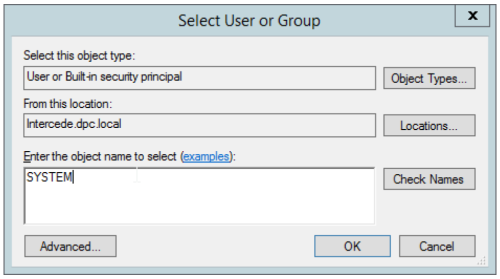
31. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.

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**.



Select User or Group

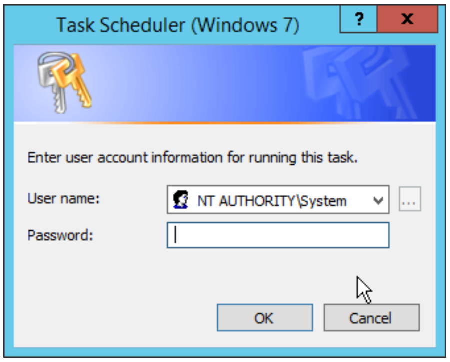
Select this object type: User or Built-in security principal

From this location: Intercede.dpc.local

Enter the object name to select (examples): SYSTEM

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**.



Task Scheduler (Windows 7)

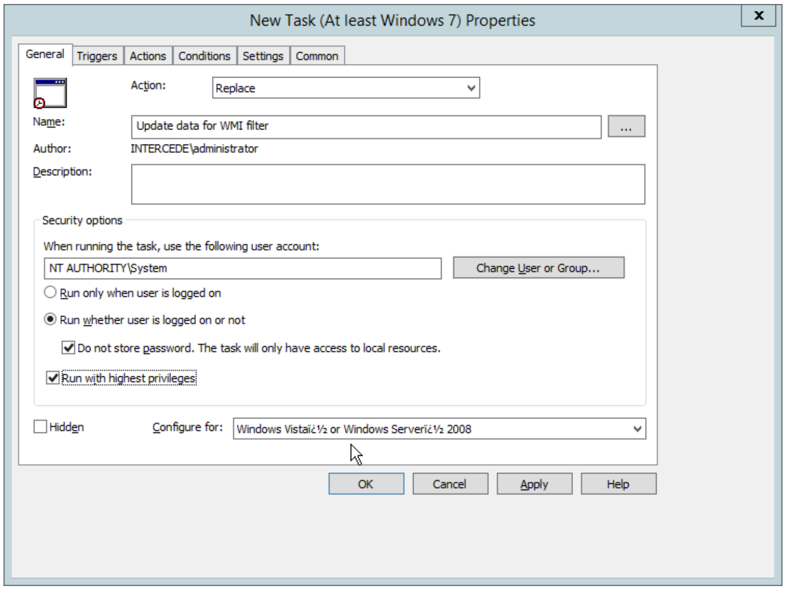
Enter user account information for running this task.

User name: NT AUTHORITY\System

Password:

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**.


New Task (At least Windows 7) Properties

General | Triggers | Actions | Conditions | Settings | Common

Action: Replace

Name: Update data for WMI filter

Author: INTERCEDE\administrator

Description:

Security options

When running the task, use the following user account:

NT AUTHORITY\System

Change User or Group...

○ Run only when user is logged on

● Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources.

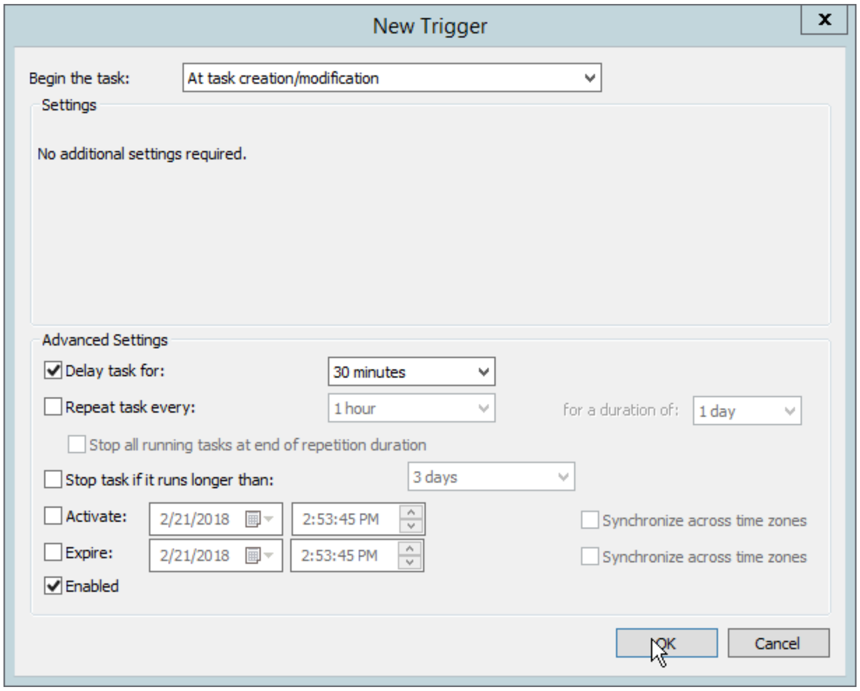
☑ Run with highest privileges

□ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

OK | Cancel | Apply | Help

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**.



Begin the task: At task creation/modification

Settings

No additional settings required.

Advanced Settings

☑ Delay task for: 30 minutes

□ Repeat task every: 1 hour   for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

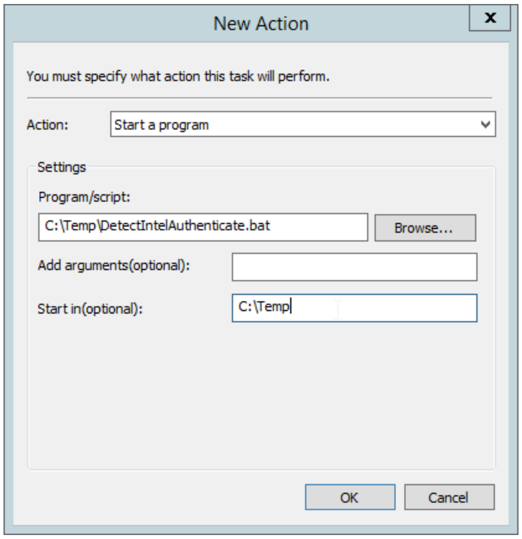
□ Stop task if it runs longer than: 3 days

□ Activate: 2/21/2018 2:53:45 PM □ Synchronize across time zones

□ Expire: 2/21/2018 2:53:45 PM □ Synchronize across time zones

☑ Enabled

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**.



New Action

You must specify what action this task will perform.

Action: Start a program

Settings

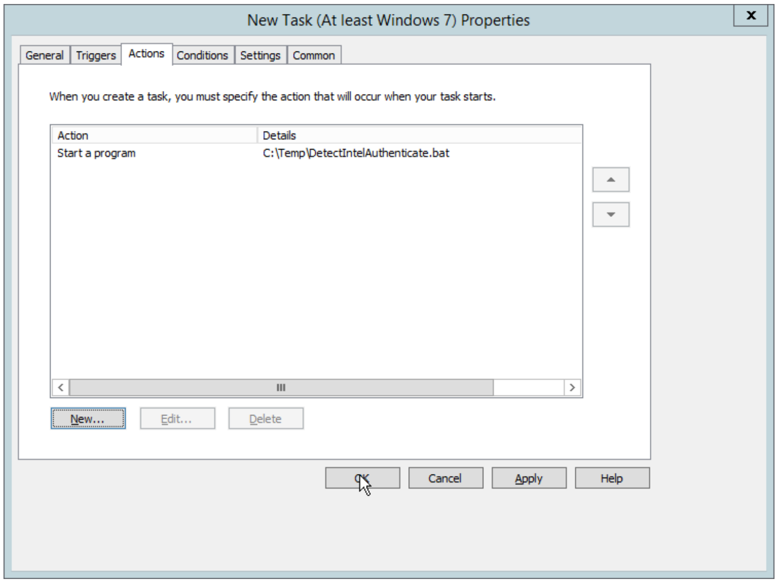
Program/script: C:\Temp\DetectIntelAuthenticate.bat

Add arguments(optional):

Start in(optional): C:\Temp

1002

1003 52. Click **OK**.

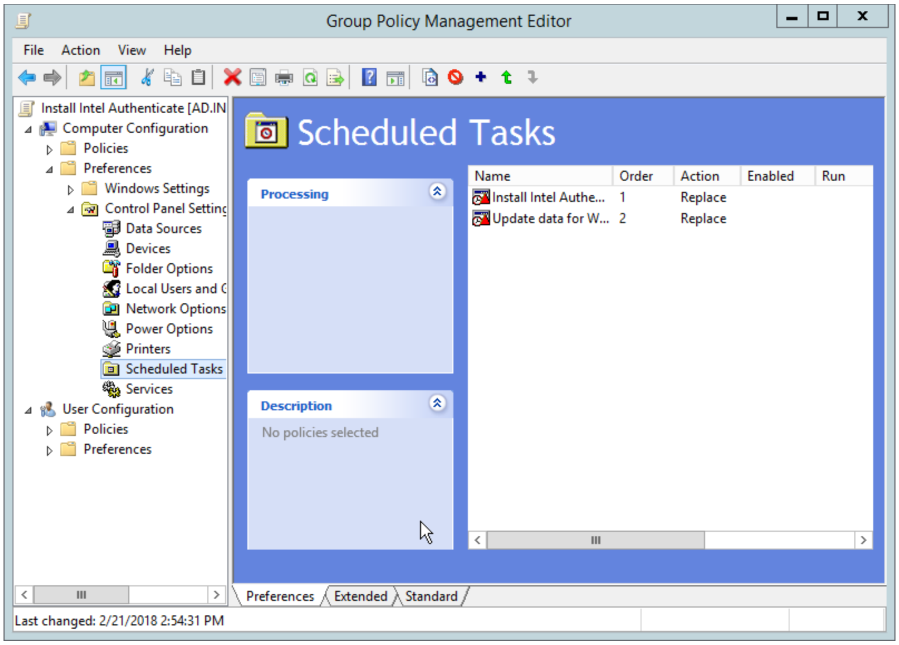


New Task (At least Windows 7) Properties

When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Temp\DetectIntelAuthenticate.bat

1004

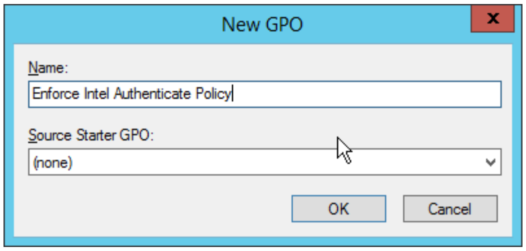


Name	Order	Action	Enabled	Run
Install Intel Authe...	1	Replace		
Update data for W...	2	Replace		

Last changed: 2/21/2018 2:54:31 PM

2.2.6.7 Creating a GPO to Enforce the Policy

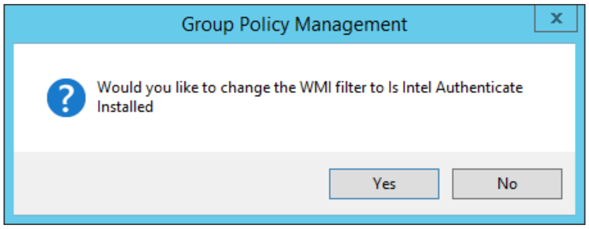
1. Open **Group Policy Management**.
2. In the Group Policy Management tree, right-click the domain and select **Create a GPO in the domain and Link it here**.
3. Enter a name for this GPO
4. Click **OK**.



Name: Enforce Intel Authenticate Policy

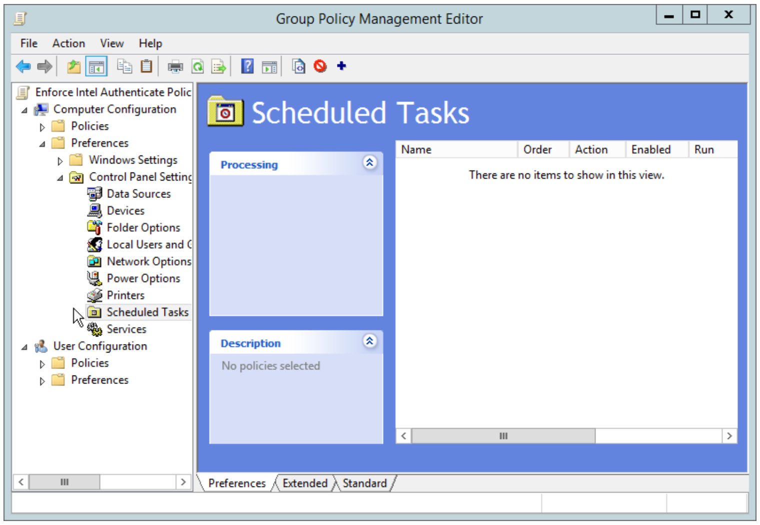
Source Starter GPO: (none)

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



Would you like to change the WMI filter to Is Intel Authenticate Installed

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



There are no items to show in this view.

No policies selected

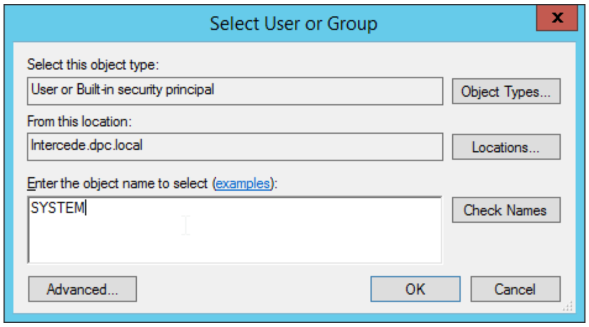
8. Right-click **Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks** and select **New > Scheduled Task (At least Windows 7)**.

