NISTIR 8055 (Draft)

Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research

Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya
Paul Fox
Mike Miller
Ryan Holley
Karen Scarfone

This publication is available free of charge

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

NISTIR 8055 (Draft)

Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research

Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

Paul Fox
Mike Miller
Microsoft Corporation
Redmond, WA

Ryan Holley
Intercede
Reston, VA

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

This publication is available free of charge

July 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Internal Report 8055
100 pages (July 2015)

This publication is available free of charge

Public comment period: *July 14, 2015* through *August 24, 2015*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: dpc@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

This report documents proof of concept research for Derived Personal Identity Verification (PIV) Credentials. Smart card-based PIV Cards cannot be readily used with most mobile devices, such as smartphones and tablets, but Derived PIV Credentials (DPCs) can be used instead to PIV-enable these devices and provide multi-factor authentication for mobile device users. This report captures existing requirements related to DPCs, proposes an architecture that supports these requirements, and then demonstrates how such an architecture could be implemented and operated.

Keywords

authentication; credentials; derived credentials; Derived PIV Credential (DPC); electronic authentication; electronic credentials; mobile devices; Personal Identity Verification (PIV); smart cards

Acknowledgements

The authors wish to thank their colleagues, in particular David Cooper and Hildy Ferraiolo from NIST, Aman Arneja, Shweta Vaidya, Himanshu Soni, and Nelly Porter from Microsoft, and Andrew Atyeo and Chris Edwards from Intercede who reviewed drafts of this report and contributed to its technical content.

Audience

The intended audience for this report is individuals who have responsibilities for implementing NIST standards and guidelines to develop cybersecurity solutions. This includes technical subject matter experts in Identity Management Systems (IDMS) and PIV technology, engineers, integrators, product vendors, and security professionals. These individuals should already have general knowledge of enterprise information technology (IT) infrastructure services, PIV Cards, IDMS, Public Key Infrastructure (PKI) technology, mobile devices, and authentication and authorization technologies.

Trademark Information

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

1.1 Purpose and Scope

The purpose of this report is to document Derived Personal Identity Verification (PIV) Credentials proof of concept research using commercial-off-the-shelf hardware and software found in NIST's research laboratories. It represents the experimental research NIST has performed to develop an example of an implementation of Derived PIV Credentials (DPCs) based on NIST Special Publication (SP) 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials.*[1]

Other types of derived credentials are out of the scope of this report.

Background information on PIV Cards, DPCs, and electronic authentication is not provided in this report. For more information on these topics, see NIST SP 800-157*;* Federal Information Processing Standard (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*[2]; and NIST SP 800-63-2, *Electronic Authentication Guideline*[3].

1.2 Report Structure

The remainder of this report is organized into the following sections and appendices:

- Section 2 provides a summary of the business opportunities for using DPCs with modern mobile client devices.
- Section 3 describes usage scenarios for issuing PIV credentials and associated DPCs.
- Section 4 explains the application of Microsoft and Intercede technologies in accordance with NIST SP 800-157 to support the organization-provisioned PIV credentials usage scenario.
- The following sections discuss DPC-related activities:
  - Section 5: Initial issuance
  - Section 6: Maintenance
  - Section 7: Termination
  - Section 8: Usage
- Section 9 briefly looks at next steps for research in the area of DPCs.
- Appendix A provides mappings between the DPC requirements from this report and requirements from other federal government standards and guidelines.
- Appendix B defines acronyms and abbreviations used in the report.
- Appendix C provides a bibliography for the report.

[1] http://dx.doi.org/10.6028/NIST.SP.800-157
[2] http://dx.doi.org/10.6028/NIST.FIPS.201-2
[3] http://dx.doi.org/10.6028/NIST.SP.800-63-2

2 Business Opportunities for Using DPCs with Mobile Client Devices

This section provides a summary of the business opportunities for using Derived PIV Credentials (DPCs) with modern mobile client devices based on NIST SP 800-157 recommendations. First, the section introduces the challenges with using PIV Cards with mobile devices. Then the section describes an overview of the proposed DPC solution. The section ends with a summary of the requirements related to DPCs as described in NIST SP 800-157.

2.1 Challenges with Using PIV Cards on Mobile Devices

Organizations protect their information systems, in part, by "granting users only those accesses they need to perform their official duties."[4] This principle of "least privilege" requires both authentication and authorization processes. FIPS 201-2 recommends using X.509 smart cards with user data in conjunction with passwords/personal identification numbers (PINs) to provide two-factor authentication to federal information systems.

While many desktop and laptop computers have built-in card readers, enterprises today rely heavily on the productivity of mobile devices (e.g., smartphones and tablets) that do not easily accommodate card readers. Organizations reliant on smart card and password two-factor authentication need to authenticate users of mobile devices in a way that is more tamper-resistant than a password and as easy to use as a smart card. However, it is challenging to use smart cards on mobile devices due to their form factor. Attaching or tethering a separate external smart card reader to smartphones or tablets creates usability and portability challenges that make the card an impractical authentication token.

2.2 Proposed Solution: DPCs

NIST SP 800-157 defines the use of a DPC as one possible solution to PIV-enable a mobile device. NIST SP 800-157 specifies the use of cryptographic tokens on mobile devices in which DPCs and their corresponding private keys may be used. The use of tokens with alternative form factors greatly improves the usability of electronic authentication from mobile devices to remote IT resources, while maintaining the goals of Homeland Security Presidential Directive 12 (HSPD-12)[5] for common identification that is secure, reliable, and interoperable government-wide.

This solution leverages a public key infrastructure (PKI) with credentials derived from a PIV Card. The X.509-based DPCs will be used for logical access to remote resources hosted within an on-premises data center or in the public cloud. The corresponding derived private key will be stored in a cryptographic module with an alternative form factor such as embedded hardware or software in a mobile device, or a removable token such as a Secure Digital (SD) card, Universal Integrated Circuit Card (UICC, the new generation of Subscriber Identity Module (SIM) cards), or Universal Serial Bus (USB) token.

---

[4] NIST Interagency Report (IR) 7298 Revision 2, *Glossary of Key Information Security Terms*, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[5] *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, http://www.dhs.gov/homeland-security-presidential-directive-12

2.3 DPC Requirements

This section summarizes requirements throughout the primary lifecycle activities for the DPC as described in NIST SP 800-157. To achieve interoperability with the PIV infrastructure and its applications, the solution uses PKI technology as the basis for the DPC. An X.509 public key certificate that has been issued by the Identity Management System (IDMS) 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*[6] serves as the Derived PIV Authentication certificate.

2.3.1 General Requirements

2.3.1.1 A DPC is issued for which the corresponding private key is stored in a cryptographic module that is an alternative form factor to the PIV Card.

2.3.1.2 Tokens with alternative form factors to the PIV Card that may be inserted into mobile devices, such as microSD tokens, USB tokens, UICCs, or that are embedded in the mobile or computing device, are used.

2.3.1.3 The PKI-based DPCs specified in this document are issued at levels of assurance (LOA) 3 and 4.

2.3.1.4 DPCs are based on the general concept of a derived credential in NIST SP 800-63-2, which leverages identity proofing and vetting results of current and valid credentials.

2.3.1.5 Applicant's proof of possession of a valid PIV Card is required to receive a DPC.

2.3.1.6 The Derived PIV Authentication certificate is an X.509 public key certificate 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.*

2.3.1.7 The digital signature and key management keys can be included on the mobile devices.

2.3.2 Initial Issuance Requirements

2.3.2.1 A DPC shall be issued following verification of the Applicant's identity using the PIV Authentication key on his or her existing PIV Card by demonstrating possession and control of the related PIV Card via the PKI-AUTH authentication mechanism as per Section 6.2.3.1 of FIPS 201-2.

2.3.2.2 The revocation status of the Applicant's PIV Authentication certificate should be rechecked seven calendar days following issuance of the DPC.

2.3.2.3 A DPC can be issued at identity assurance level three or four (LOA-3 or LOA-4).

2.3.2.4 An LOA-3 DPC may be issued remotely or in person, while an LOA-4 DPC is issued in-person in accordance with NIST SP 800-63-2.

2.3.2.5 If the credential is issued remotely, all communications shall be authenticated and protected from modification (e.g., using Transport Layer Security (TLS)), and encryption shall be used to protect the confidentiality of any private or secret data.

2.3.2.6 If the issuance process involves two or more electronic transactions for an LOA-3 DPC, the Applicant must identify himself/herself in each new encounter by presenting a temporary secret that was issued in a previous transaction, as described in Section 5.3.1 of NIST SP 800-63-2.

---

[6] http://www.idmanagement.gov/sites/default/files/documents/commonpolicy.pdf

2.3.2.7 The Applicant shall identify himself/herself using a biometric sample that can be verified against the Applicant's PIV Card when enrolling for an LOA-4 DPC.

2.3.2.8 If there are two or more transactions during the issuance process, the Applicant shall identify himself/herself using a biometric sample that can be verified either against the PIV Card or against a biometric that was recorded in a previous transaction when issuing an LOA-4 DPC.

2.3.2.9 If an LOA-4 credential has been issued, the issuer shall retain for future reference the biometric sample used to validate the Applicant.

2.3.2.10 NIST SP 800-157 does not preclude the issuance of multiple DPCs to the same Applicant on the basis of the same PIV Card.

2.3.3 Maintenance Requirements

2.3.3.1 When certificate re-key or modification is performed remotely for an LOA-4 DPC, communication between the issuer and the cryptographic module in which the PIV derived authentication private key is stored shall occur only over mutually authenticated secure sessions between tested and validated cryptographic modules.

2.3.3.2 When certificate re-key or modification is performed remotely for an LOA-4 DPC, data transmitted between the issuer and the cryptographic module in which the PIV derived authentication private key is stored shall be encrypted and contain data integrity checks.

2.3.3.3 The initial issuance process shall be followed for re-key of an expired or compromised DPC.

2.3.3.4 The initial issuance process shall be followed for re-key of a DPC at LOA-4 to a new hardware token.

2.3.3.5 The Derived PIV Authentication certificate shall be revoked or the token containing the corresponding private key shall be either zeroized or destroyed when any of these circumstances occurs:

2.3.3.5.1 The token containing the private key corresponding to the DPC is lost, stolen, damaged, or compromised.

2.3.3.5.2 The token containing the private key corresponding to the DPC is transferred to another individual, including when a mobile device with an embedded cryptographic module is transferred to another individual.

2.3.3.5.3 The department or agency that issued the credential determines that the Subscriber is no longer eligible to have a PIV Card (i.e., PIV Card is terminated).

2.3.3.5.4 The department or agency that issued the credential determines that the Subscriber no longer requires a DPC, even if the Subscriber's PIV Card is not being terminated. This may happen, for example, when the Subscriber's role in the agency changes such that he/she no longer has the need to access agency resources from a mobile device using a DPC.

2.3.3.6 If the Subscriber's PIV Card is reissued as a result of the Subscriber's name changing and the Subscriber's name appears in the Derived PIV Authentication certificate, a new Derived PIV Authentication certificate with the new name will also need to be issued.

2.3.4 Linkage with PIV Card Requirements

2.3.4.1 A DPC issuer shall only issue a DPC to an Applicant if the DPC issuer has access to information about the Applicant's PIV Card from the issuer of the PIV Card.

2.3.4.2 The DPC issuer shall have a mechanism to periodically check with the PIV Card issuer to determine if the PIV Card has been terminated or if information about the individual that will appear in the DPC (e.g., name) has changed, as these would require revocation or modification of the DPC.

2.3.4.3 The DPC issuer should check every 18 hours on the termination status. The periodic checking requirement can also be met if:

2.3.4.3.1 A notification mechanism is in place between the PIV Card issuer and the DPC issuer, or

2.3.4.3.2 The PIV Card record and the DPC record are stored in the same system and termination of the PIV Card automatically triggers termination of the DPC.

2.3.4.4 The issuer of the DPC shall not solely rely on tracking the revocation status of the PIV Authentication certificate as a means of tracking the termination status of the PIV Card.