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**.



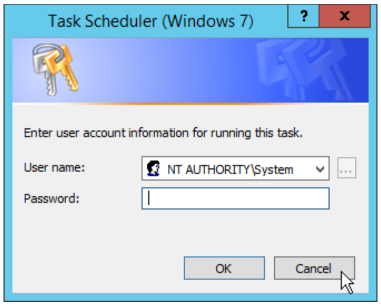
Select this object type:
User or Built-in security principal

From this location:
Intercede.dpc.local

Enter the object name to select (examples):
SYSTEM

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**.



Task Scheduler (Windows 7)

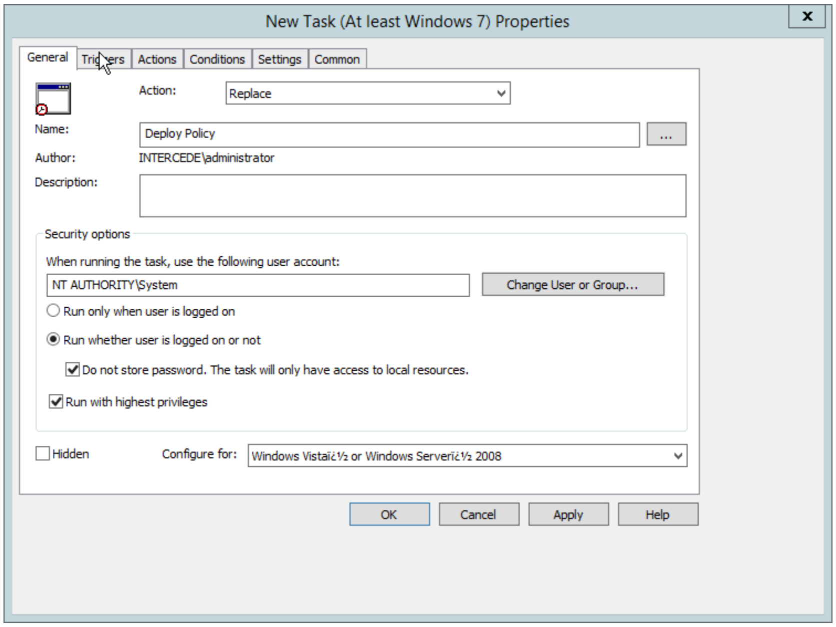
Enter user account information for running this task.

User name: NT AUTHORITY\System

Password:

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**.



New Task (At least Windows 7) Properties

Action: Replace

Name: Deploy Policy

Author: INTERCEDE\administrator

Description:

Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources.

☑ Run with highest privileges

☐ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

17. Select the **Triggers** tab.

18. Click **New…**.

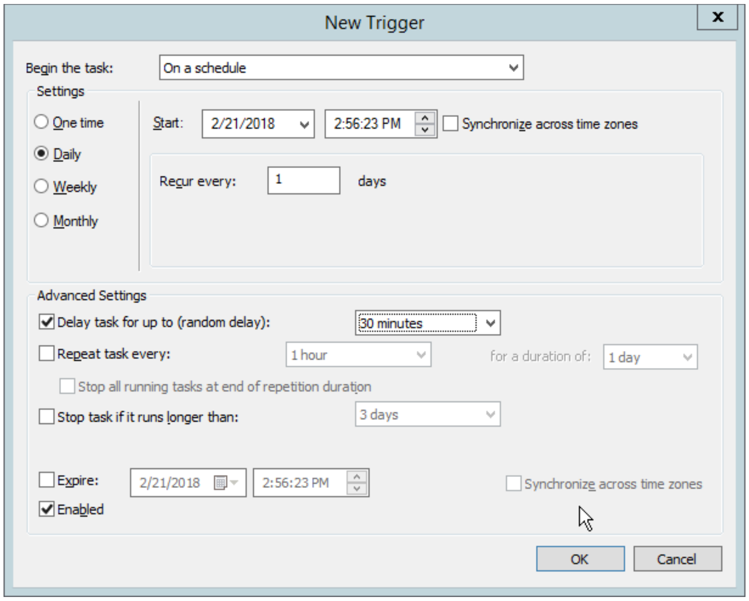
19. Select **On a schedule** for **Begin the task**.

20. Select **Daily**.

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

22. Select **30 minutes**.

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



New Trigger

Begin the task: On a schedule

Settings

○ One time

● Daily

○ Weekly

○ Monthly

Start: 2/21/2018 2:56:23 PM □ Synchronize across time zones

Recur every: 1 days

Advanced Settings

☑ Delay task for up to (random delay): 30 minutes

□ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

□ Expire: 2/21/2018 2:56:23 PM □ Synchronize across time zones

☑ Enabled

24. Select the **Actions** tab.

25. Click **New…**.

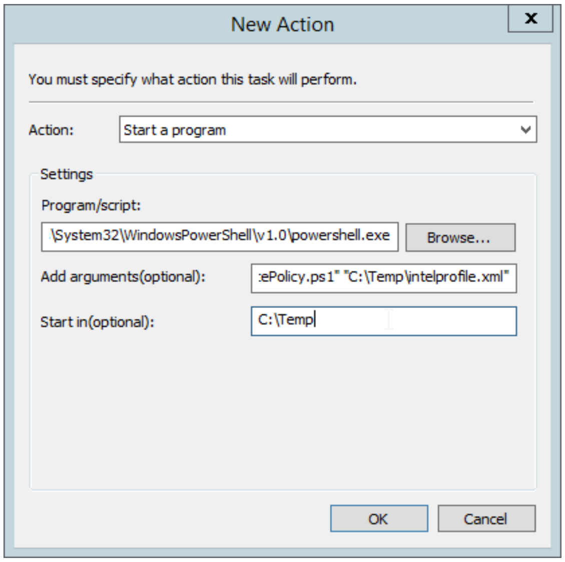
26. Select **Start a program**.

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**.



New Action

You must specify what action this task will perform.

Action: Start a program

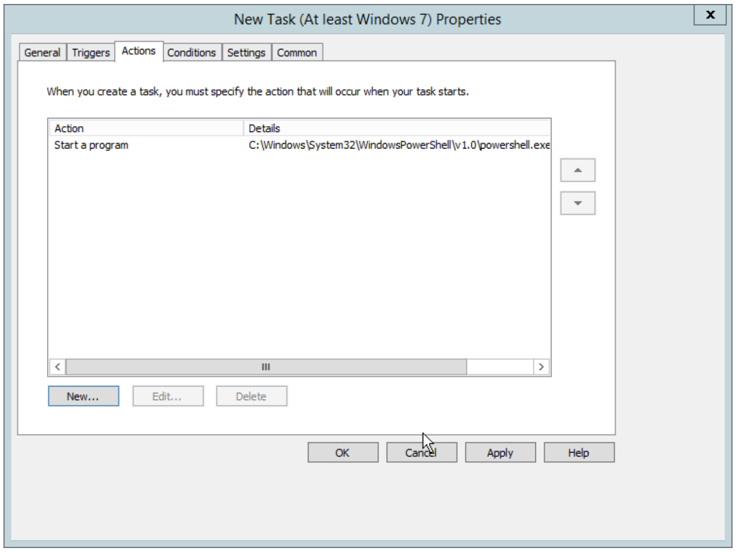
Settings

Program/script: \System32\WindowsPowerShell\v1.0\powershell.exe

Add arguments(optional): :ePolicy.ps1" "C:\Temp\intelprofile.xml"

Start in(optional): C:\Temp

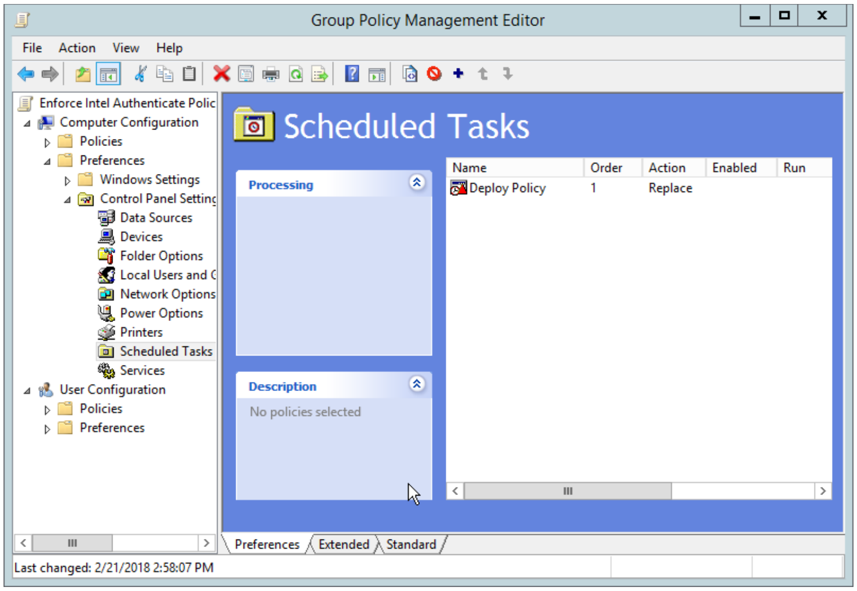
31. Click **OK**.



New Task (At least Windows 7) Properties

When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe



Name	Order	Action	Enabled	Run
Deploy Policy	1	Replace		

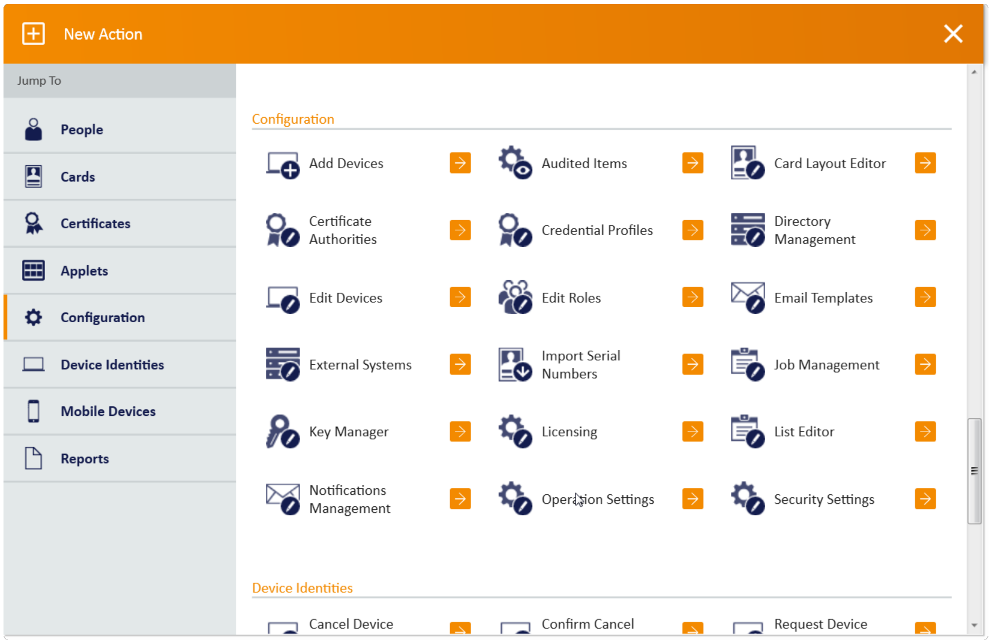
Last changed: 2/21/2018 2:58:07 PM

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**.

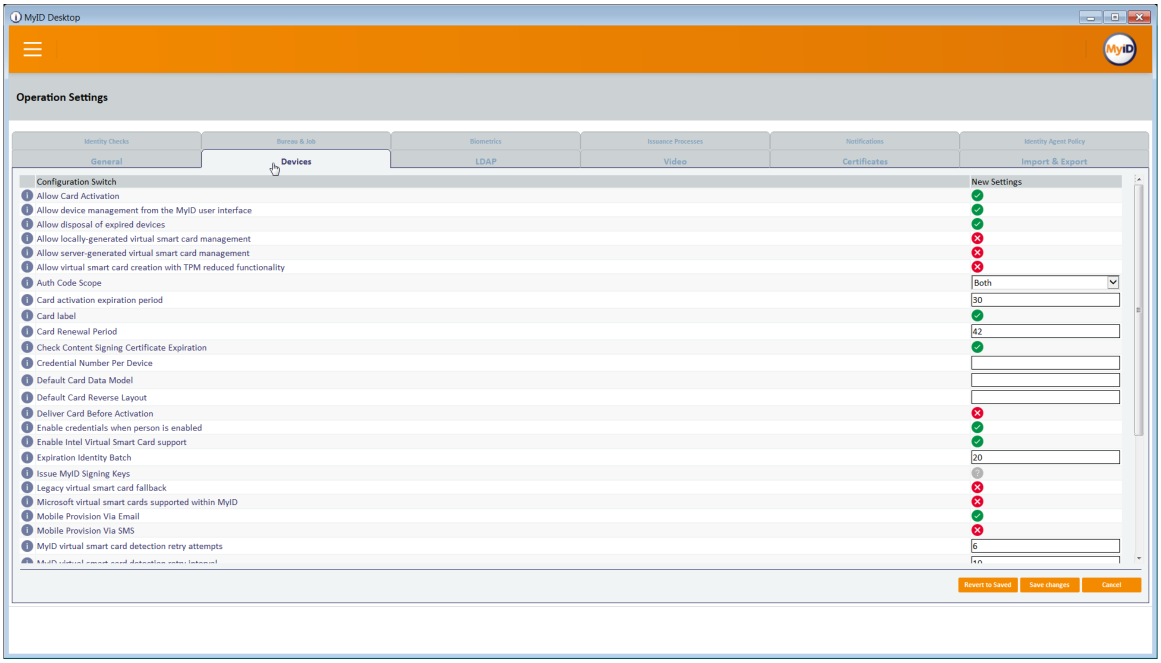


4. Go to the **Devices** tab.

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

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

7. Click **Save changes**.

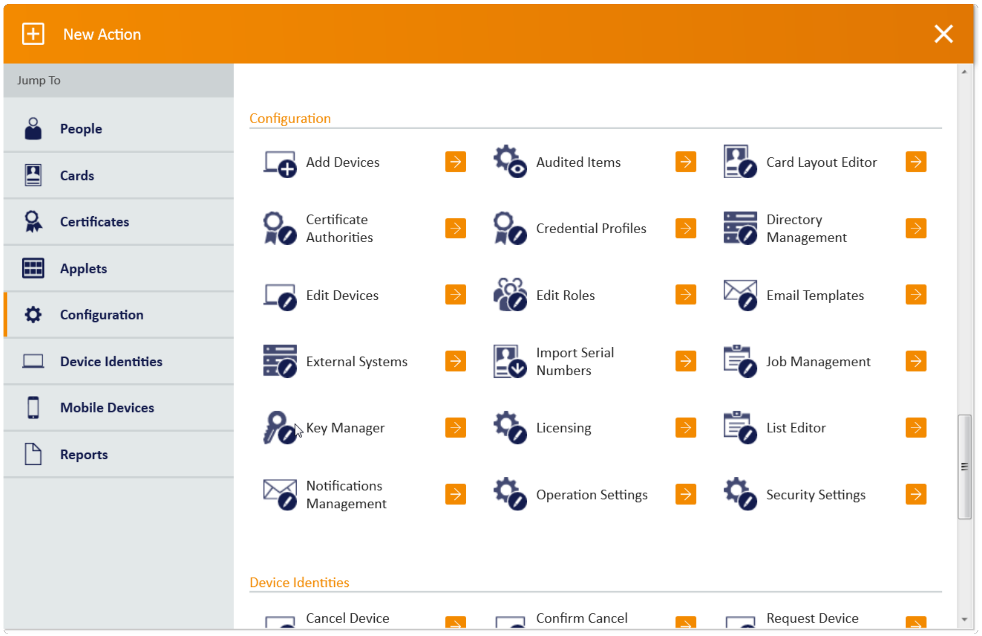


Configuration Switch	New Settings
Allow Card Activation	✓
Allow device management from the MyID user interface	✓
Allow disposal of expired devices	✓
Allow locally-generated virtual smart card management	✗
Allow server-generated virtual smart card management	✗
Allow virtual smart card creation with TPM reduced functionality	✗
Auth Code Scope	Both
Card activation expiration period	30
Card label	✓
Card Renewal Period	42
Check Content Signing Certificate Expiration	✓
Credential Number Per Device	
Default Card Data Model	
Default Card Reverse Layout	
Deliver Card Before Activation	✗
Enable credentials when person is enabled	✓
Enable Intel Virtual Smart Card support	✓
Expiration Identity Batch	20
Issue MyID Signing Keys	?
Legacy virtual smart card fallback	✗
Microsoft virtual smart cards supported within MyID	✗
Mobile Provision Via Email	✓
Mobile Provision Via SMS	✗
MyID virtual smart card detection retry attempts	6
MyID virtual smart card detection retry interval	10

2.2.7.2 Setting Up a PIN Protection Key

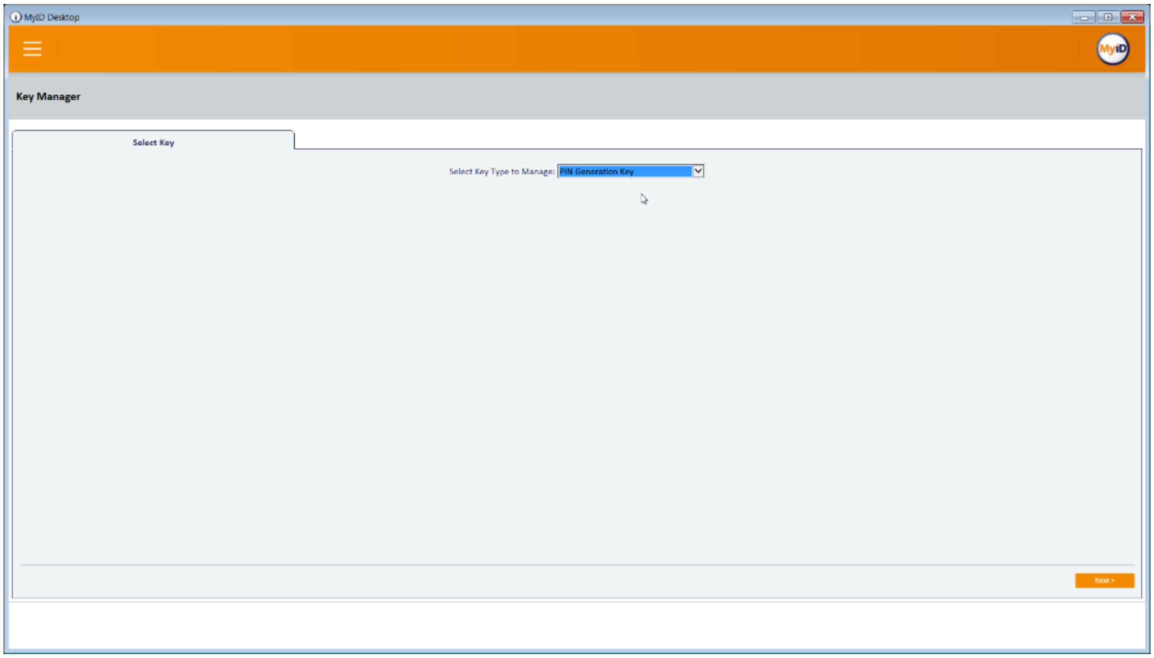
1. Click **New Action**.

2. Click **Configuration > Key Manager**.



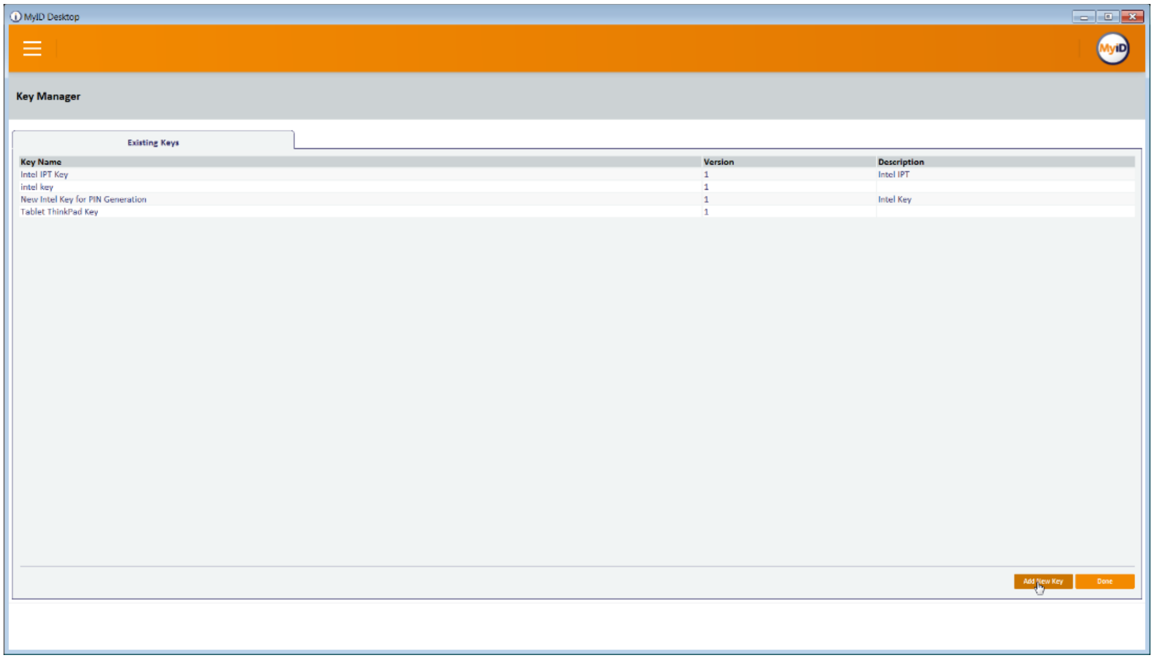
3. For **Select Key Type to Manage,** select **PIN Generation Key**.

4. Click **Next**.



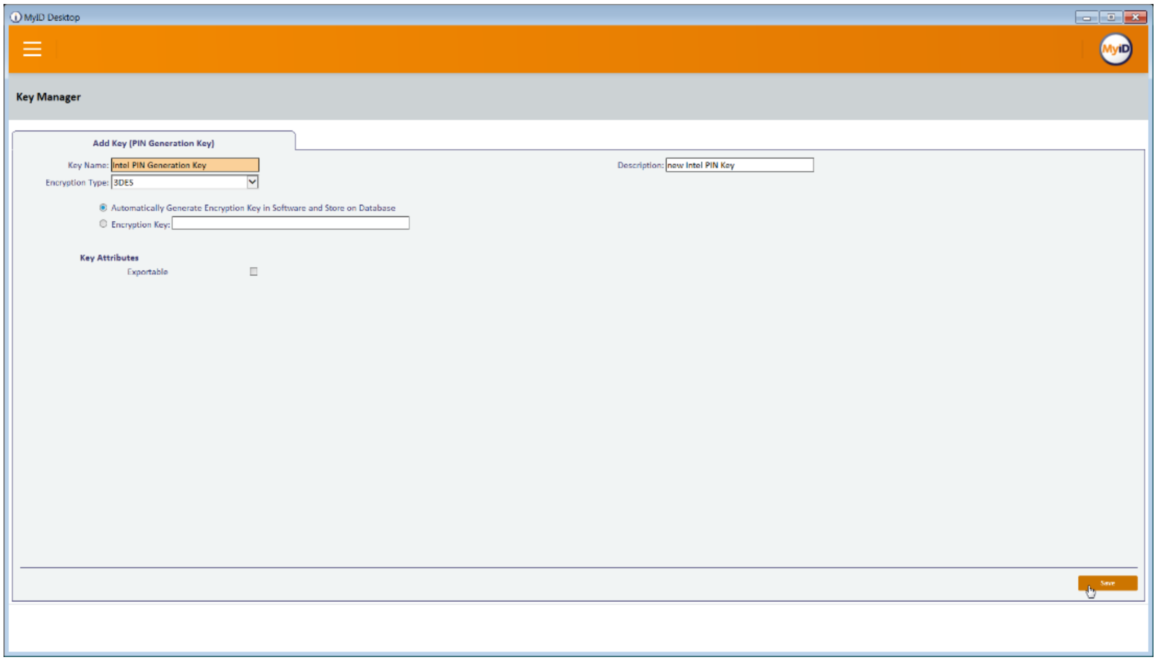
Select Key Type to Manage: PIN Generation Key

5. Click **Add New Key**.



Key Name	Version	Description
Intel IPT Key	1	Intel IPT
intel key	1	
New Intel Key for PIN Generation	1	Intel Key
Tablet ThinkPad Key	1	

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**.