2.3.4.5 Additional methods must be employed for obtaining information about the PIV Card from the PIV Card issuer such as:

2.3.4.5.1 If the DPC is issued by the same agency or issuer that issued the Subscriber's PIV Card, then the DPC issuer may have direct access to the IDMS database implemented by the issuing agency that contains the relevant information about the Subscriber.

2.3.4.5.2 When the issuer of the DPC is different from the PIV Card Issuer, the following mechanisms may be applied:

2.3.4.5.2.1 The Backend Attribute Exchange (BAE) can be queried for the termination status of the PIV Card, if an attribute providing this information is defined and the issuer of the PIV Card maintains this attribute for the Subscriber. The BAE can also be queried for other attributes about the Subscriber (e.g., name) that may appear in the Derived PIV Authentication certificate.

2.3.4.5.2.2 The issuer of the DPC notifies the original PIV issuer when a DPC is created. The issuer of the PIV Card maintains a list of corresponding DPC issuers and sends notification to the latter set when the PIV Card is terminated or when attributes about the cardholder change. Such notification should provide evidence of receipt and the integrity of the message.

2.3.4.5.2.3 If a Uniform Reliability and Revocation Service (URRS) is implemented in accordance with Section 3.7 of NIST Interagency Report (IR) 7817[7], the issuer of a DPC may obtain termination status of the Subscriber's PIV Card through the URRS.

[7] *A Credential Reliability and Revocation Model for Federated Identities*, http://dx.doi.org/10.6028/NIST.IR.7817

2.3.5 Technical Requirements

2.3.5.1 Certificate Policies

2.3.5.1.1 Derived PIV Authentication certificates shall be issued under either the id-fpki-common-pivAuth-derived-hardware (LOA-4) or the id-fpki-common-pivAuth-derived (LOA-3) policy of the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*.

2.3.5.1.2 The Derived PIV Authentication certificate shall comply with Worksheet 10: Derived PIV Authentication Certificate Profile found in *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program*.[8]

2.3.5.1.3 The expiration date of the Derived PIV Authentication certificate is based on the certificate policy of the issuer. There is no requirement to align the expiration date of the Derived PIV Authentication certificate with the expiration date of the PIV Authentication certificate or the expiration of the PIV Card; however, in many cases aligning the expiration dates will simplify lifecycle management.

2.3.5.2 Cryptographic Specifications

2.3.5.2.1 The cryptographic algorithm and key size requirements for the Derived PIV Authentication certificate and private key are the same as the requirements for the PIV Authentication certificate and private key, as specified in NIST SP 800-78-4.[9]

2.3.5.2.2 For Derived PIV Authentication certificates issued under id-fpki-common-pivAuth-derived-hardware (LOA-4), the Derived PIV Authentication key pair shall be generated within a hardware cryptographic module that has been validated to FIPS 140-2[10] Level 2 or higher that provides Level 3 physical security to protect the Derived PIV Authentication private key while in storage and that does not permit exportation of the private key.

2.3.5.2.3 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 140-2 Level 1 or higher.

2.3.5.3 Cryptographic Token Types

2.3.5.3.1 Removable (Non-Embedded) Hardware Cryptographic Tokens

2.3.5.3.1.1 A Derived PIV Application shall be installed on the hardware cryptographic token. The use of this data model and its interface supports interoperability and ensures the DPC interface is aligned with the interface of the PIV Card.

---

8 http://idmanagement.gov/sites/default/files/documents/CertCRLprofileForCP.pdf

9 *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, http://dx.doi.org/10.6028/NIST.SP.800-78-4

10 *Security Requirements for Cryptographic Modules*, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

2.3.5.3.1.2 The form factor supports a secure element (SE), a tamper-resistant cryptographic component that provides security and confidentiality.

2.3.5.3.1.3 The Application Protocol Data Units (APDUs) for the Derived PIV Application command interface specified in Appendix B of NIST SP 800-157 are transported to the secure element within each form factor over a transport protocol appropriate for that form factor.

2.3.5.3.1.4 As described in Appendix B of NIST SP 800-157, the Derived PIV Application may include digital signature and key management private keys and their corresponding certificates in addition to the Derived PIV Authentication private key and its corresponding certificate.

2.3.5.3.1.5 SD Card with Cryptographic Module

2.3.5.3.1.5.1 A Derived PIV Application may reside on an SD Card implementation that includes an on-board secure element or security system.

2.3.5.3.1.5.2 The secure element used for the Derived PIV Application shall support an interface with the card commands specified in Appendix B of NIST SP 800-157.

2.3.5.3.1.6 Removable UICC with Cryptographic Module

2.3.5.3.1.6.1 The Derived PIV Application shall be installed in a security domain that is separate from other security domains, dedicated to the DPC, and under the explicit control of the issuing agency.

2.3.5.3.1.6.2 The APDUs as specified in Appendix B of NIST SP 800-157 shall be used with this secure element containing the PIV Derived Application.

2.3.5.3.1.6.3 A UICC used to host a DPC shall implement the *GlobalPlatform Card Secure Element Configuration v1.0*.[11]

2.3.5.3.1.7 USB Token with Cryptographic Module

2.3.5.3.1.7.1 USB token implementations called USB Integrated Circuit(s) Card Devices (ICCDs) that contain an integrated secure element (an Integrated Circuit Card or ICC) are suitable for issuance of DPCs and comply with the *Universal Serial Bus Device Class: Smart Card ICCD Specification for USB Integrated Circuit(s) Card Devices*.[12]

[11] https://www.globalplatform.org/specificationscard.asp
[12] http://www.usb.org/developers/docs/devclass_docs/DWG_Smart-Card_USB-ICC_ICCD_rev10.pdf

2.3.5.3.1.7.2 The APDUs for the Derived PIV Application as specified in Appendix B of NIST SP 800-157 shall be transported to the secure element using the Bulk-Out command pipe, and the responses shall be received from the secure element using the Bulk-In command pipe.

2.3.5.3.1.7.3 USB tokens with cryptographic modules that support a Derived PIV Application shall also be compliant with the specifications in NIST SP 800-96[13] for APDU support for contact card readers.

2.3.5.3.2 Embedded Cryptographic Tokens

2.3.5.3.2.1 A DPC and its associated private key may be used in cryptographic modules that are embedded within mobile devices which may either be in the form of a hardware cryptographic module that is a component of the mobile device or in the form of a software cryptographic module that runs on the device.

2.3.5.3.2.2 Software-based DPCs cannot be issued at LOA-4.

2.3.5.3.2.3 A hybrid approach where the key is stored in hardware, but a software cryptographic module uses the key during an authentication operation, constitutes an LOA-3 solution.

2.3.5.3.2.4 The cryptographic module shall satisfy the requirements for certificates issued under either id-fpki-common-pivAuth-derived-hardware or id-fpki-common-pivAuth-derived.

2.3.5.3.2.5 These same cryptographic modules may also hold other keys, such as digital signature and key management private keys and their corresponding certificates.

2.3.5.4 Activation Data

2.3.5.4.1 Use of the Derived PIV Authentication private key, or access to the plaintext or wrapped private key, shall be blocked prior to password-based Subscriber authentication.

2.3.5.4.2 The password should not be easily guessable or otherwise individually identifiable in nature (e.g., part of a Social Security Number, phone number).

2.3.5.4.3 The required password length shall be a minimum of six characters.

2.3.5.4.4 There shall be a mechanism to block use of the Derived PIV Authentication private key after a number of consecutive failed activation attempts as stipulated by the department or agency.

2.3.5.4.5 Throttling mechanisms may be used to limit the number of attempts that may be performed over a given period of time.

[13] *PIV Card to Reader Interoperability Guidelines,* http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf

2.3.5.4.6 For embedded tokens at LOA-3, the authentication mechanism may be implemented by hardware or software mechanisms outside the boundary of the cryptographic module, provided that the strength of the authentication mechanism meets the requirements specified above.

2.3.5.4.7 For removable tokens, or embedded tokens at LOA-4, the authentication mechanism shall be implemented and enforced by the cryptographic module itself.

2.3.5.4.8 When password reset is performed in-person at the issuer's facility, or at an unattended kiosk operated by the issuer, it shall be implemented through one of the following processes:

2.3.5.4.8.1 The Subscriber’s PIV Card shall be used to authenticate the Subscriber (via PKI-AUTH mechanism as per Section 6.2.3.1 of FIPS 201-2) prior to password reset. The issuer shall verify that the DPC is for the same Subscriber that authenticated using the PIV Card.

2.3.5.4.8.2 A 1:1 biometric match shall be performed against the biometric sample retained during initial issuance of the DPC, a stored biometric on the PIV Card, or biometric data stored in the chain-of-trust as specified in FIPS 201-2. The issuer shall verify that the DPC is for the same Subscriber for whom the biometric match was completed.

2.3.5.4.9 When password reset is performed remotely, it shall follow the following processes:

2.3.5.4.9.1 The Subscriber’s PIV Card shall be used to authenticate the Subscriber (via PKI-AUTH authentication mechanism as per Section 6.2.3.1 of FIPS 201-2) prior to password reset.

2.3.5.4.9.2 If the reset occurs over a session that is separate from the session over which the PKI-AUTH authentication mechanism was completed, strong linkage (e.g., using a temporary secret) must be established between the two sessions.

2.3.5.4.9.3 The issuer shall verify that the DPC is for the same Subscriber that authenticated using the PIV Card.

2.3.5.4.9.4 The remote password reset shall be completed over a protected session (e.g., using TLS).

2.3.5.4.10 Removable hardware tokens shall support the password reset functionality as per Appendix B of NIST SP 800-157 and support for password reset is not required at LOA-3, and implementations may instead choose to issue a new certificate following the initial issuance process if the password is forgotten.

3 Usage Scenarios

A usage scenario is the practical way in which users interact with components of a system and how they function together. This section describes two usage scenarios. These scenarios provide the same functions from a user interaction perspective; the differentiator is where the originating PIV credential is issued. In the first usage scenario, both the PIV credential and the DPC are issued from the same internal enterprise IDMS and medium assurance PKI. In the second usage scenario, the PIV credential is issued from an external trusted shared service provider and the DPC is issued from a disparate IDMS and PKI.

The rest of this section describes the following usage scenarios:

- Organization-provisioned PIV credentials and associated DPCs are issued using an enterprise IDMS and PKI (Section 3.1)
- Shared Service Provider-provisioned PIV credentials and associated DPCs are issued using a different IDMS and PKI (Section 3.2)

3.1 Organization-Provisioned PIV Credentials Usage Scenario

Traditionally, organizations provision PIV credentials to their employees, contractors, and other logical access users based upon the Applicant's corresponding identity record within an enterprise IDMS and PKI. In this scenario, the organization is deploying modern client devices such as smartphones, tablets, and ultra-lightweight general purpose computing devices that do not have built-in or contactless PIV Card readers. However, these devices provide an embedded hardware token or software token that supports DPCs. In addition, the enterprise IDMS and medium assurance PKI are capable of supporting the issuance, use, maintenance, and termination of X.509-based DPCs. The DPCs are used to authenticate and access remote resources hosted within an on-premises data center or in a public cloud, as well as to sign and encrypt email on the client device.

3.1.1 Workflow

An employee who has been through the PIV identity proofing process and possesses a valid PIV credential is eligible for a DPC. The employee requires a mobile device for work. The mobile device with a cryptographic module is ordered and a request for the issuance of a DPC is submitted to the agency's approval authority. Multiple DPCs can be issued to the same employee on the basis of the same PIV Card. Once the employee has received the device and the request has been approved, the employee starts the issuance process.

If the credential being issued is at an LOA-4, the issuance process must occur in person and include a biometric match to the employee's PIV credential. The biometric sample used for verification must be retained for future reference. The issuance process of an LOA-3 credential may happen remotely and does not require a biometric match. LOA-3 issuance may be initiated remotely by an entity operated by a Registration Authority (RA) associated with the Certificate Authority (CA) that will issue the DPC. The process of enrollment requires protected communications between all required components. The Applicant must show proof of possession of the PIV Client Authentication certificate by entering the PIN for his or her PIV Card. Since

the employee cannot use the PIV Card with the mobile device, the employee performs this step from a known and trusted computer.