Key Manager

Add Key (PIN Generation Key)

Key Name: Intel PIN Generation Key

Description: new Intel PIN Key

Encryption Type: 3DES

● Automatically Generate Encryption Key in Software and Store on Database

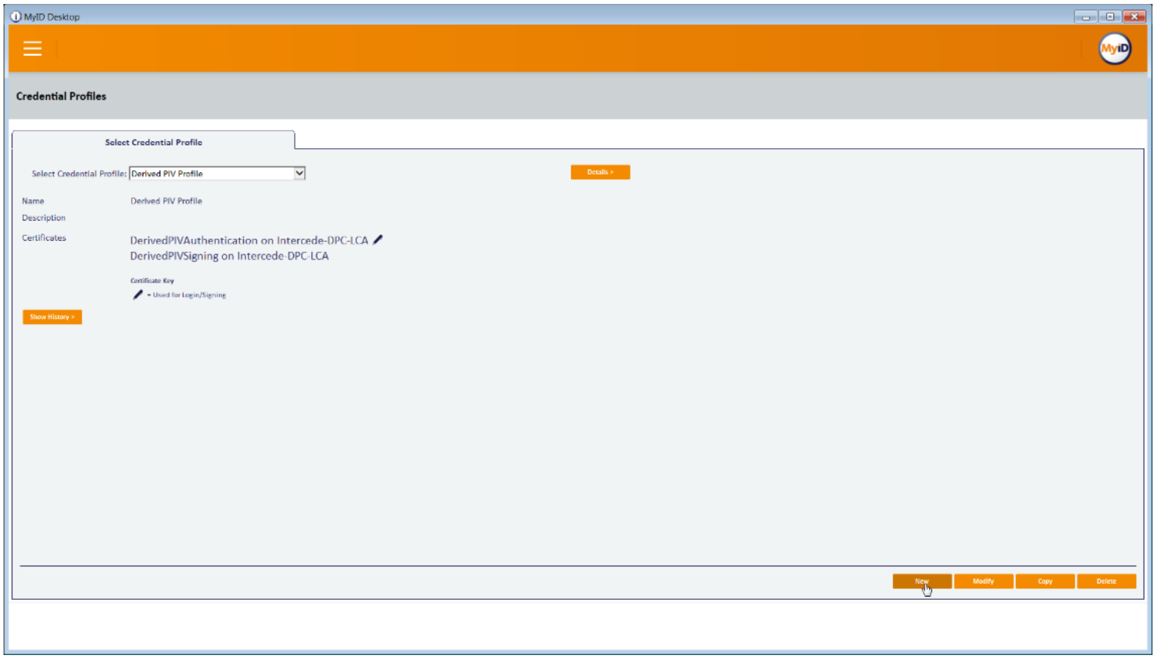
○ Encryption Key:

Key Attributes

Exportable □

2.2.7.3 Creating a Credential Profile

1. Click **New Action**.
2. Click **Configuration > Credential Profiles**.
3. Click **New**.



Select Credential Profile: Derived PIV Profile

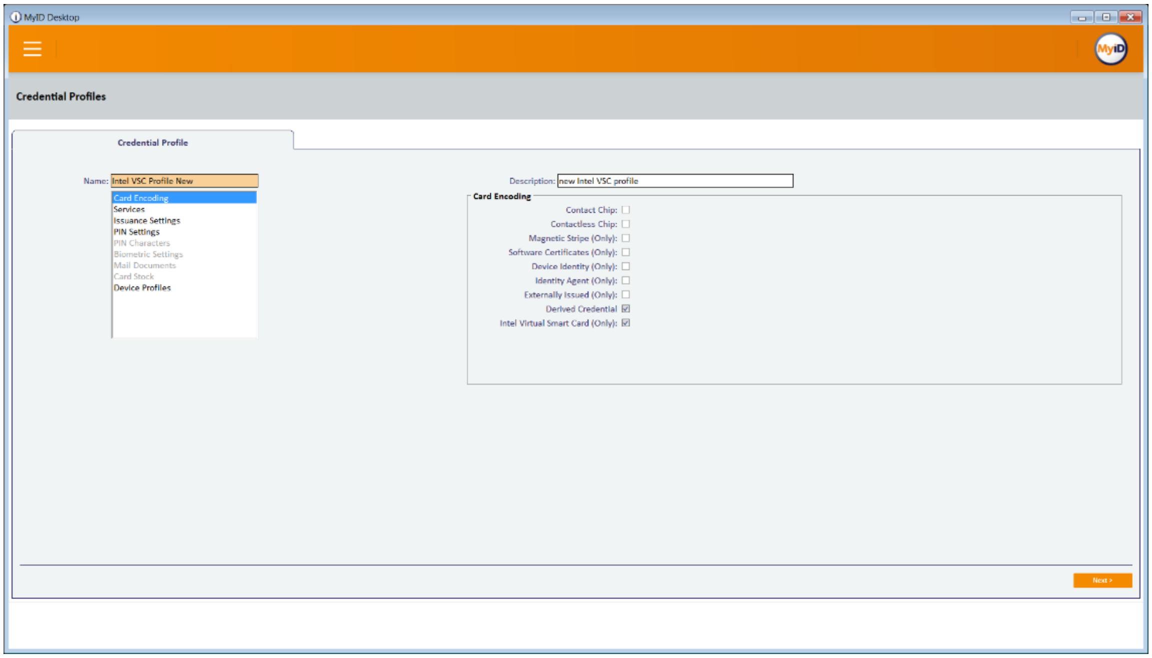
Name: Derived PIV Profile

Description:

Certificates: DerivedPIVAuthentication on Intercede-DPC-LCA
DerivedPIVSigning on Intercede-DPC-LCA

Certificate Key
= Used for Login/Signing

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)**.



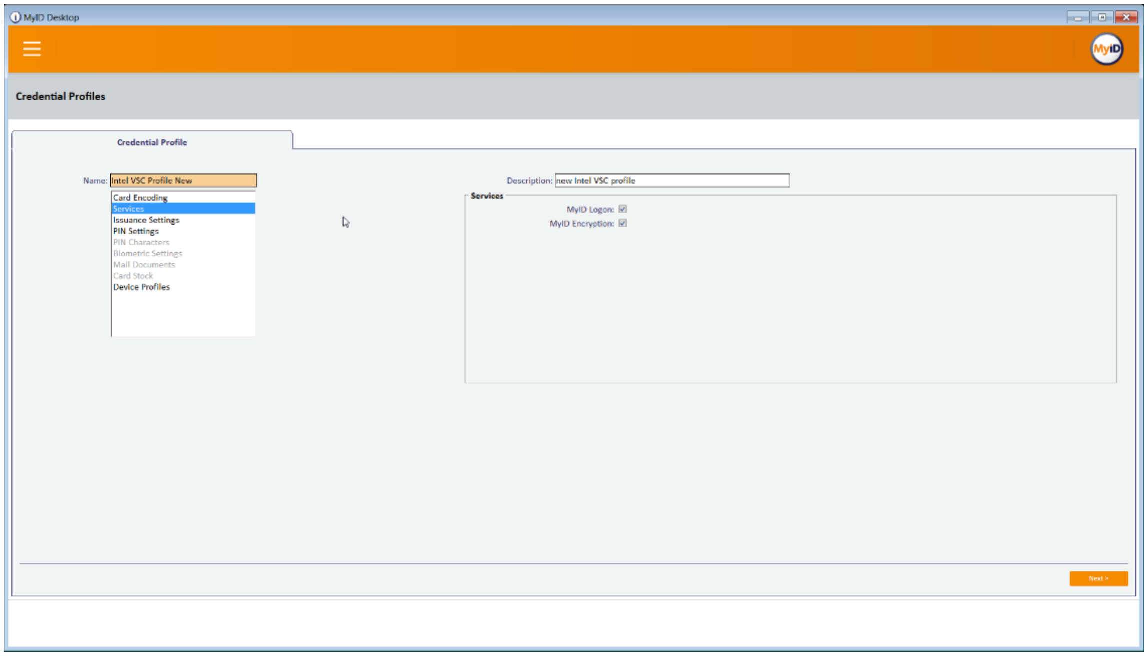
Name: Intel VSC Profile New

Description: new Intel VSC profile

Card Encoding

- Contact Chip: □
- Contactless Chip: □
- Magnetic Stripe (Only): □
- Software Certificates (Only): □
- Device Identity (Only): □
- Identity Agent (Only): □
- Externally Issued (Only): □
- Derived Credential ☑
- 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**.



MyID Desktop

Credential Profiles

Credential Profile

Name: Intel VSC Profile New

Description: new Intel VSC profile

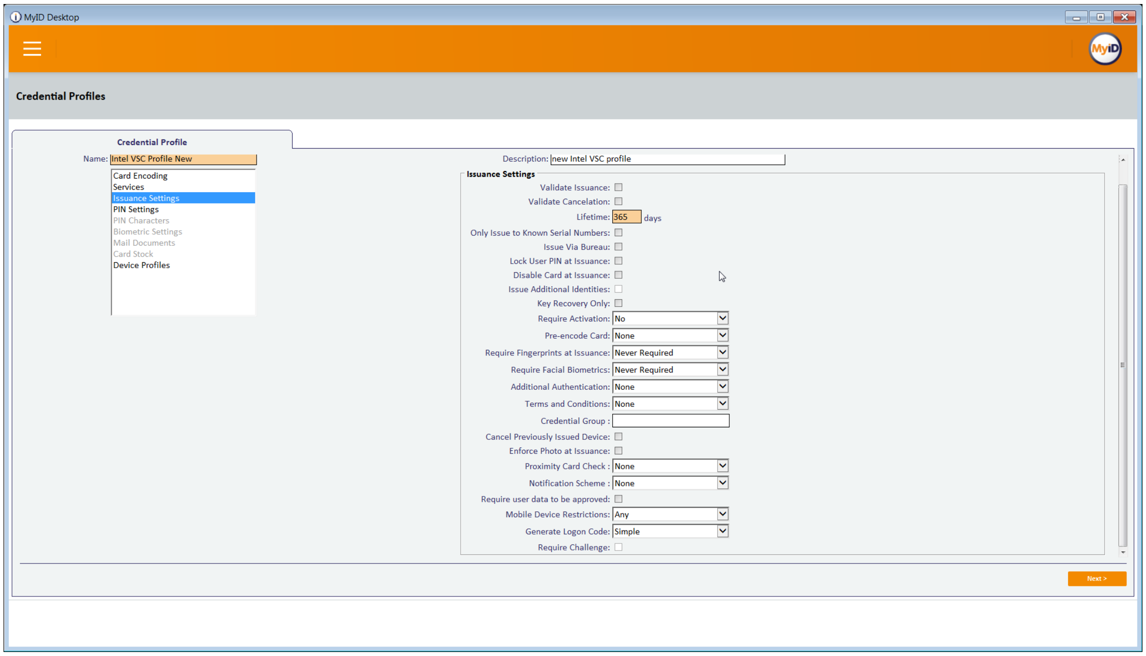
Services

MyID Logon: ☑

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**.



Name: Intel VSC Profile New

Description: new Intel VSC profile

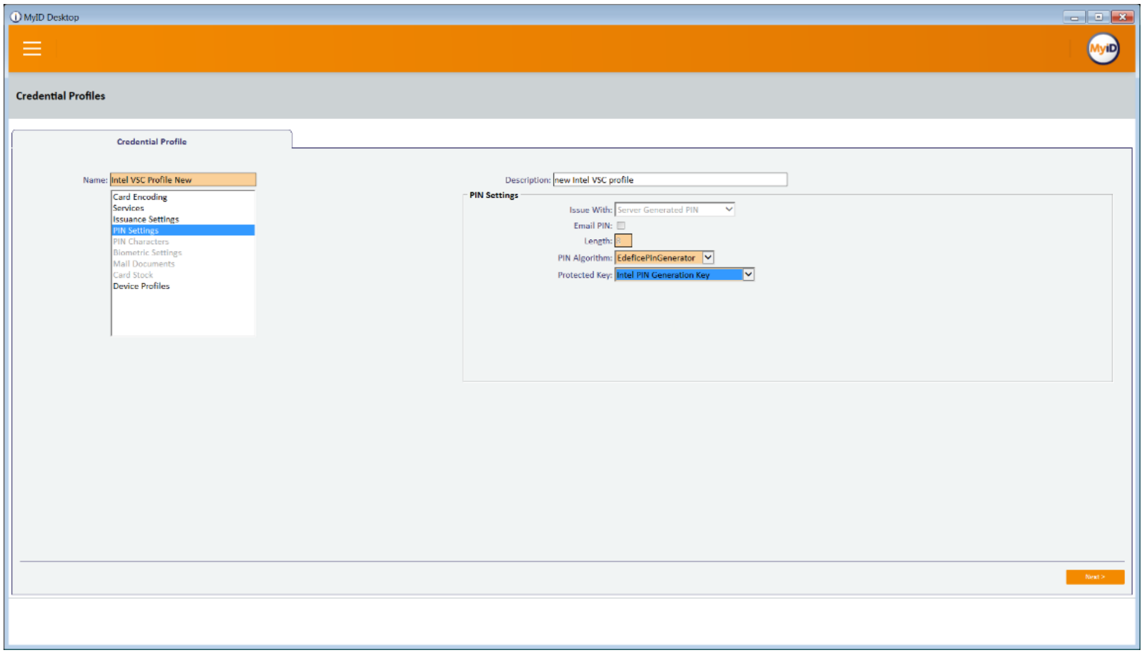
Issuance Settings

Validate Issuance: □
Validate Cancelation: □
Lifetime: 365 days
Only Issue to Known Serial Numbers: □
Issue Via Bureau: □
Lock User PIN at Issuance: □
Disable Card at Issuance: □
Issue Additional Identities: □
Key Recovery Only: □
Require Activation: No
Pre-encode Card: None
Require Fingerprints at Issuance: Never Required
Require Facial Biometrics: Never Required
Additional Authentication: None
Terms and Conditions: None
Credential Group :
Cancel Previously Issued Device: □
Enforce Photo at Issuance: □
Proximity Card Check : None
Notification Scheme : None
Require user data to be approved: □
Mobile Device Restrictions: Any
Generate Logon Code: Simple
Require Challenge: □

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

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

24. For **Protected Key**, select the PIN generation key created earlier.



Name: Intel VSC Profile New

Description: new Intel VSC profile

PIN Settings

Issue With: Server Generated PIN

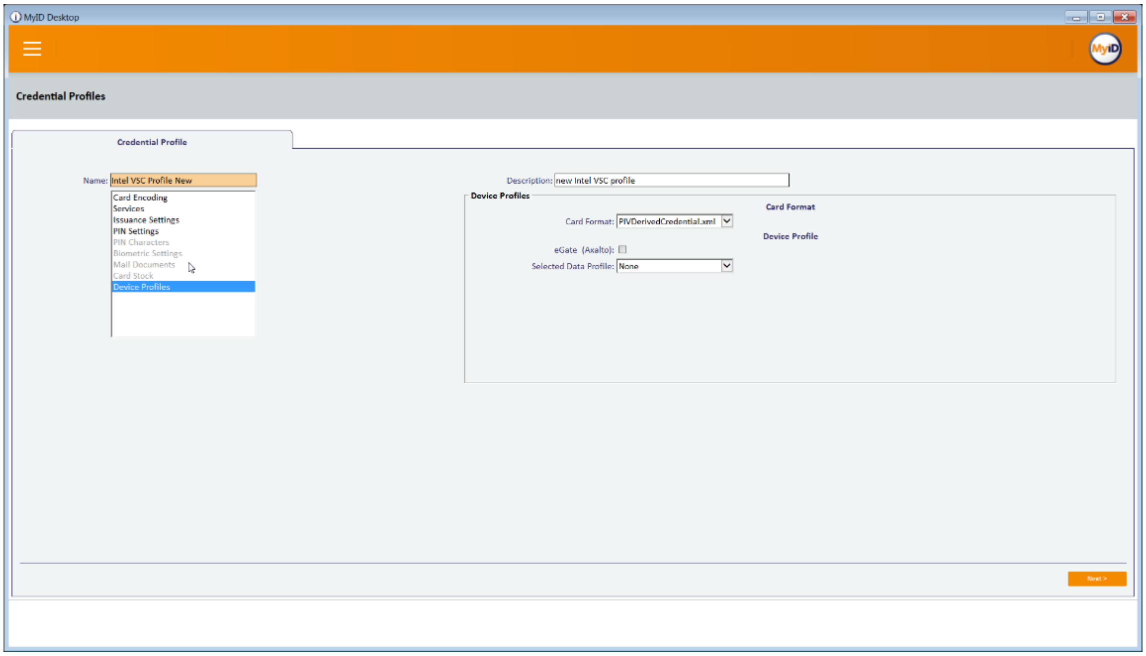
Email PIN: □

Length:

PIN Algorithm: EdeficePINGenerator

Protected Key: Intel PIN Generation Key

25. Select the **Device Profiles** tab.
26. For **Card Format**, select **PIVDerivedCredential.xml**.
27. Click **Next**.



Name: Intel VSC Profile New

Description: new Intel VSC profile

Device Profiles

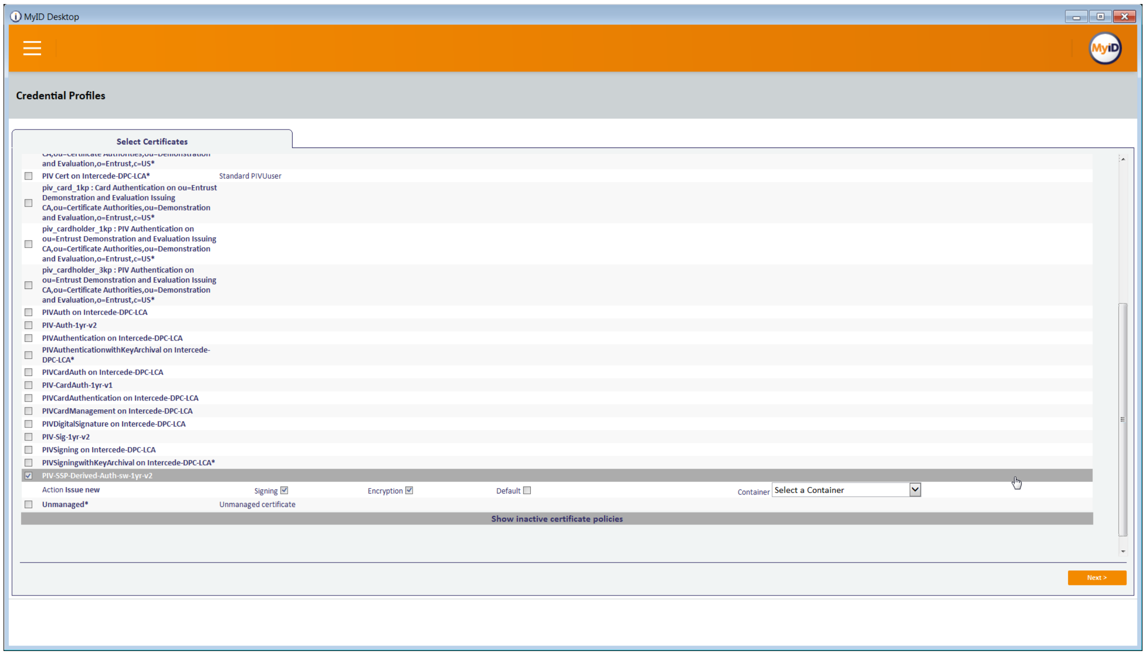
Card Format: PIVDerivedCredential.xml

eGate (Axalto): □

Selected Data Profile: None

28. Select the certificates to be issued with the VSC.

29. Click **Next**.



MyID Desktop

Credential Profiles

Select Certificates

CA,ou=Certificate Authorities,ou=Demonstration
and Evaluation,o=Entrust,c=US*

☐ PIV Cert on Intercede-DPC-LCA* Standard PIVUuser

☐ piv_card_1kp : Card Authentication on ou=Entrust Demonstration and Evaluation Issuing CA,ou=Certificate Authorities,ou=Demonstration and Evaluation,o=Entrust,c=US*

☐ piv_cardholder_1kp : PIV Authentication on ou=Entrust Demonstration and Evaluation Issuing CA,ou=Certificate Authorities,ou=Demonstration and Evaluation,o=Entrust,c=US*

☐ piv_cardholder_3kp : PIV Authentication on ou=Entrust Demonstration and Evaluation Issuing CA,ou=Certificate Authorities,ou=Demonstration and Evaluation,o=Entrust,c=US*

☐ PIVAuth on Intercede-DPC-LCA

☐ PIV-Auth-1yr-v2

☐ PIVAuthentication on Intercede-DPC-LCA

☐ PIVAuthenticationwithKeyArchival on Intercede-DPC-LCA*

☐ PIVCardAuth on Intercede-DPC-LCA

☐ PIV-CardAuth-1yr-v1

☐ PIVCardAuthentication on Intercede-DPC-LCA

☐ PIVCardManagement on Intercede-DPC-LCA

☐ PIVDigitalSignature on Intercede-DPC-LCA

☐ PIV-Sig-1yr-v2

☐ PIVSigning on Intercede-DPC-LCA

☐ PIVSigningwithKeyArchival on Intercede-DPC-LCA*

☑ PIV-SSP-Derived-Auth-sw-1yr-v2

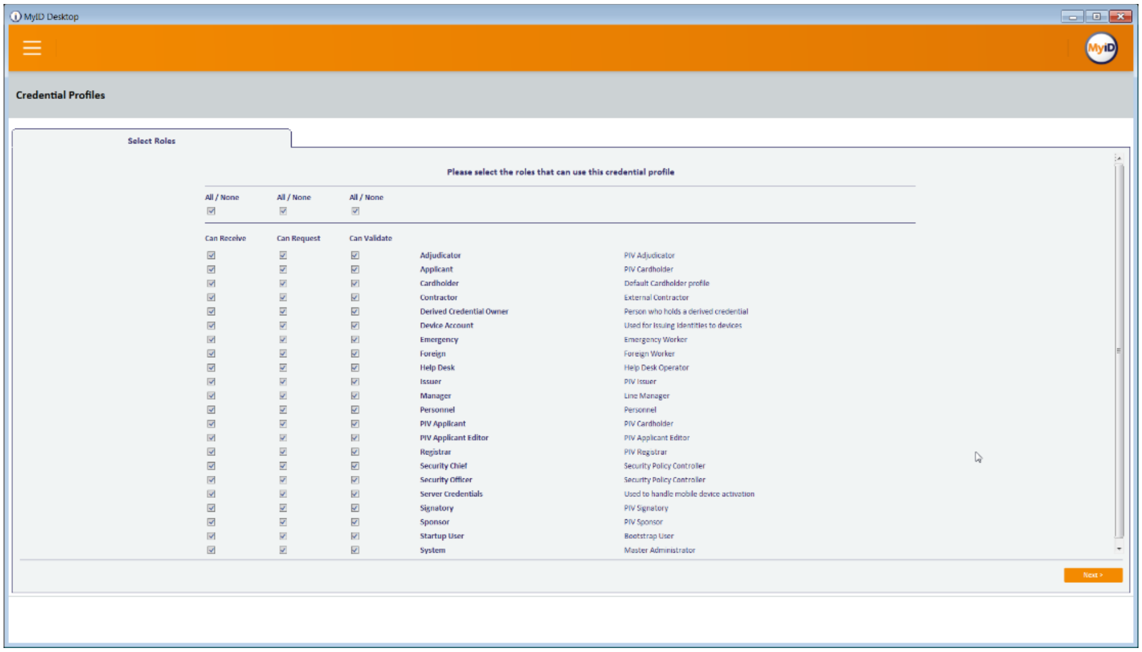
Action Issue new Signing ☑ Encryption ☑ Default ☐ Container Select a Container

☐ Unmanaged* Unmanaged certificate

Show inactive certificate policies

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

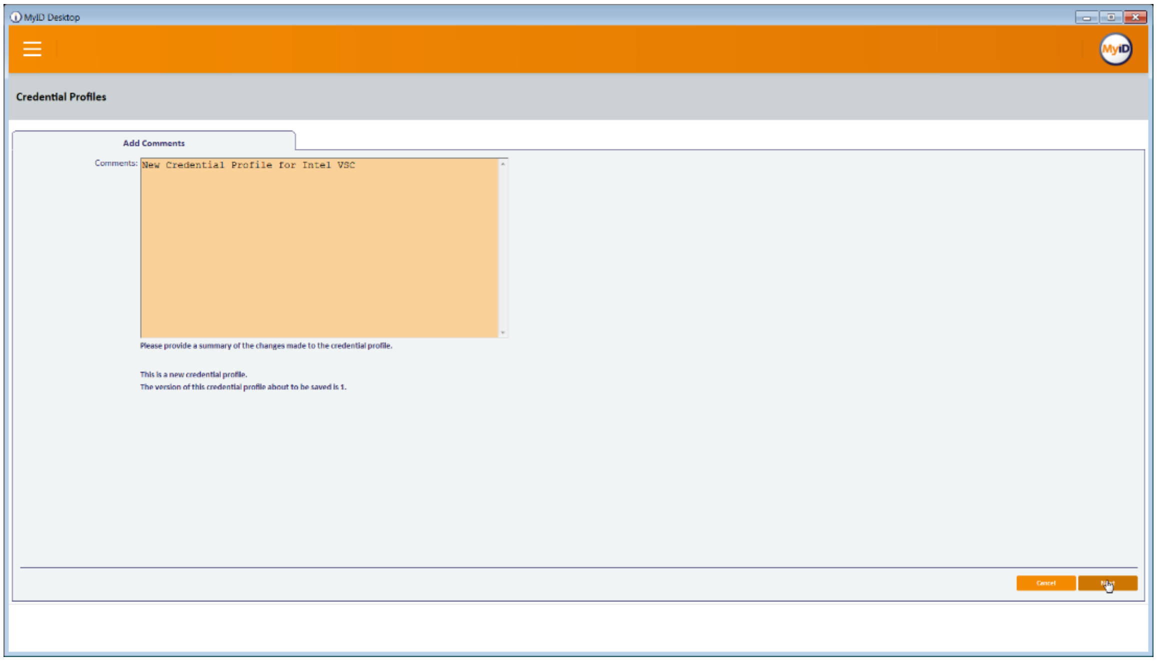
31. Click **Next**.



Please select the roles that can use this credential profile

All / None	All / None	All / None		
☑	☑	☑		
Can Receive	**Can Request**	**Can Validate**		
☑	☑	☑	Adjudicator	PIV Adjudicator
☑	☑	☑	Applicant	PIV Cardholder
☑	☑	☑	Cardholder	Default Cardholder profile
☑	☑	☑	Contractor	External Contractor
☑	☑	☑	Derived Credential Owner	Person who holds a derived credential
☑	☑	☑	Device Account	Used for Issuing Identities to devices
☑	☑	☑	Emergency	Emergency Worker
☑	☑	☑	Foreign	Foreign Worker
☑	☑	☑	Help Desk	Help Desk Operator
☑	☑	☑	Issuer	PIV Issuer
☑	☑	☑	Manager	Line Manager
☑	☑	☑	Personnel	Personnel
☑	☑	☑	PIV Applicant	PIV Cardholder
☑	☑	☑	PIV Applicant Editor	PIV Applicant Editor
☑	☑	☑	Registrar	PIV Registrar
☑	☑	☑	Security Chief	Security Policy Controller
☑	☑	☑	Security Officer	Security Policy Controller
☑	☑	☑	Server Credentials	Used to handle mobile device activation
☑	☑	☑	Signatory	PIV Signatory
☑	☑	☑	Sponsor	PIV Sponsor
☑	☑	☑	Startup User	Bootstrap User
☑	☑	☑	System	Master Administrator

32. Enter a description and click **Next**.



Comments: New Credential Profile for Intel VSC

Please provide a summary of the changes made to the credential profile.

This is a new credential profile.
The version of this credential profile about to be saved is 1.