By requiring the use of the PIV Client Authentication certificate when connecting to the Credential Management System (CMS), the server not only authenticates the Applicant, but also verifies that the Applicant is still eligible to possess a PIV credential. The revocation status of the employee's PIV authentication certificate must also be checked seven calendar days following issuance of the DPC. This check prevents the issuance of DPCs from a stolen or compromised PIV credential.

After proving PIV eligibility, the DPC issuance process is initiated. The CMS communicates with the PKI's DPC CA to request the X.509 Derived PIV Client Authentication certificate and the optional signing and encryption certificates. The CA issues the requested certificates and the CMS provisions the certificate(s) to the device that is requesting the credential. The specific workflow for credential collection will differ depending on the organization's specific technology choices, policies, and processes. The employee might need to visit a self-collection station, browse to a TLS-enabled mobile website, or possibly use a mobile application to collect the DPC.

If the collection process requires more than two interactive sessions, a job-associating identifier is required. The identifier is dependent upon the level of assurance the DPC will assert.

Figure 1 depicts a notional DPC enrollment and issuance workflow.

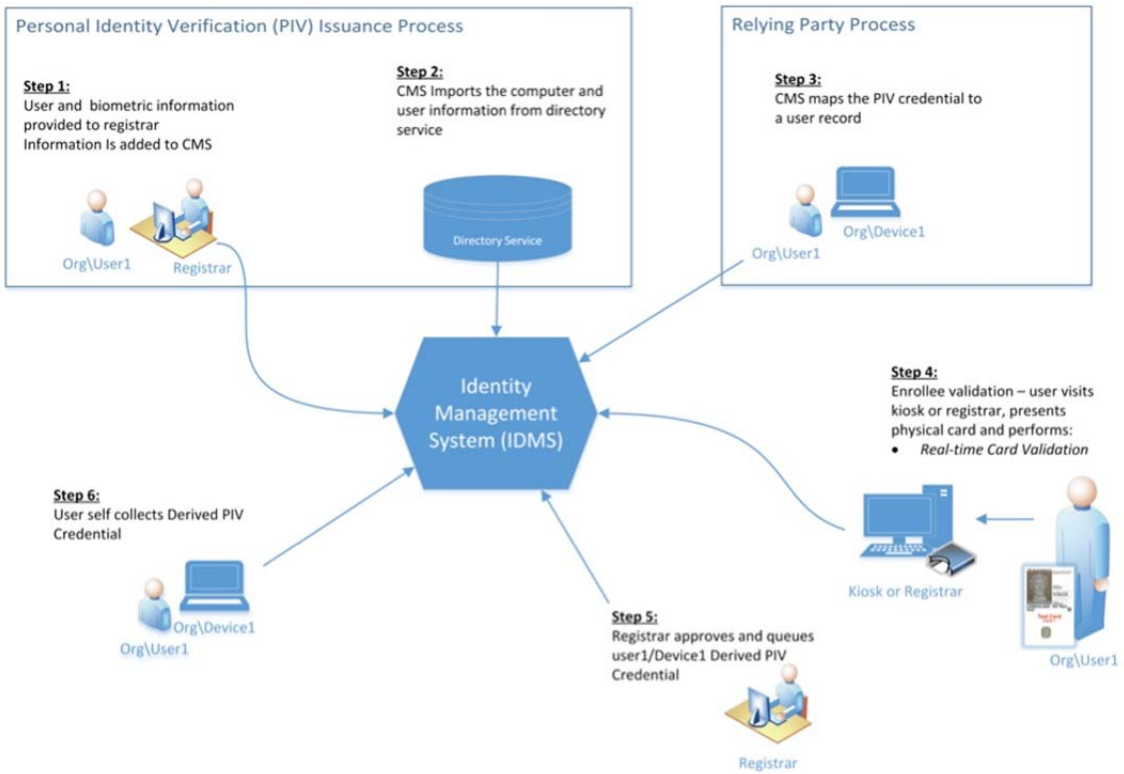


Figure 1: Enrollment and Issuance Workflow

3.1.2 Lifecycle Management

The DPC is a separate credential from the PIV Card but only remains valid if the PIV Card it was based upon remains un-terminated. Like any other credential used for authentication and authorization, it requires maintenance and lifecycle management functions. Throughout the lifetime of a Subscriber's DPC a number of events may occur that will trigger a lifecycle management function to take place. The events that can cause these can range from a Subscriber's name change to the compromise of a DPC. Table 1 describes events that occur during the life of a DPC and the corresponding actions required to address these events.

Table 1: Lifecycle Management Functions

Event	Action Required
Cardholder name change and reissued PIV credential	Reissue DPC certificates
Credential is compromised	Issuance process
Credential expired / re-key	Issuance process
Token containing private key is lost	Zeroized/Destroyed/Revocation
Token containing private key is issued to different employee	Zeroized/Destroyed/Revocation
Subscriber no longer eligible to have PIV Card	Zeroized/Destroyed/Revocation
Subscriber no longer requires DPC	Zeroized/Destroyed/Revocation

Figure 2 shows the relationship between the lifecycle for PIV and DPC, and in particular there is only direct linkage for the reissuance and termination of the PIV card.

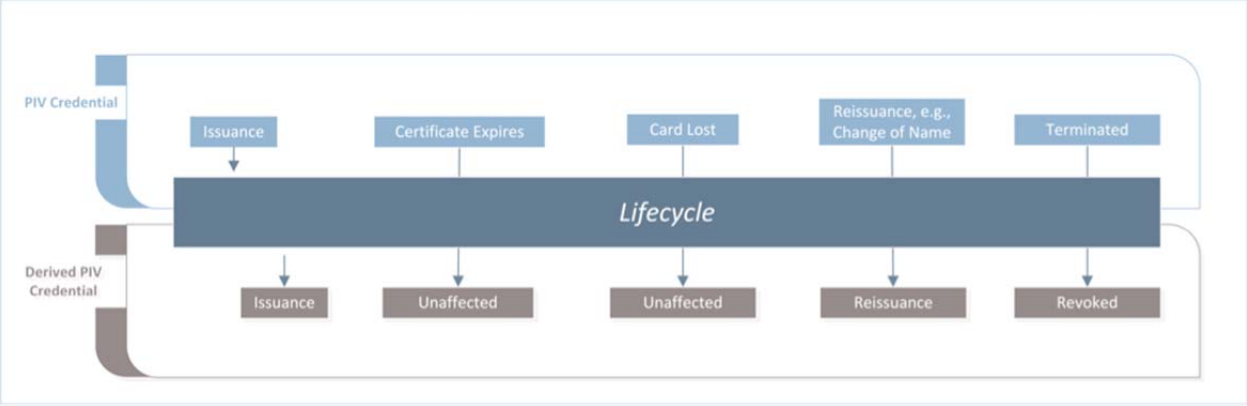


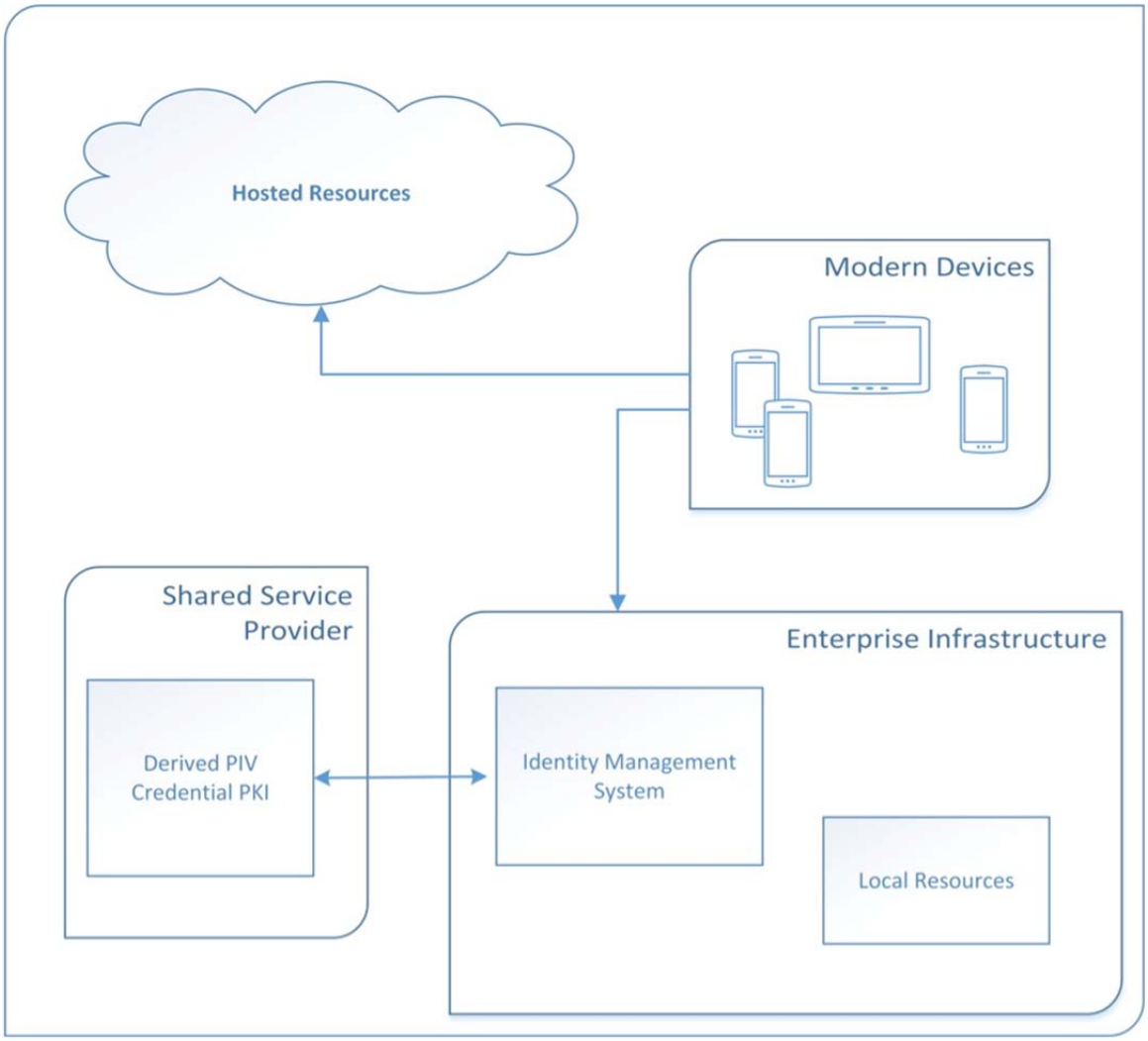
Figure 2: PIV and DPC Lifecycle

3.1.3 Proposed Architecture

The use of DPCs requires enterprise infrastructure to support issuance, usage, maintenance, and termination activities. This usage scenario makes the following assumptions:

- Organization is using an enterprise IDMS
- Organization has a medium assurance PKI that is allowed to issued DPCs
- The resources are hosted in the cloud and the enterprise data center

689 The organization's internal PIV IDMS is capable of issuing and maintaining DPCs to modern
690 devices with form factors that do not support the use of a physical PIV Card. The enterprise PKI
691 needs to be expanded upon to include additional subordinate CAs. These new CAs will support
692 the issuance of DPCs at different LOAs in accordance with NIST SP 800-63-2. Additional
693 infrastructure will be required to support the self-collection of DPCs. Specific resources may
694 differ depending on the organization's technology choices, policies, and processes, but could
695 include additional application servers, mobile applications, physical self-collection stations, etc.
696 Figure 3 summarizes the components that are required to support the usage scenario.



697
698 **Figure 3: Scenario 1 Proposed Architecture**

699 ### 3.2 Shared Service Provider-Provisioned PIV Credentials Usage Scenario

700 In this scenario, an organization wants to leverage Shared Service Provider (SSP) provisioned
701 PIV credentials to generate DPCs to be used on various computing devices. A local CMS system
702 and PKI support the issuance, use, maintenance, and termination of the X.509-based DPCs.
703 Before the issuance of the DPCs can occur, the local IDMS needs to verify the validity of the
704 employee's PIV credential. The requirement to verify the validity of an Applicant's PIV Card

introduces the need for the local IDMS to have a communication channel to the shared provider. This communication between local IDMS and service provider must also provide a way to notify the local IDMS of a PIV credential event such as PIV termination.

In this usage scenario, there is a secure channel of communication between the enterprise IDMS and the SSP's IDMS. Figure 4 illustrates the additional infrastructure required for issuing DPCs based on an SSP-issued PIV.

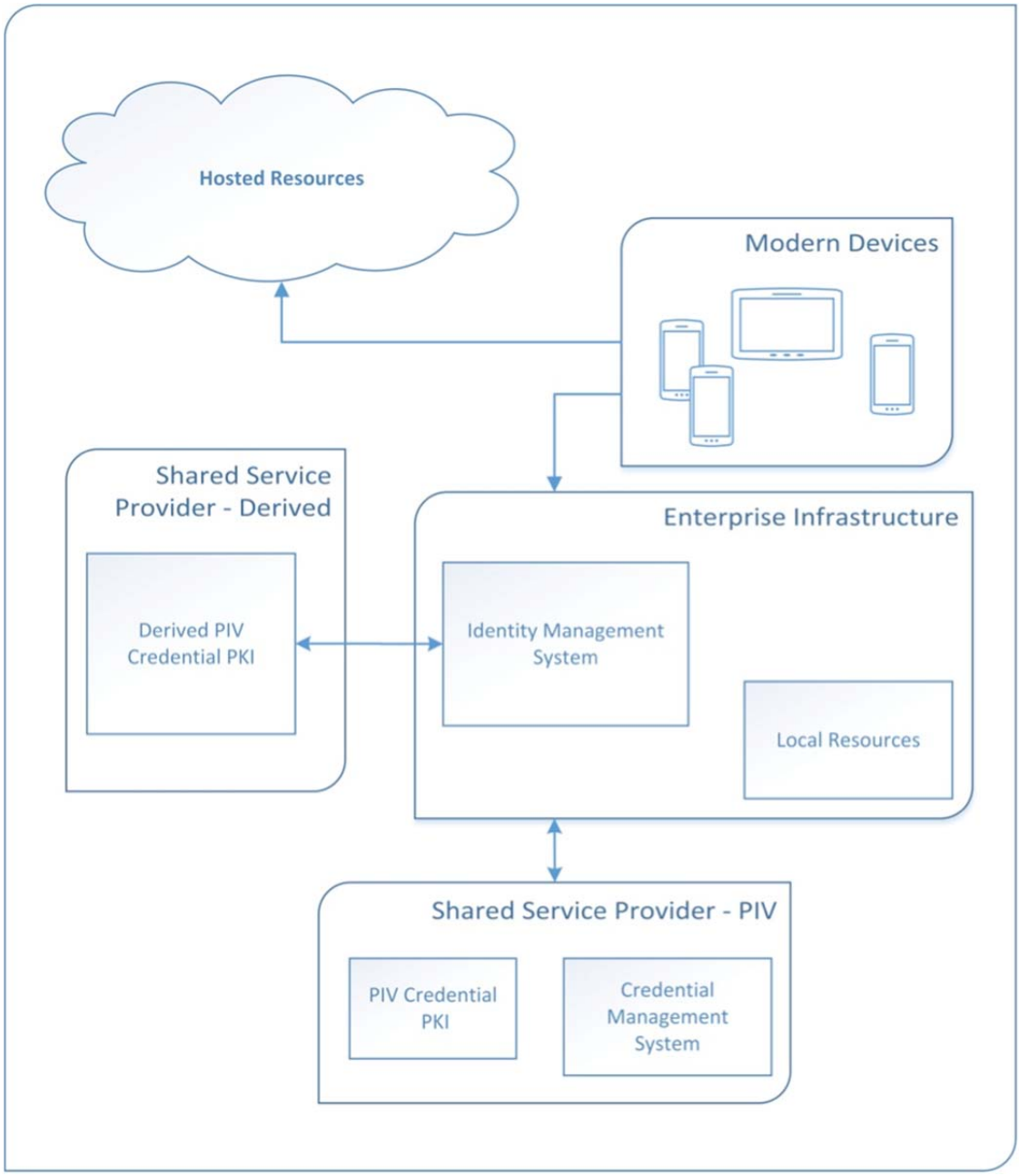


Figure 4: Scenario 2 Proposed Architecture

4 POC Research for Organization-Provisioned PIV Credentials

This section explains the application of Microsoft and Intercede technologies in accordance with NIST SP 800-157 to support the organization-provisioned PIV credentials usage scenario. Microsoft technologies provide the identity store, mobile devices, supporting infrastructure, and applications. Intercede MyID, which is a FIPS 201-compliant identity and credential management system that adheres to the NIST SP 800-157 specifications, is used as a CMS. The Intercede MyID Credential Management System is part of the overall IDMS referred to in NIST SP 800-157. This section focuses on the issuance, usage, maintenance, and termination of LOA-3 credentials based upon the guidance of NIST SPs 800-157 and 800-63-2, as well as industry-available technologies. Both hardware and software cryptographic modules are used to protect the private key of the DPC.

4.1 Enterprise Infrastructure

A cloud-based prototypical environment was developed for the purpose of verifying technology interoperability for this research. The instantiation of this environment has been configured as a tenant within the Microsoft Azure Government (MAG) Infrastructure as a Service (IaaS)[14]. The use of cloud-based infrastructure was chosen for its highly available, collaborative environment. This environment can be deployed in other cloud-based IaaS environments.

The cloud-based infrastructure serves as the identity domain for the users that are issued PIV credentials and DPCs. These users are within the DerivedPIVCredentials.com domain name space (e.g., user1@DerivedPIVCredentials.com). The applications that the users will access are the cloud-based Microsoft Office 365 Enterprise E3 services.[15] Users will be provisioned DPCs to their mobile devices. The user authenticates to the DerivedPIVCredentials.com Active Directory (AD) domain using his or her X.509-based DPC. Figure 5 describes the core components of the IaaS architecture.

[14] http://azure.microsoft.com/en-us/features/gov/
[15] http://products.office.com/en-us/business/office-365-enterprise-e3-business-software

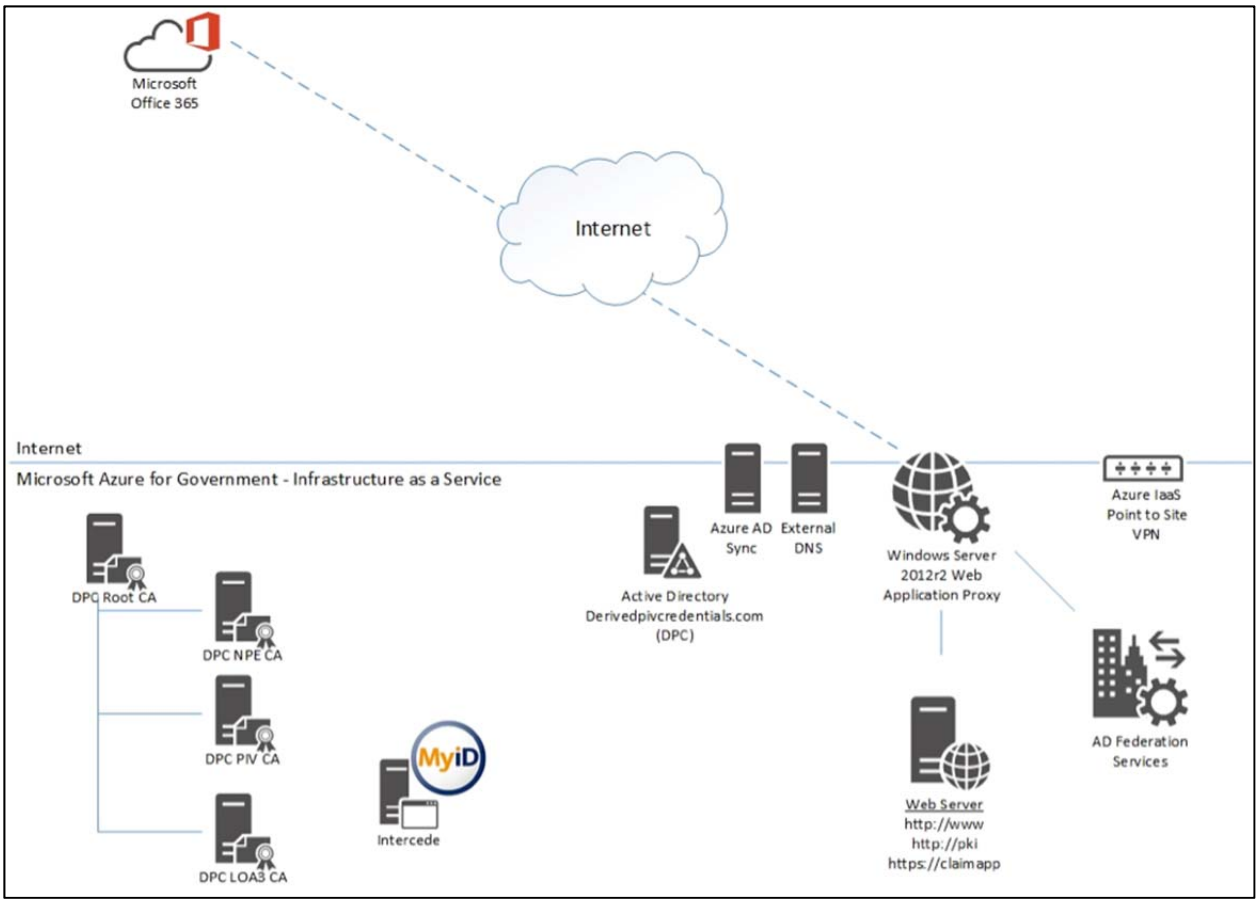


Figure 5: Architecture Core Components

4.2 DerivedPIVCredentials.com Identities

Figure 6 depicts the user identity store (AD) used in this research.

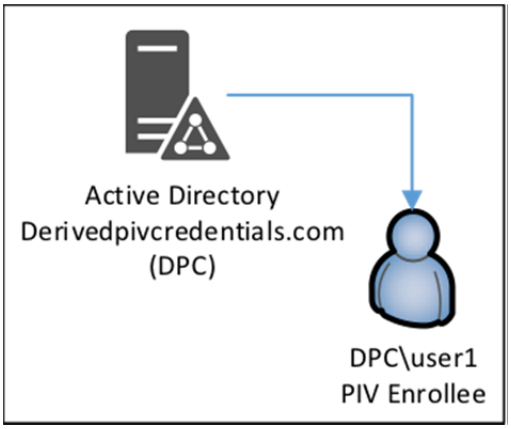


Figure 6: Active Directory User Identities

744 Microsoft Windows Server 2012R2 Active Directory Domain Services (ADDS) serves as the
745 central user identity store and is the Key Distribution Center (KDC) for the
746 DerivedPIVCredentials.com domain's Kerberos realm. Kerberos communication is enabled
747 between all the servers within the same Azure IaaS Virtual Network (VNet)[16]. This network is
748 not exposed to the Internet. The PIV and Derived PIV Subscribers must have user accounts
749 within this AD domain. The AD domain controller performs the X.509 chaining and validation
750 of the PIV and Derived PIV Client Authentication certificate used for Kerberos authentication.[17]
751 The ADDS role is enabled on two MAG virtual machines running within a single Azure IaaS
752 Cloud Service.[18] This provides high availability for the AD service.

753 The users' identities are synchronized to the associated Azure AD tenant using the Azure Active
754 Directory Synchronization[19] engine. The users' passwords are not synchronized to Azure AD
755 and are explained further in the following sections. Office 365 uses these identities to assign
756 services (e.g., email, OneDrive, SharePoint Online, Skype for Business) to users. Only the Office
757 365-required attributes[20] are synchronized to the associated Azure AD tenant. Figure 7 depicts
758 the identity synchronization with Office 365.