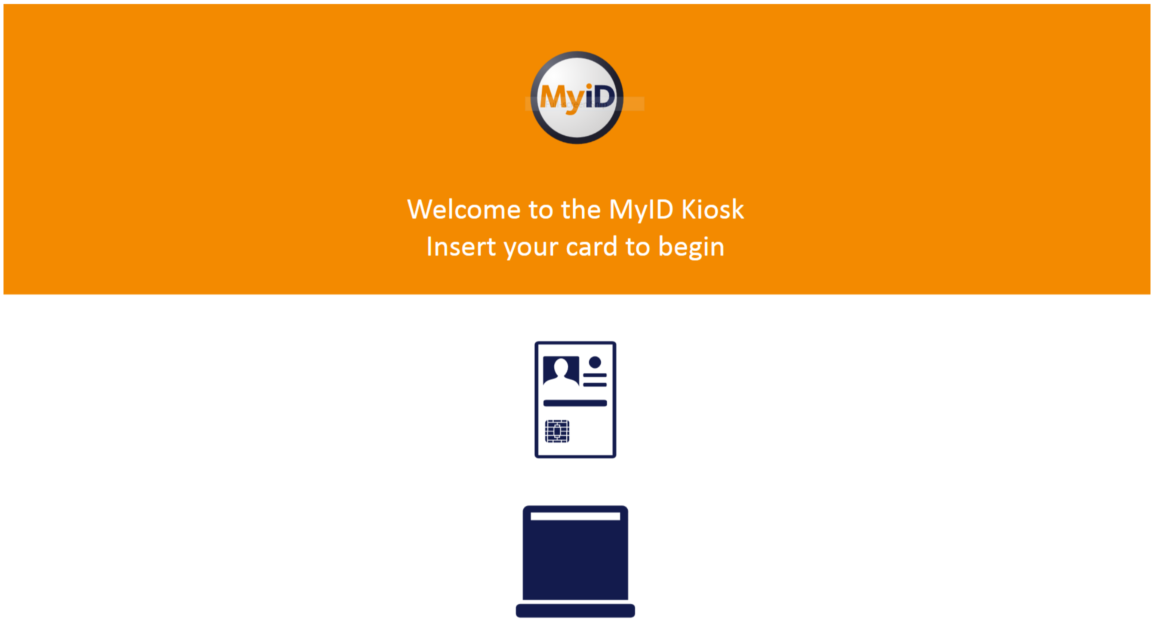
2.2.8 DPC Lifecycle Workflows

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

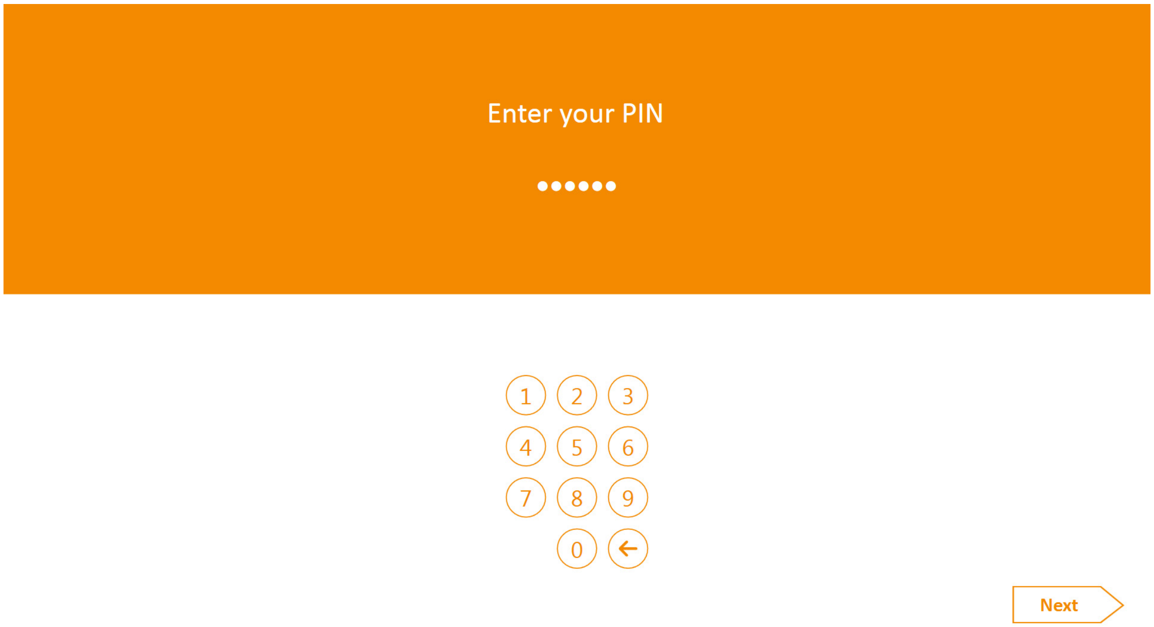
The following steps are performed by the DPC Applicant by using the MyID Self-Service Kiosk and the MyID Identity Agent application on the target mobile device.

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

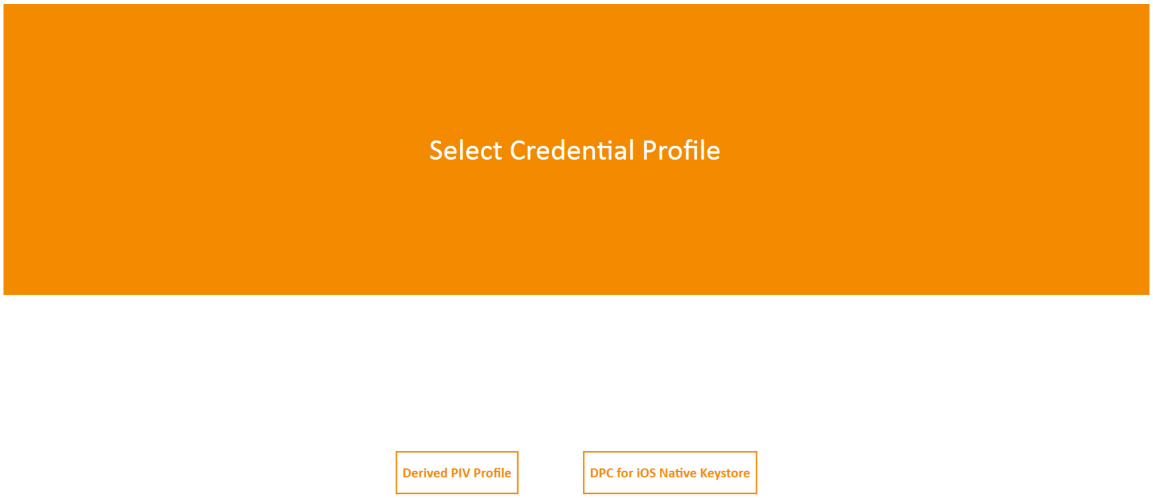
2. On the **Enter your PIN** screen:
   a. Enter the PIN used to activate the inserted PIV Card.
   b. Select **Next**.



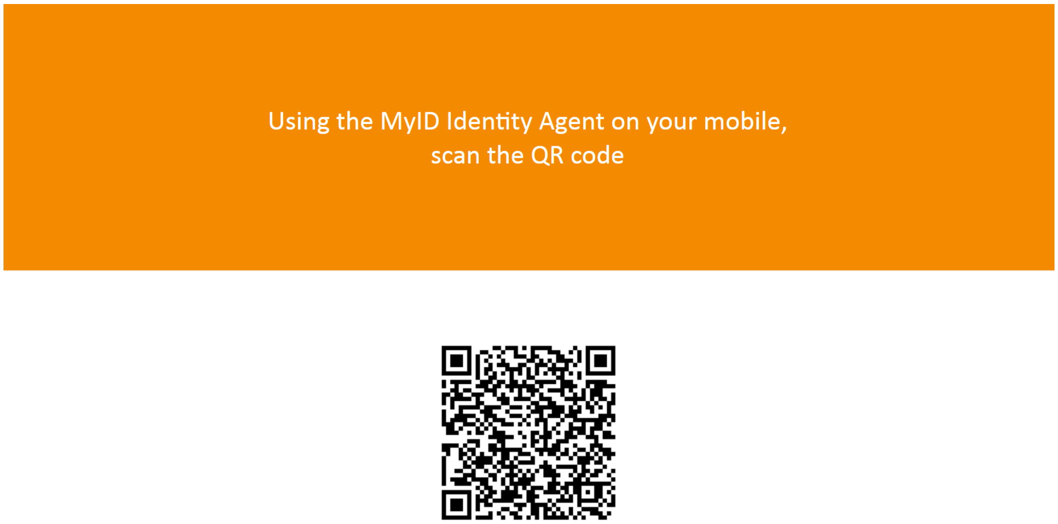
3. On the **Select Credential Profile** screen:

   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**.



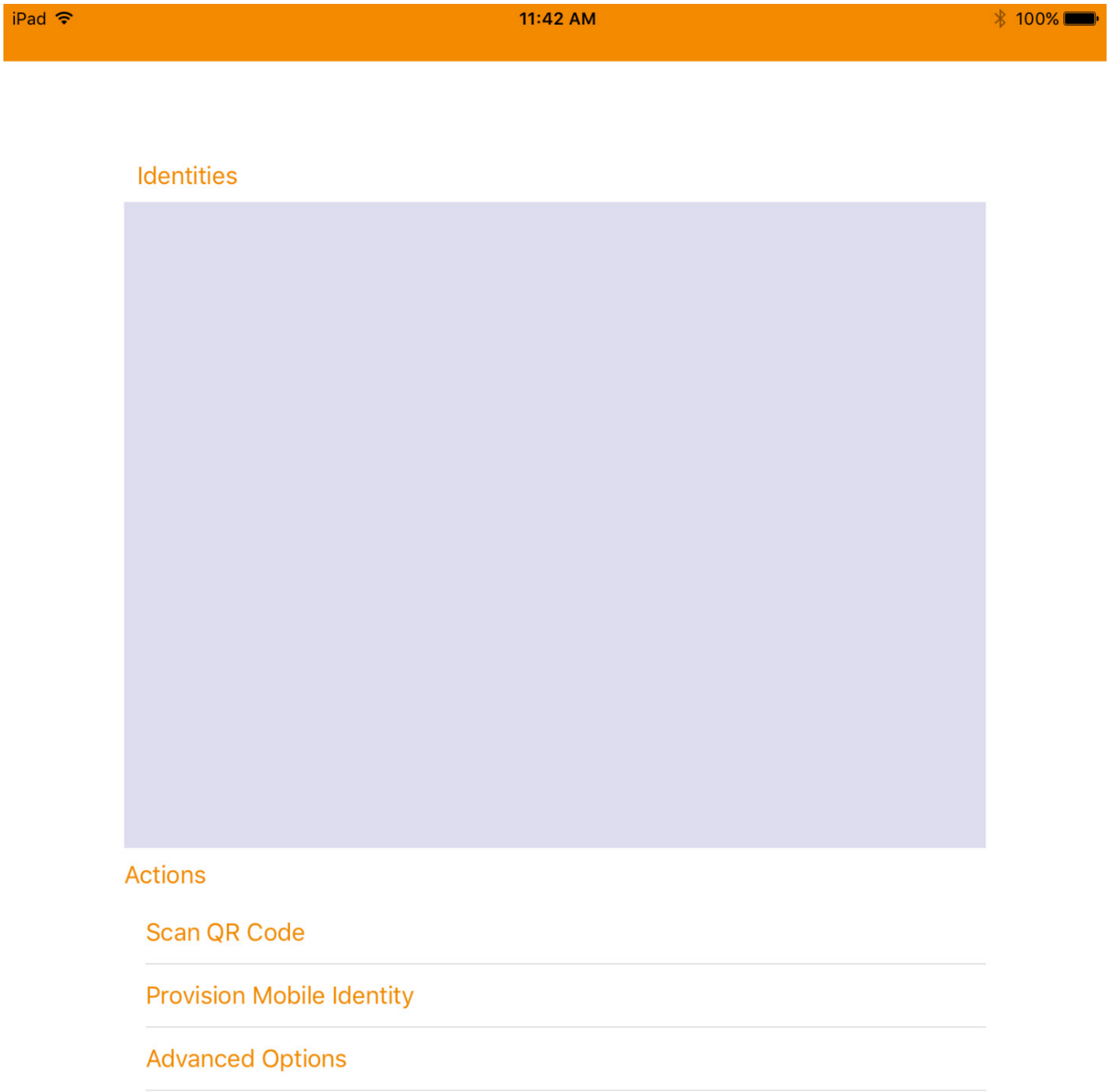
   c. The MyID Self-Service Kiosk will display a QR code; the remaining steps are completed by using the MyID Identity Agent application on the target mobile device.