16 https://msdn.microsoft.com/en-us/library/azure/jj156007.aspx
17 http://www.microsoft.com/en-us/download/details.aspx?id=9427
18 http://azure.microsoft.com/en-us/documentation/services/cloud-services/
19 http://www.microsoft.com/en-us/download/details.aspx?id=44225
20 http://social.technet.microsoft.com/wiki/contents/articles/19901.dirsync-list-of-attributes-that-are-synced-by-the-azure-active-directory-sync-tool.aspx

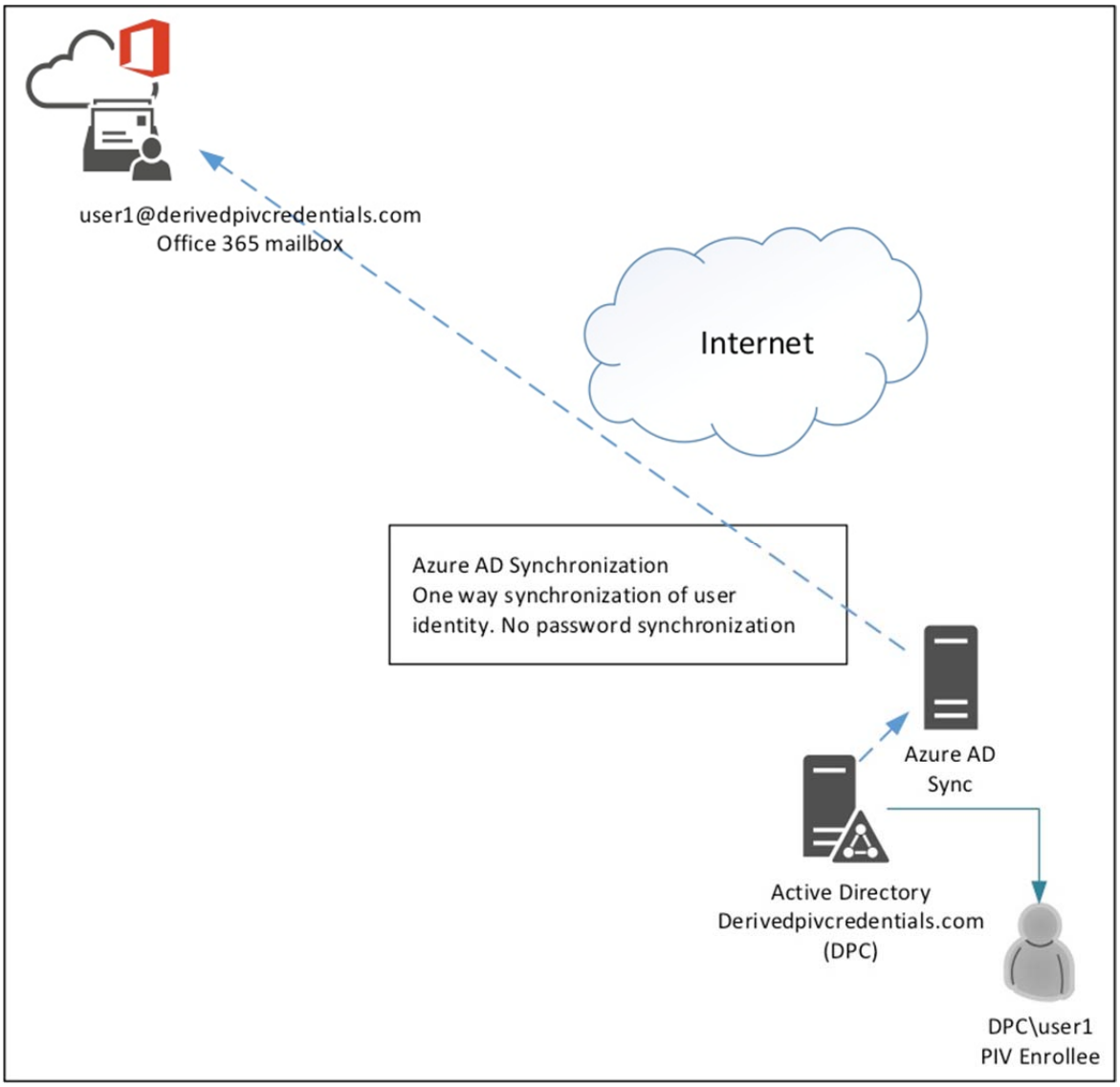
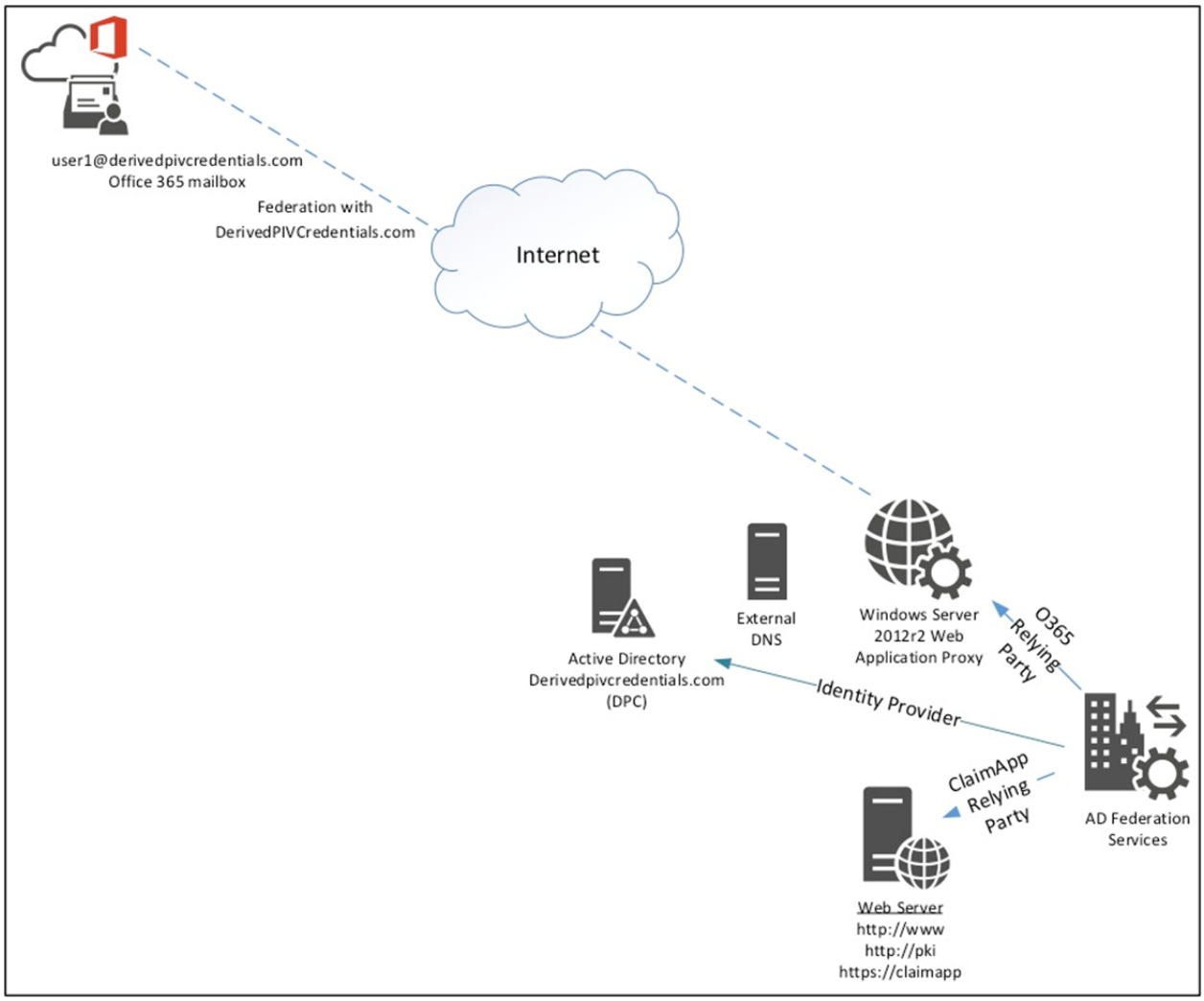


Figure 7: Office 365 Identity Synchronization

4.3 Remote Services and Federation

Figure 8 represents the remote service and federation architecture. Microsoft Office 365, relying party, will provide the services, which the mobile users will access using their PIV and DPC X.509-based credentials. NIST SP 800-157 states, “The scope of the Derived PIV Credential is to provide PIV-enabled authentication services on the mobile device to authenticate the credential holder to remote systems.” Authentication (validation of X.509 credential and account mapping) occurs within the IaaS-based DerivedPIVCredentials.com AD domain. The DerivedPIVCredentials.com Office 365 tenant will be federated with the IaaS-based Active Directory Federation Services (ADFS) serving as the Identity Provider (IdP) for the DerivedPIVCredentials.com domain. The Azure AD Synchronization service is configured not to synchronize the users’ AD passwords. DerivedPIVCredentials.com is registered as a federated,

773 custom domain. All user authentication occurs at the IaaS-based DerivedPIVCredentials.com AD
774 domain via ADFS.



775

776 **Figure 8: Federation Architecture**

777 The ADFS service is provided by two Windows Server 2012R2 virtual machines with the ADFS
778 role enabled within an Azure IaaS cloud service. These virtual machines are connected to the
779 same VNet as the DerivedPIVCredentials.com domain controllers since Kerberos
780 communication is required between the ADFS and ADDS servers. External communication to
781 the ADFS service is provided by two Windows Server 2012R2 virtual machines in a single
782 Azure IaaS cloud service running the Routing and Remote Access Service (RRAS), Web
783 Application Proxy (WAP) role. These virtual machines are not domain joined and are attached to
784 a separate VNet. X.509 authentication to the ADFS/WAP IdP service uses the TLS Client Key
785 Exchange / CertificateVerify[21] method.

[21] http://tools.ietf.org/html/rfc5246#section-7.4.8

786 The DerivedPIVCredentials.com Domain Name System (DNS) is configured as a "split DNS."
787 External name queries are sent to the external DNS server and internal DNS queries are handled
788 by the ADDS-integrated DNS servers. Split DNS is a common technique employed to be able to
789 represent a single namespace as different source IP addresses (internal versus external) for client
790 requests that redirect to the federation endpoint for authentication.

791 A sample federation claims application[22] is configured on the "web server" (Internet Information
792 Services, IIS 8) to render the claims that are generated by the ADFS service. This ASP.NET
793 application is associated with the ADFS server as a relying party and displays the Security
794 Assertion Markup Language (SAML) token created by the ADFS service to the user's web page.
795 This application will be used to demonstrate the ability to determine which credential the user
796 authenticated with and provide a level of authentication assurance.

797 ### 4.4 PKI

798 The PKI used to support the DerivedPIVCredentials.com environment, as shown in Figure 9, is
799 based upon the Windows Server 2012R2 Active Directory Certificate Services (ADCS) role.
800 Three issuing CAs are used to issue PIV, Derived PIV, and non-person entity (NPE) certificates.
801 These issuing CAs are subordinate to the DPC Root CA. The CRLs and certificates required for
802 chain building and validation are publicly available.[23] The DPC NPE CA is used to issue non-
803 person end entity certificates to support the DerivedPIVCredentials.com environment (e.g.,
804 domain controller certificates). The DPC PIV CA issues the PIV Cards' certificates. The DPC
805 LOA-3 CA issues the DPC's certificates for the users' mobile device DPCs. This report only
806 focuses on the issuance, usage, and maintenance of an LOA-3 DPC. The test Object Identity
807 (OID), 2.16.840.1.101.3.2.1.48.173[24], is the id-fpki-common-pivAuth-derived identifier within
808 the certificate's CertificatePolicy extension to identify the Derived PIV Authentication
809 certificate. Since this is a demonstration environment, these certificates do not chain to the
810 Federal Common Policy CA as would a valid DPC certificate.

811

[22] http://technet.microsoft.com/en-us/library/dn280943.aspx
[23] http://pki.derivedpivcredentials.com/crlstatus.htm
[24] http://csrc.nist.gov/groups/ST/crypto_apps_infra/csor/pki_registration.html

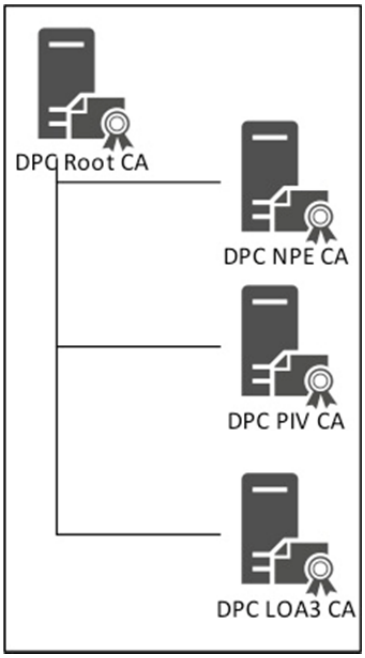


Figure 9: Public Key Infrastructure

NIST SP 800-157 does not specify the operational architecture of the supporting PKI. For this report, the issuance of the id-fpki-common-pivAuth-derived and id-fpki-common-common-authentication certificates is performed by separate issuing CAs. It is likely that HSPD-12 SSPs will stand up new CAs for the issuance of DPCs to avoid certificate reissuance of existing SSP CAs to include the id-fpki-common-pivAuth-derived and id-fpki-common-pivAuth-derived-hardware OIDs, and to minimize the potential growth of the CRLs due to NIST SP 800-157 termination requirements.

The End Entity Signature certificate (i.e., digital signature) will be issued for DPC LOA-3 CA to demonstrate Secure/Multipurpose Internet Mail Extensions (S/MIME) capabilities with the Office 365 email system. Refer to *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program* for the certificate formats.

4.5 Intercede MyID FIPS 201 CMS

Intercede MyID CMS, as shown in Figure 10, is a commercially available product that comes out of the box configured to be FIPS 201 compliant. As the FIPS 201 standard evolves, MyID's functionality has been enhanced to include issuance of DPCs to a range of mobile device platforms. In this scenario, MyID performs the entire lifecycle of the PIV credential, including PIV identity verification, credential issuance, and lifecycle management and termination workflows. The MyID self-service kiosk guides Applicants through the DPC issuance processes. Within the DerivedPIVCredential.com domain, MyID issues the Applicant's PIV Card, so the CMS already has a vetted identity record on which to base the request for the DPC. NIST SP 800-157 Section 2.4 discusses associating a DPC issued by an agency that is linked to a PIV identity from another agency. This capability is available with MyID but will not be included within this research.

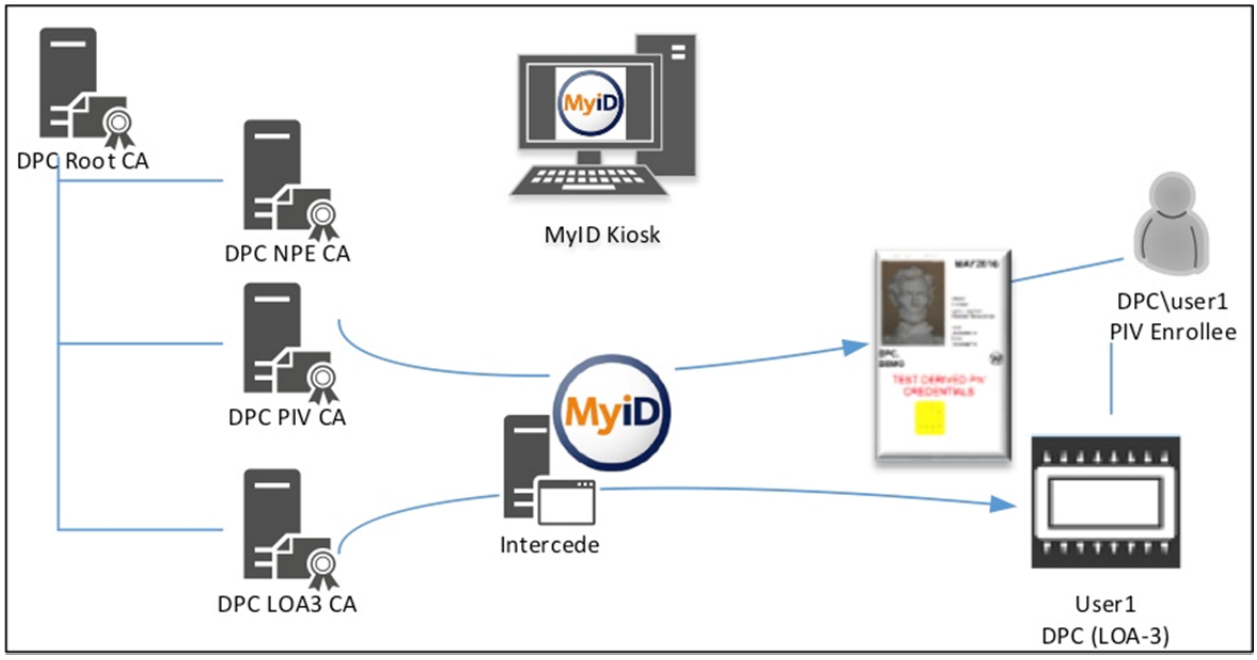


Figure 10: Intercede MyID CMS

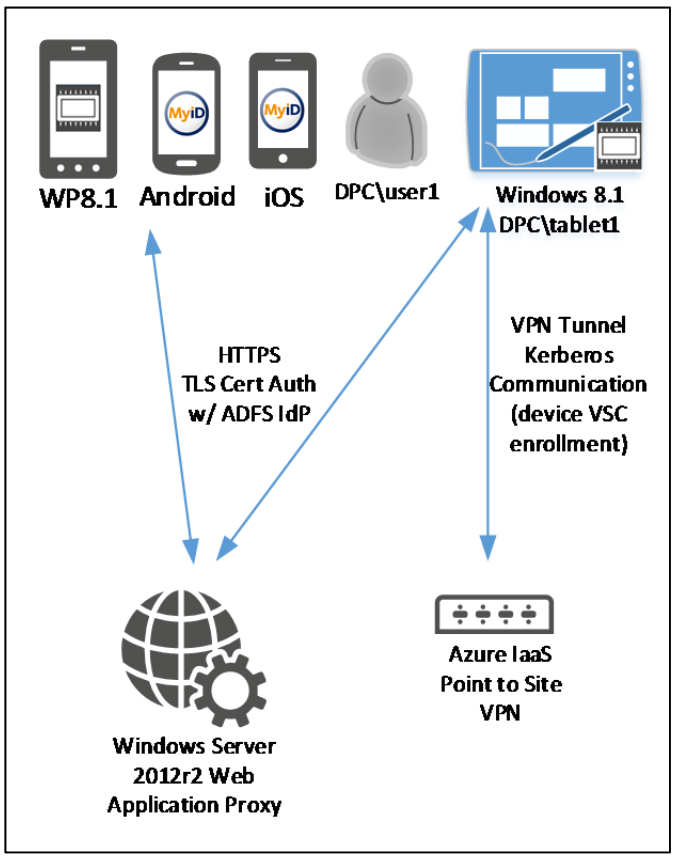
4.6 Mobile Devices

Figure 11 represents the various mobile devices used in the research. Starting with Windows 8, Microsoft introduced the Virtual Smart Card[25] (VSC) technology to emulate the functionality of traditional X.509-based smart cards. The Microsoft VSC platform utilizes the Trusted Platform Module[26] (TPM) chip onboard most modern computers. Windows 10 will include the VSC technology and it will support all the features described in this document. Windows 10 will introduce the Hello and Passport[27] features that further expand the VSC technology. The DPCs used within this research will be Virtual Smart Cards on the Windows 8.1 and Windows Phone 8.1 platforms. A tablet computer running the Windows 8.1 operating system (OS) is joined to the DerivedPIVCredentials.com domain. The domain-joined Windows 8.1 tablet communicates to the DerivedPIVCredentials.com AD domain via the Azure IaaS Point to Site Virtual Private Network (VPN).[28] MyID will perform VSC issuance via this VPN tunnel for domain-joined devices. An established VPN will demonstrate the usage of a DPC internal to the organizational IT boundaries (e.g., desktop logon). When the tablet is not connected via VPN to DerivedPIVCredentials.com, authentication and access will be provided via the ADFS/WAP federation service. When the workstation is unable to perform Kerberos-based communication with the DerivedPIVCredentials.com AD domain, the VSC desktop logon access utilizes the cached credentials Windows feature.

---

[25] http://www.microsoft.com/en-us/download/details.aspx?id=29076
[26] http://www.trustedcomputinggroup.org/developers/trusted_platform_module
[27] http://blogs.windows.com/bloggingwindows/2015/03/17/making-windows-10-more-personal-and-more-secure-with-windows-hello/
[28] https://msdn.microsoft.com/en-us/library/azure/dn133798.aspx

858



859 **Figure 11: Mobile Devices**

860 The Microsoft Windows Phone 8.1 includes the TPM and the Windows 8 VSC technology. The
861 Windows Phone is a DPC container to be used for VPN authentication, ADFS X.509
862 authentication (TLS CertificateVerify), and digital signature S/MIME. The Windows Phone 8.1
863 used in this research is a Nokia Lumia 920 running Windows 8.1 (OS version 8.10.14219341).
864 The Intercede MyID Windows Phone applet is required for the enrollment, maintenance, and
865 termination of the phone-based credential. The Intercede MyID Identity Agent application is
866 available in the Windows Phone Store. Once the DPC is issued to the Windows Phone 8.1
867 device, the Virtual Smart Card behaves similarly to the Windows 8.1 VSC and physical smart
868 card.

869 The Android v4.4.2 and iOS v7.x and above mobile devices use the MyID Identity Agent to
870 provide the cryptographic module that generates and protects the DPC.

871 The most current version of the MyID Identity Agent should be installed from the platform-
872 respective official App Store or Market Place.

4.7 DerivedPIVCredentials.com Environment

Figure 12 depicts all the components of the test environment previously described:

- Identity store – AD
- DPC issuance – MyID
- PKI – ADCS
- Mobile devices – Windows, iOS, and Android
- Cloud-based resources – Office 365
- Federation – ADFS

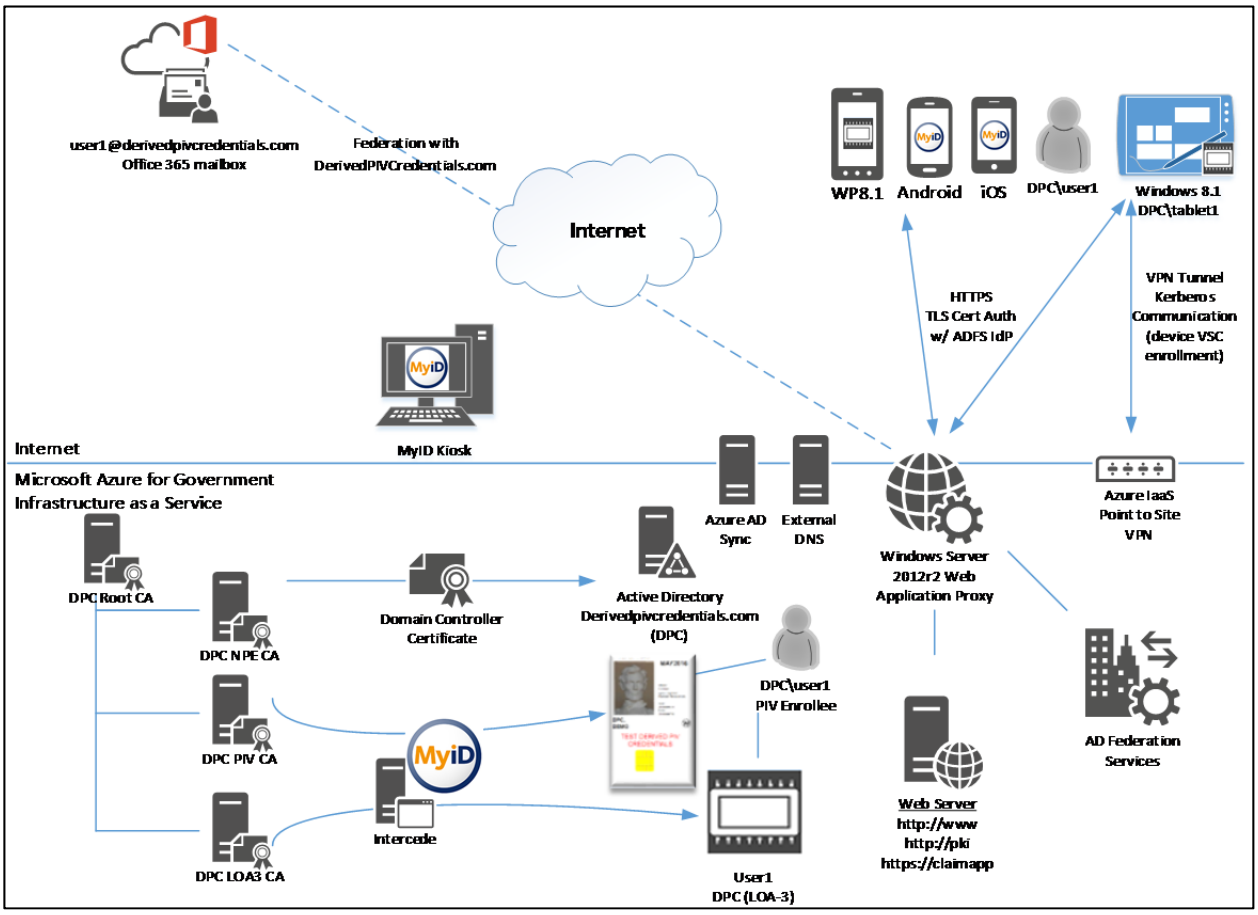


Figure 12: Complete Architecture of the research

4.8 Implementation Capabilities

This section describes the technical controls that comprise the demonstrated solution.