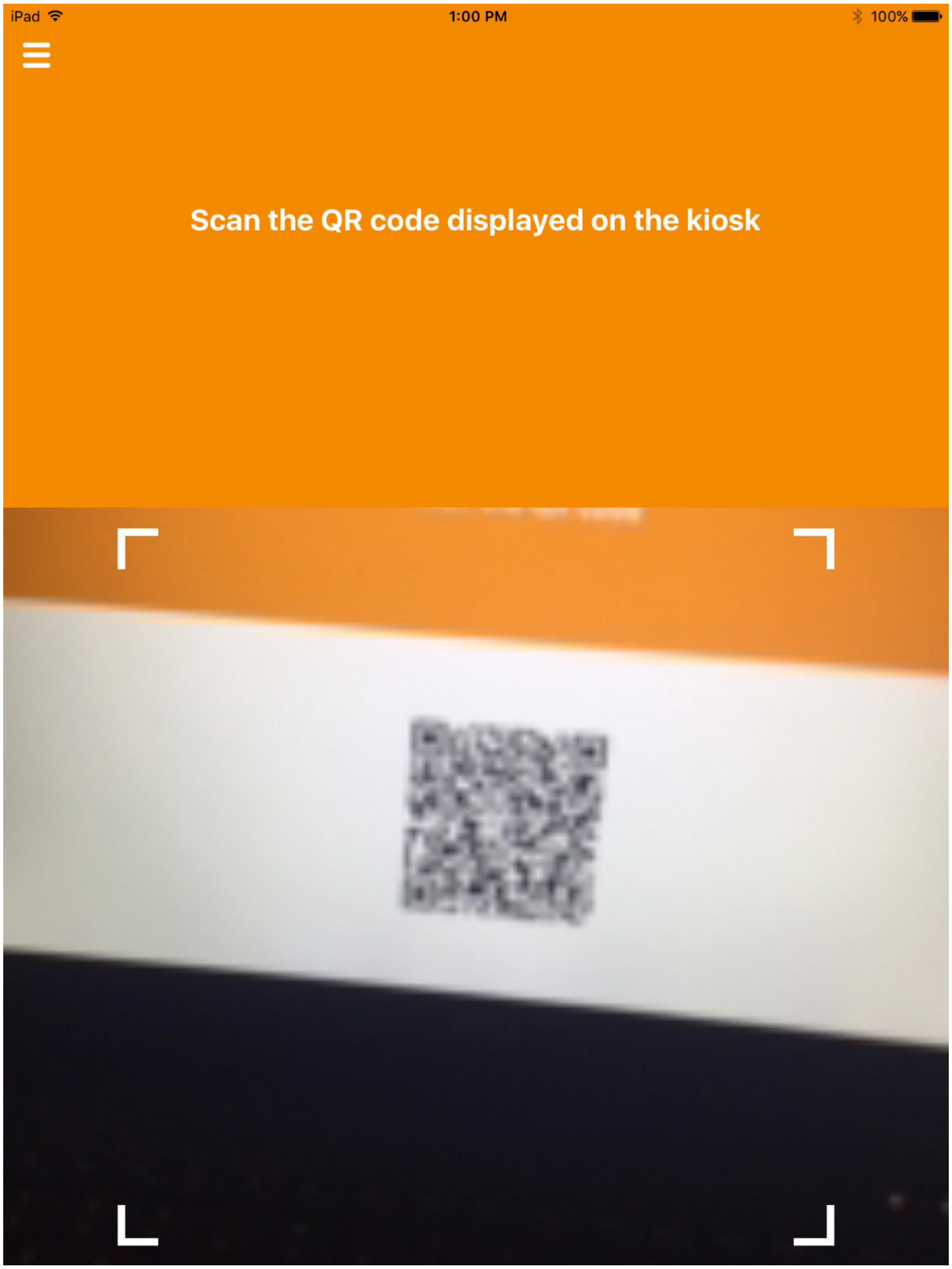
Using the MyID Identity Agent on your mobile,
scan the QR code

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.

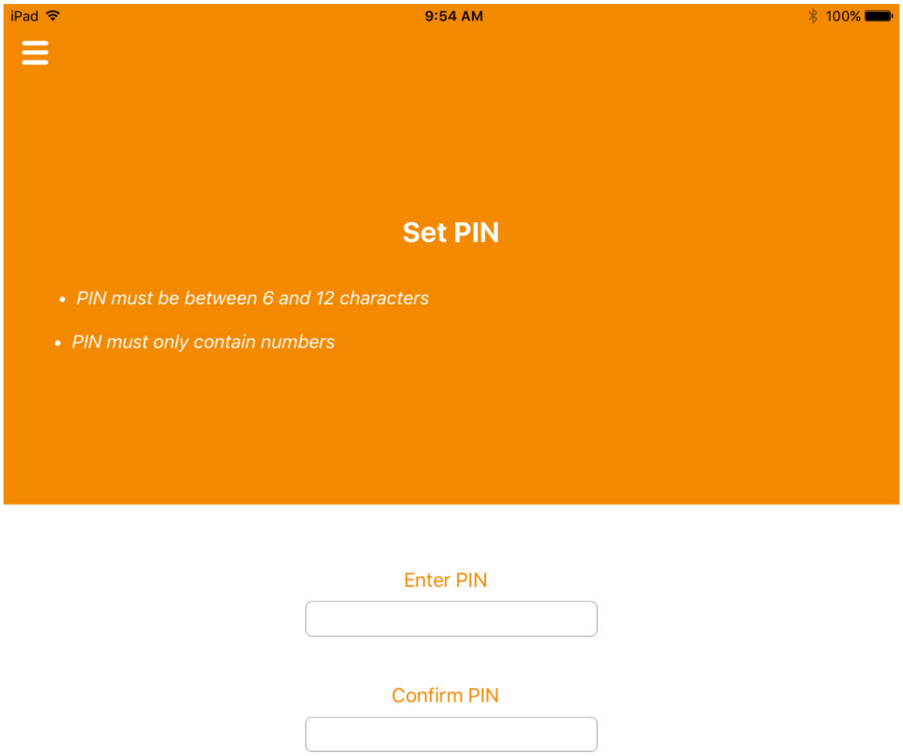


Scan the QR code displayed on the kiosk

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.



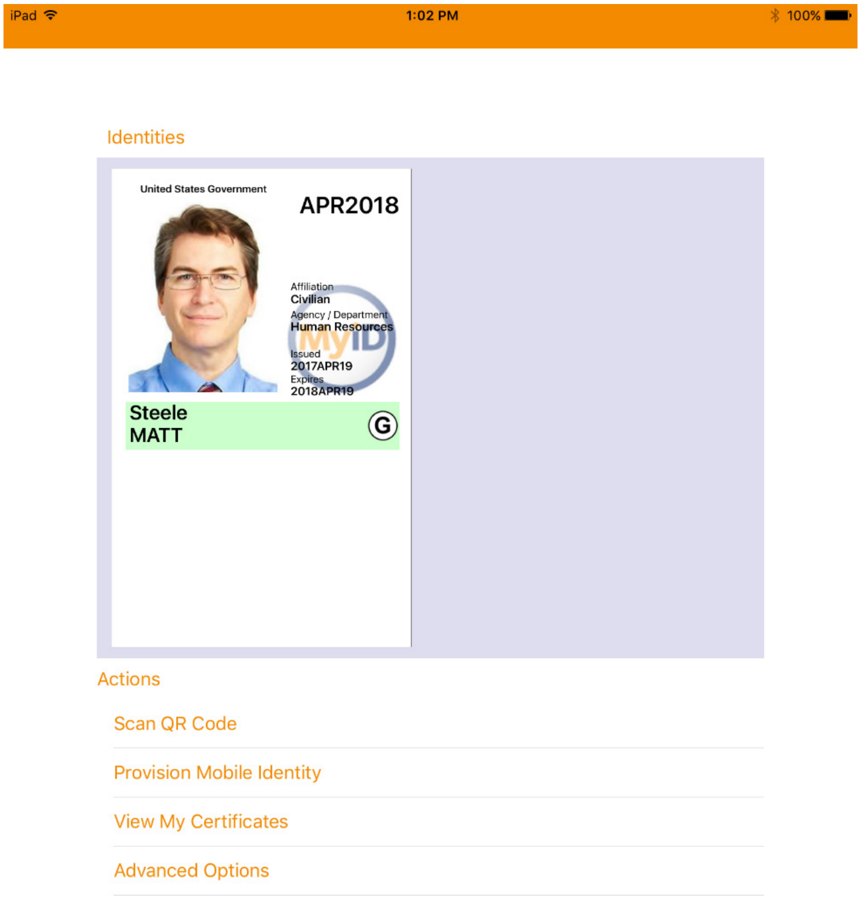
Set PIN

- *PIN must be between 6 and 12 characters*
- *PIN must only contain numbers*

Enter PIN

Confirm 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.



United States Government

APR2018

Affiliation
Civilian

Agency / Department
Human Resources

Issued
2017APR19

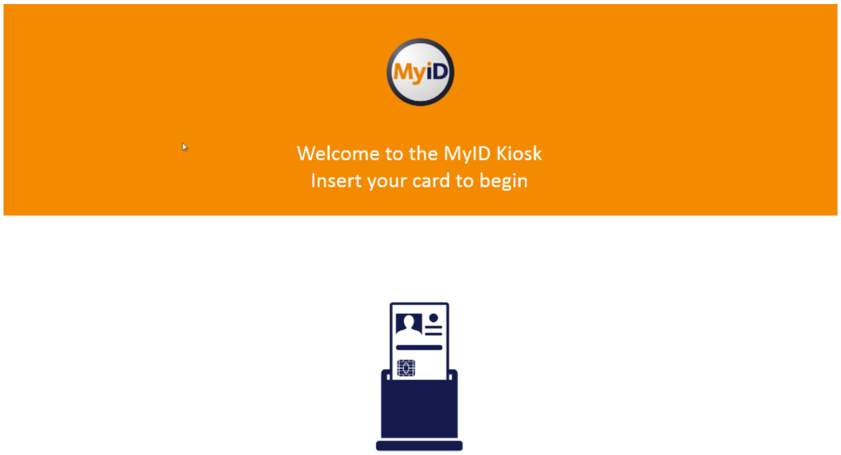
Expires
2018APR19

Steele
MATT

2.2.8.2 Intel Authenticate Issuance Workflow

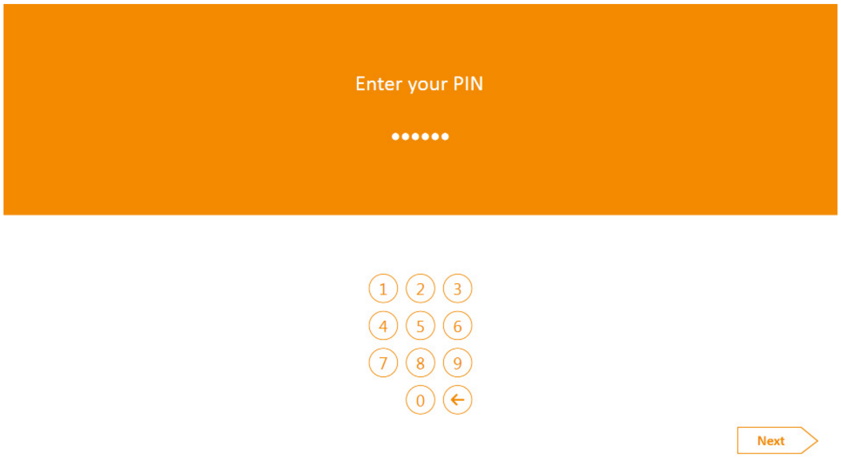
2.2.8.2.1 Requesting a DPC for Intel VSC

1. Go to a **MyID Kiosk**.



Welcome to the MyID Kiosk
Insert your card to begin

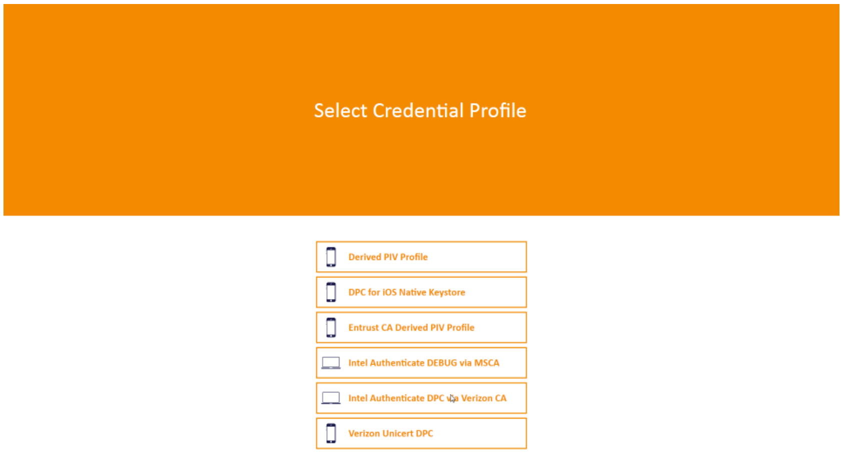
2. Insert a PIV Card.
3. Enter the PIN for the PIV Card.



Enter your PIN

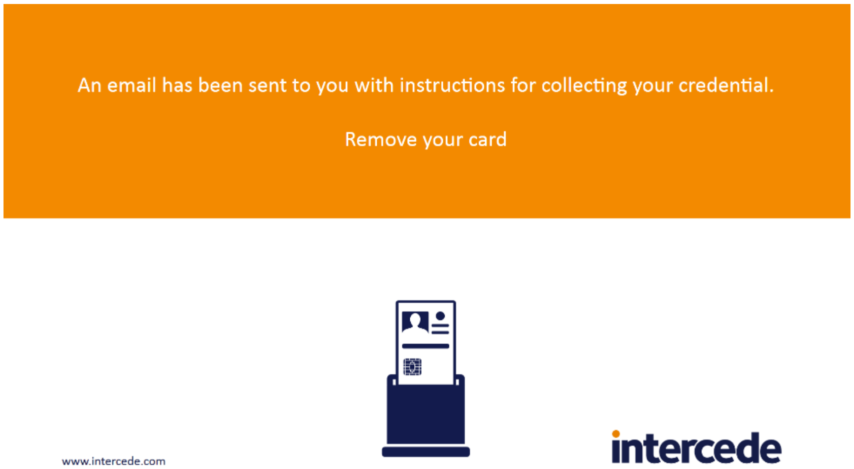
••••••

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



Select Credential Profile

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



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

Remove your card

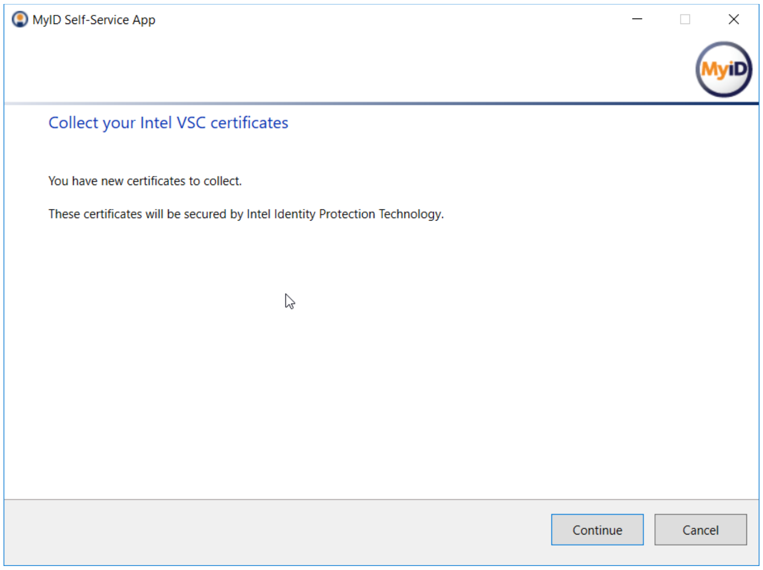
2.2.8.2.2 Collecting the DPC

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**.