4.8.1 NIST SP 800-63-2 LOA

NIST SP 800-157 defines certificate issuance policies based upon the NIST SP 800-63-2 LOAs the credential can assert. DPCs can assert LOA-3 (id-fpki-common-pivAuth-derived,

2.16.840.1.101.3.2.1.3.40) and LOA-4 (id-fpki-common-pivAuth-derived-hardware, 2.16.840.1.101.3.2.1.3.41). NIST SP 800-63-2 recommends that agencies select appropriate e-authentication technologies after completing a risk assessment and mapping the identified risks to the required assurance level based upon Office of Management and Budget (OMB) M-04-04, *E-Authentication Guidance for Federal Agencies.*[29] The guidance states specific technical requirements for each of the four levels of assurance.

4.8.2 X.509 Certificate and CRL Extensions Profile for the SSP Program

The Federal Public Key Infrastructure Policy Authority's Derived PIV Authentication Certificate Profile (Worksheet 11: Derived PIV Authentication Certificate Profile) is followed for the creation of the DPC authentication certificate profile. The deviations from the certificate profile are:

- The test OID 2.16.840.1.101.3.2.1.48.173 is used for the policyIdentifier extension to signify id-fpki-common-pivAuth-derived (LOA-3).
- The Subscriber's DerivedPIVCredentials.com AD UserPrincipalName is added as an otherName within the subjectAltName extension.

The End Entity Signature Certificate Profile is followed for the creation of the DPC End Entity Signature certificate profile. The deviation from the certificate profile is:

- The Secure Email OID 1.3.6.1.5.5.7.3.4 was added to the extKeyUsage to support Outlook Web Access S/MIME digital signature.

4.8.3 Identity Proofing

NIST SP 800-157 states that the identity proofing and registration used for issuance of the Applicant's PIV Card can be applied to the issuance of the Applicant's DPC as to not repeat the identity vetting process. The Applicant must demonstrate possession and control of the PIV Card by performing authentication with the PIV Authentication certificate credential. How the Applicant enrolls for the DPC is one factor in determining the credential's level of assurance. The MyID CMS can perform both LOA-4 (in-person, biometric match) and LOA-3 (remote) enrollments. This research demonstrates LOA-3 enrollments.

4.8.4 Tokens

NIST SP 800-63-2 defines the following tokens and their associated assurance levels:

Level 4 Multi-Factor Hardware Cryptographic Token: Cryptographic module shall be FIPS 140-2 validated, Level 2 or higher; with physical security at FIPS 140-2 Level 3 or higher. It shall require the entry of a password, PIN, or biometric to activate the authentication key. It shall not allow the export of authentication keys.

[29] https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

Level 3 Multi-Factor Software Cryptographic Token: The cryptographic module shall be validated at FIPS 140-2 Level 1 or higher. Each authentication shall require entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication.

Table 2: NIST SP 800-63-2 LOA Mappings

NIST SP 800-63-2 Assurance Level	PIV Derived Authentication Certificate Policy	Cryptographic Token FIPS 140-2 Validation Level	Enrollment Requirements
LOA-3	id-fpki-common-pivAuth-derived	FIPS 140-2 Level 1	Remote enrollment allowed
LOA-4	id-fpki-common-pivAuth-derived-hardware	FIPS 140-2 Level 2 / Level 3 physical security	In-person enrollment required

Only LOA-3 hardware and software cryptographic tokens are implemented.

4.8.5 Microsoft VSC Technology

The Microsoft Windows 8.1 VSC is a multi-factor X.509-based cryptographic device.[30] The system's TPM protects the DPC's cryptographic key that is activated through a second authentication factor (e.g., PIN). Authentication is accomplished by proving possession of the device and control of the key. All private key cryptographic functions occur within the TPM. Cryptographic message digests occur within the OS's Cryptographic Service Provider (CSP). VSCs utilizing a TPM support three main security principles:

- **Non-exportability:** Since all private information on the VSC is encrypted by using the host machine's TPM, it cannot be used on a different machine with a different TPM. Additionally, TPMs are designed to be tamper-resistant and non-exportable themselves, so an adversary cannot reverse engineer an identical TPM or install the same one on a different machine.
- **Isolated cryptography:** TPMs provide the same properties of isolated cryptography offered by conventional smart cards, and this is utilized by VSCs. When used, unencrypted copies of private keys are loaded only within the TPM and never into memory accessible by the OS. All cryptographic operations with these private keys occur inside the TPM.
- **Anti-hammering:** If a user enters a PIN incorrectly, the VSC responds by using the anti-hammering logic of the TPM, which rejects further attempts for a period of time instead of blocking the card. This is also known as lockout.

ADCS supports TPM attestation,[31] which provides the ability for the issuing CA to confirm that the key in the certificate request is protected by a known TPM. There are three methods of TPM attestation:

[30] http://www.microsoft.com/en-us/download/details.aspx?id=29076
[31] https://technet.microsoft.com/en-us/library/dn581921.aspx

- **User credential:** The CA trusts the user-provided EKPub (the public key of the TPM endorsement key) as part of the certificate request, and no validation is performed other than the requester's domain credentials.
- **EKCert:** The CA validates the EKCert (the certificate associated with the TPM EKPub key) chain that is provided as part of the certificate request and is a member of a list of allowed EKCert chains.
- **EKPub:** The CA validates that the EKPub provided as part of the certificate request is a member of a list of allowed EKPubs.

TPMs implement anti-hammering functionality to reduce the threat of brute force PIN guessing attacks. The VSC relies upon this functionality to further secure the credential. The VSC will implement a TPM lockout[32] after five failed PIN attempts. The TPM lockout period will expire but the VSC will remain blocked. The TPM lockout period is dependent upon the manufacturer's implementation of the feature. On mobile devices that are domain joined, the MyID Operator can reset the VSC lockout by performing a challenge/response passphrase exchange. TPM lockout will affect all services that leverage the TPM. Other services that utilize the TPM, for example Bitlocker, use a different PIN to enable access to the TPM-protected keys. Therefore, the VSC and Bitlocker PINs should have different values.

At the time of this report's publication, there are only two TPM manufacturers[33] that produce TPMs that are validated to FIPS 140-2 Level 1. The Windows 8, Windows RT, Windows Server 2012, Windows Storage Server 2012, and Windows Phone 8 Enhanced Cryptographic Provider is a FIPS 140-2 Level 1 compliant, software-based cryptographic service provider. The cryptographic boundary is defined by the enclosure of the computer system in which the VSC resides.[34] Windows ADCS supports TPM attestation. DPC issuers can use this functionality to ensure credentials are issued only to known TPM-based secure elements. This research effort will not perform TPM attestation during issuance. The Windows devices that DPCs are issued to are deemed valid FIPS 140-2 Level 1 cryptographic tokens if the TPM embedded in the device is FIPS 140-2 Level 1 validated.

The Microsoft CSP layer presents the VSC in the same manner as a physical smart card. This allows X.509-aware applications (e.g., Outlook, Internet Explorer) to use the VSC without any additional drivers or software. Both the Windows and Windows Phone OSs use the same CSP. Therefore the VSC experience on Windows and Windows Phone is the same.

4.8.6 Android and iOS Device Tokens

The MyID Identity Agent provides the cryptographic module that generates, protects, and interacts with the DPC. The MyID Mobile Software Development Kit (SDK) is embedded within the MyID Identity Agent app. RSA private keys for DPCs are generated inside a FIPS 140-2 Level 1 software cryptographic module (OpenSSL FIPS Object Module[35]), which ships

[32] https://technet.microsoft.com/en-us/library/dd851452.aspx
[33] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2023.pdf and http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2014.pdf
[34] https://technet.microsoft.com/en-us/library/security/cc750357.aspx
[35] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf

embedded in the MyID Identity Agent app. As such only LOA-3 (software) derived credentials are currently available for Android/iOS.

The private key data is persisted for storage by the MyID Identity Agent app such that only apps signed by the same code-signing certificate can access the data. Access to the private key shall go via the MyID Mobile SDK. Data is encrypted at rest.

The MyID Mobile SDK allows the private keys to be used (e.g., for authentication). The MyID Mobile SDK is built into applications that are “derived credential enabled” – such as MyID Browser iOS, MyID Browser Android, MyID Mail iOS, and MyID Mail Android. These apps are signed by the corresponding code-signing certificate to enable them to access the derived credential data. If third parties wish to leverage the derived credentials, the SDK can be made available to the third party following the relevant commercial agreement.

The MyID Mobile SDK implements password/PIN verification, enforcing verification of the password prior to activation of the Derived PIV Authentication private key. After a number of consecutive failed verification attempts, the password and private key will become blocked. For LOA-3 software RSA key pairs on iOS/Android, this password protection exists outside of the cryptographic module and is implemented in the MyID Mobile SDK.

5 DPC Initial Issuance

The MyID CMS includes the ability to issue additional X.509 credentials based upon the existing Applicant's PIV enrollment information. For this research, PIV cardholders' smart cards have already been provisioned from MyID. The PIV cardholders' records within MyID will be used as the DPC Applicants' authoritative identity records.

5.1 Issuance

The issuance requirements for a DPC are dependent upon the LOA the credential asserts. The MyID CMS is a workflow-based system that can issue both LOA-4 and LOA-3 DPCs. This research will demonstrate the issuance of LOA-3 credentials. The issuance of a LOA-3 credential allows for remote issuance to a mobile device. LOA-3 enrollment can be performed by either the MyID self-service kiosk or email notification, which uses out-of-band one-time passwords. Only client authentication and S/MIME digital signature usage will be demonstrated. The key management (encryption) keys/certificate can be recovered from MyID and provisioned to the mobile device, but it will not be implemented in the test environment.

5.2 MyID LOA-3 Self-Service Kiosk Issuance

MyID provides multiple enrollment models for issuance of DPCs in order to be flexible as it fits into the business processes of the organization. An example of how an Applicant could receive their DPCs is by using the MyID self-service kiosk. The kiosk provides the ability for the user to securely perform a NIST SP 800-157 self-enrollment for a DPC. The kiosk resides on a Windows 7 or Windows 8 OS running the MyID self-service kiosk application. The kiosk will perform all the tasks required for issuance in accordance with the guidance provided by NIST SP 800-157 as well as ensuring all communications between the MyID self-service kiosk and the MyID CMS occur over TLS 1.2 provided by Microsoft IIS. All communications with the MyID CMS occur over the TLS-protected transport.

The mobile device on which the DPC will be generated and reside must have the MyID Identity Agent installed. The Identity Agent communicates with the MyID server in order to securely issue the DPC on the mobile device. This mobile app is available from the respective mobile device app stores or marketplaces. MyID works with several of the major enterprise mobility management systems, including Mobile Device Management (MDM) solutions, so that this application can be distributed via non-public methods.