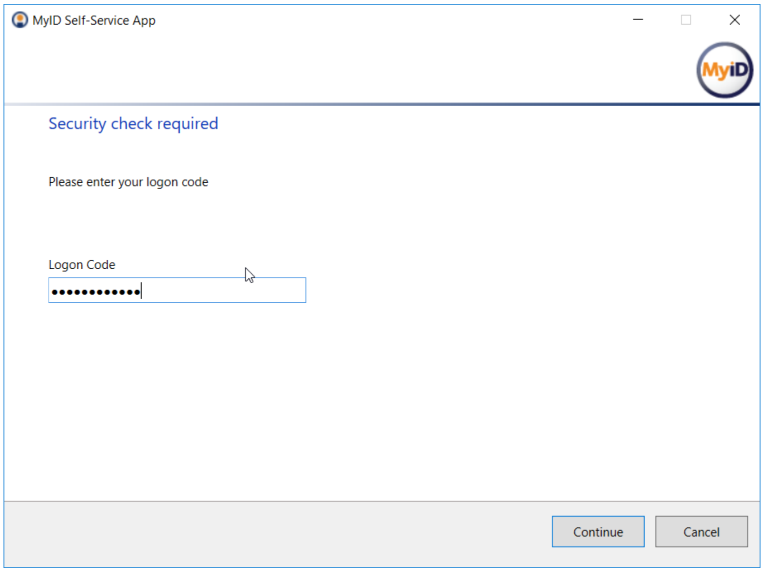

MyID Self-Service App

Collect your Intel VSC certificates

You have new certificates to collect.

These certificates will be secured by Intel Identity Protection Technology.

3. Enter the **Logon Code** from the email.
4. Click **Continue**.

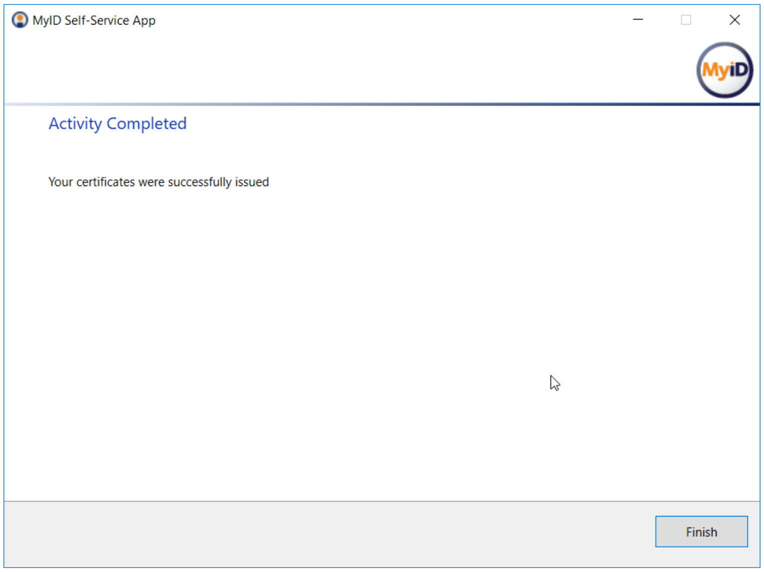

MyID Self-Service App

Security check required

Please enter your logon code

Logon Code: ••••••••••••

5. Click **Finish** after the certificates are successfully collected.



Activity Completed

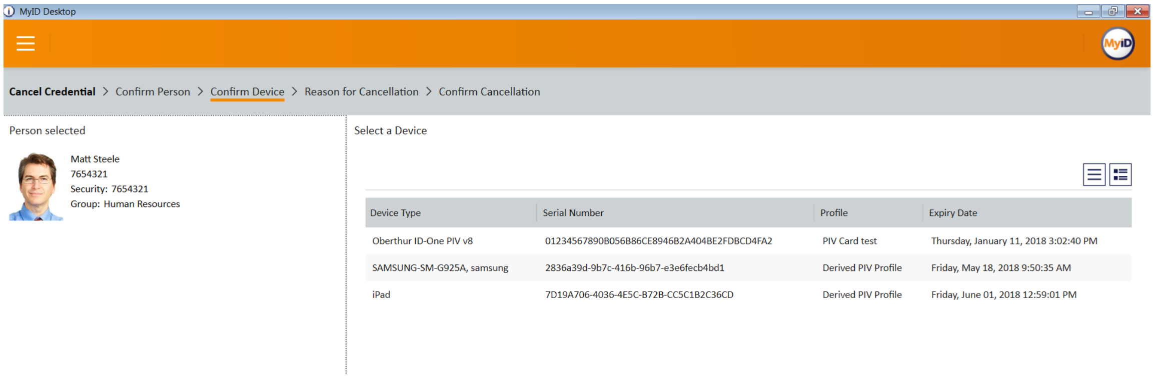
Your certificates were successfully issued

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.



MyID Desktop
MyID
Cancel Credential > Confirm Person > Confirm Device > Reason for Cancellation > Confirm Cancellation

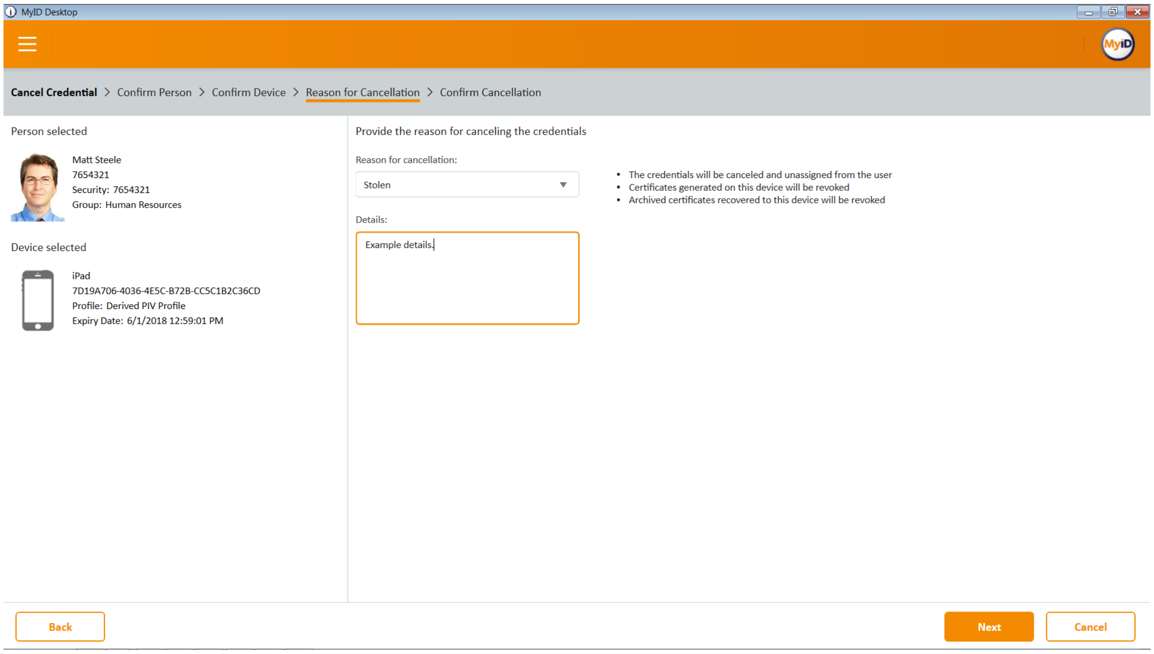
Person selected

Matt Steele
7654321
Security: 7654321
Group: Human Resources

Select a Device

Device Type	Serial Number	Profile	Expiry Date
Oberthur ID-One PIV v8	01234567890B056B86CE8946B2A404BE2FDBCD4FA2	PIV Card test	Thursday, January 11, 2018 3:02:40 PM
SAMSUNG-SM-G925A, samsung	2836a39d-9b7c-416b-96b7-e3e6fecb4bd1	Derived PIV Profile	Friday, May 18, 2018 9:50:35 AM
iPad	7D19A706-4036-4E5C-B72B-CC5C1B2C36CD	Derived PIV Profile	Friday, June 01, 2018 12:59:01 PM

2. Select a reason for termination and enter any other required information for policy compliance.



Cancel Credential > Confirm Person > Confirm Device > Reason for Cancellation > Confirm Cancellation

Person selected

Matt Steele
7654321
Security: 7654321
Group: Human Resources

Device selected

iPad
7D19A706-4036-4E5C-B72B-CC5C1B2C36CD
Profile: Derived PIV Profile
Expiry Date: 6/1/2018 12:59:01 PM

Provide the reason for canceling the credentials

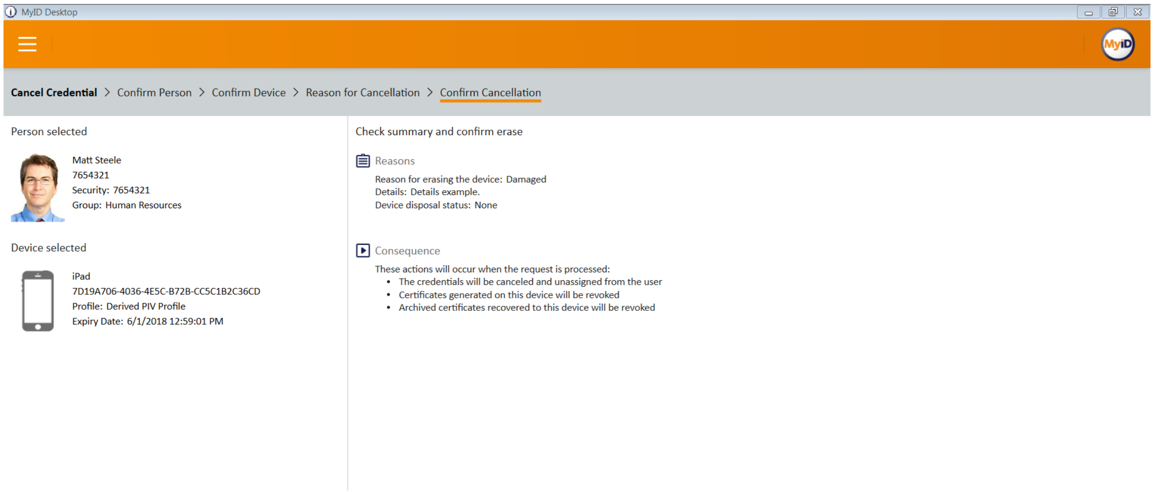
Reason for cancellation: Stolen

Details: Example details.

- The credentials will be canceled and unassigned from the user
- Certificates generated on this device will be revoked
- Archived certificates recovered to this device will be revoked

3. Click **Next**

4. Confirm the termination of the DPC.



Cancel Credential > Confirm Person > Confirm Device > Reason for Cancellation > Confirm Cancellation

Person selected

Matt Steele
7654321
Security: 7654321
Group: Human Resources

Device selected

iPad
7D19A706-4036-4E5C-B72B-CC5C1B2C36CD
Profile: Derived PIV Profile
Expiry Date: 6/1/2018 12:59:01 PM

Check summary and confirm erase

Reasons

Reason for erasing the device: Damaged
Details: Details example.
Device disposal status: None

Consequence

These actions will occur when the request is processed:

- The credentials will be canceled and unassigned from the user
- Certificates generated on this device will be revoked
- Archived certificates recovered to this device will be revoked

Appendix A List of Acronyms

AD	Active Directory
CA	Certificate Authority
CAPI	Cryptographic Application Interface
CMS	Credential Management System
CPS	Cryptographic Service Provider
DMZ	Demilitarized Zone
DN	Distinguished Name
DPC	Derived PIV Credential
EMM	Enterprise Mobility Management
FASC-N	Federal Agency Smart Card Number
GPO	Group Policy Object
IDG	Identity Guard
IT	Information Technology
JCE	Java Cryptography Extension
JTK	Java Tool Kit
LDAP	Lightweight Directory Access Protocol
MDAC	Microsoft Data Access Components
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OID	Object Identifier
OS	Operating System
OU	Organizational Unit
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
QR	Quick Response [code]
RSA	Rivest-Shamir-Adleman
SCEP	Simple Certificate Enrollment Protocol
SP	Special Publication
SQL	Structured Query Language

SSL	Secure Sockets Layer
SSM	Self-Service Module
SSP	Shared Service Provider
TLS	Transport Layer Security
UPI	UniCERT Programmatic Interface
UPN	User Principal Name
URL	Universal Resource Locator
UUID	Universal Unique Identifier
VLAN	Virtual Local Area Network
VSC	Virtual Smart Card
WMI	Windows Management Instrumentation
WSVC	World Wide Web Publishing Service