The Applicant begins the issuance process by inserting his or her PIV smart card in the kiosk's smart card reader as depicted in Figure 13.

Figure 13: MyID Self-Service Kiosk Initial Screen

When a user presents a PIV to MyID, the Card Holder Unique Identifier (CHUID) and PIV Authentication certificate containers are read from the PIV card. These containers are validated on the MyID CMS server. It is verified that the Federal Agency Smart Credential Number (FASC-N) in the CHUID matches the FASC-N in the PIV authentication certificate. The CHUID is then examined to determine whether the presented PIV card is from an agency (and/or site within an agency) that may obtain derived credentials from this system. This aspect is configurable per MyID CMS installation.

If these tests are passed, the user is prompted to enter his or her PIN as shown in Figure 14, which enables additional access to the PIV Card.

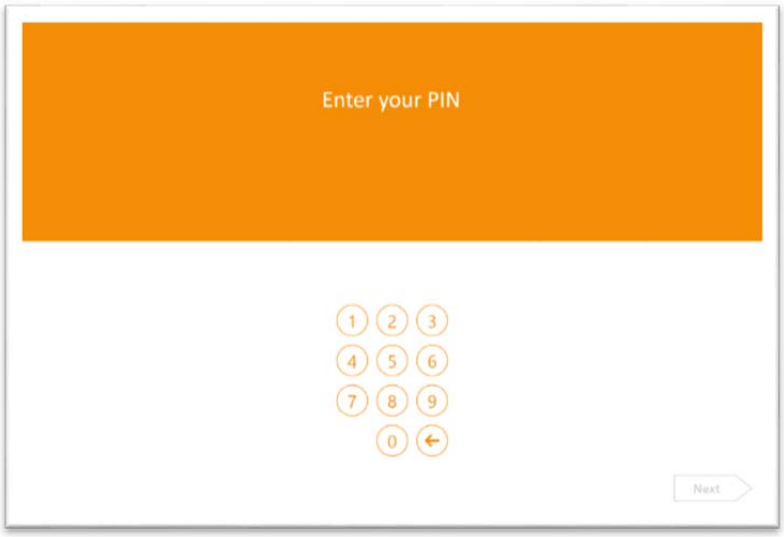


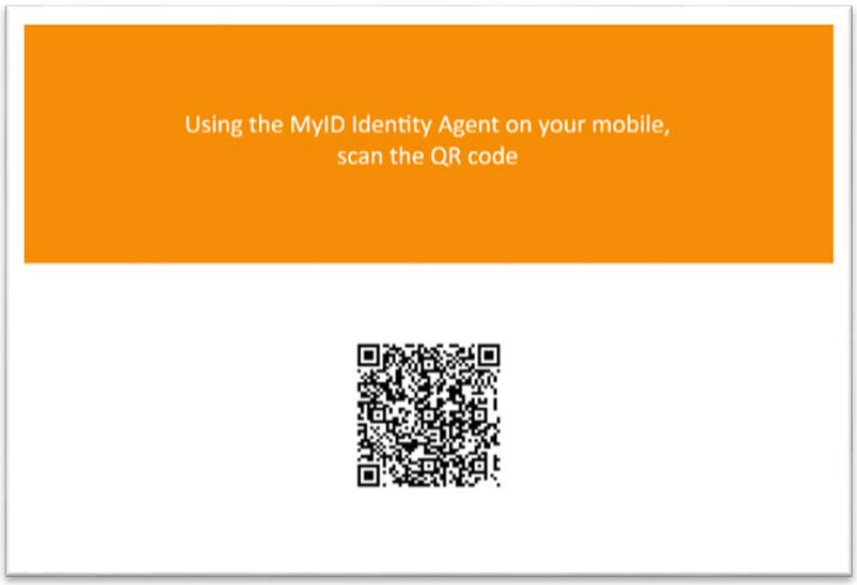
Figure 14: MyID Self-Service Kiosk PKI-AUTH

The MyID CMS validates the user's PIV Client Authentication certificate, checking revocation status for the certificate chain, ensuring the certificate is issued within the Federal Common Policy CA hierarchy, and asserts the correct OID for id-fpki-common-authentication. If validation fails, the kiosk will not proceed.

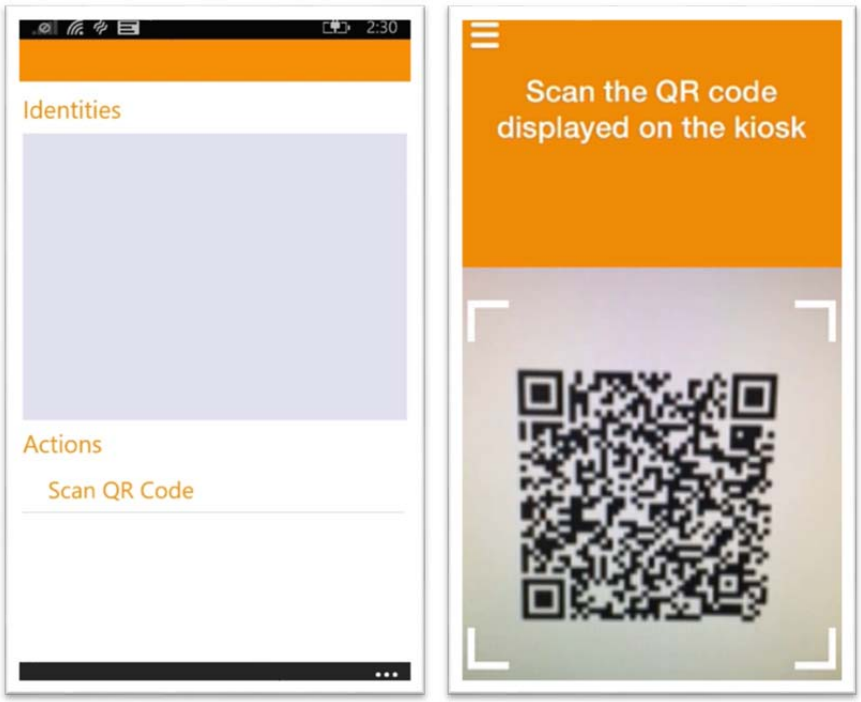
If validated, MyID CMS then schedules the seven-day certificate revocation check task for the user's PIV Client Authentication certificate.

A server-generated challenge is sent to the kiosk, and the kiosk communicates with the PIV Card to sign the challenge using the private key associated with the PIV Authentication certificate. The MyID CMS server verifies that the returned signature has been performed by the PIV Authentication certificate validated as described above. This concludes the PKI-AUTH check demonstrating possession of a valid PIV Card by the cardholder.

Once the user has been validated, a Quick Response (QR) code appears on the screen in front of the user as shown in Figure 15. The QR code contains the required elements for the Identity Agent to communicate with the MyID CMS and its associated enrollment record. These elements are the web service endpoint URL, a unique job number, a global unique identifier for this task, and a one-time passcode. All of these elements are what allows MyID to ensure the Applicant is collecting the intended job. At this stage, the user starts the MyID Identity Agent on the mobile device and selects Scan QR Code as shown in Figure 16.



1068
1069 **Figure 15: MyID Self-Service Kiosk QR Code**



1070
1071 **Figure 16: MyID Identity Agent QR Code Scan**

Once the QR code is scanned, the Identity Agent connects to the MyID CMS web service. The job identifier, the enrollment unique identifier, and an encoded one-time access code are presented to MyID. Once all values are confirmed, the mobile agent communicates to the MyID CMS to collect the DPC as shown in Figure 17.

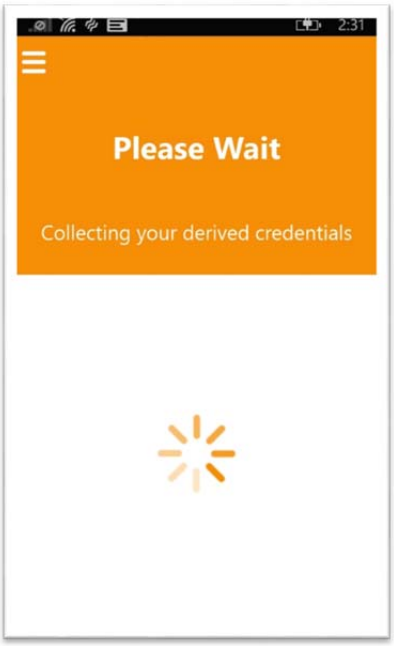


Figure 17: MyID Identity Agent Job Collection

Once the communications are established, the kiosk portion of the enrollment process is complete, and the Applicant can remove the PIV Card as shown in Figure 18.

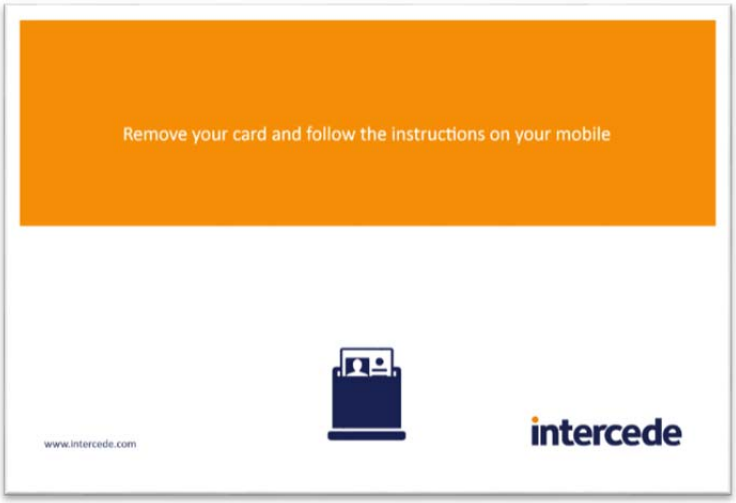


Figure 18: MyID Self-Service Kiosk Completion

On the mobile device the user is prompted to set the PIN for private key access as shown in Figure 19. The PIN Policy is enforced within the MyID CMS.

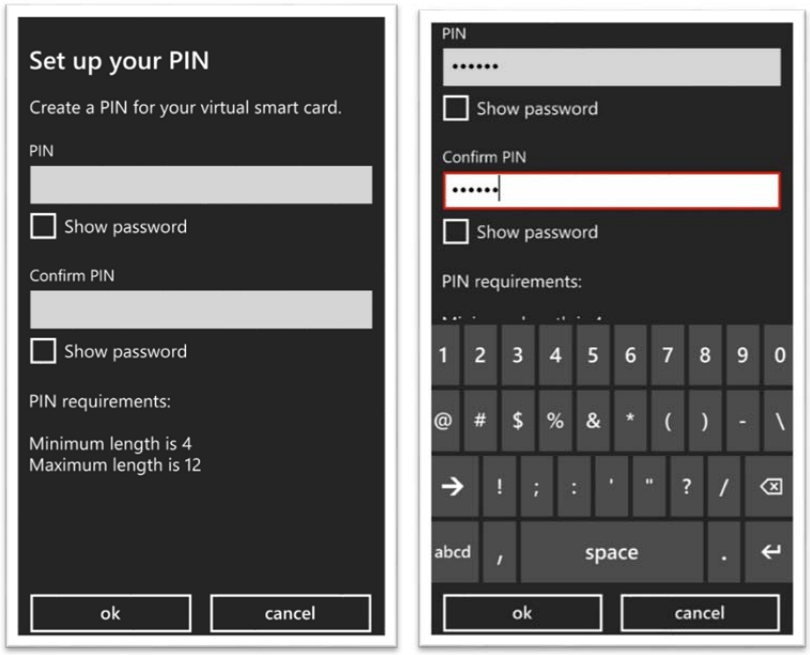


Figure 19: MyID Identity Agent PIN Creation

The associated key pairs (i.e., client authentication and digital signature) are generated on the mobile device within the cryptographic module. The MyID Identity Agent communicates with the MyID CMS to perform certificate issuance. The newly generated public key is sent back to the MyID server as a Public-Key Cryptography Standard (PKCS) #10. MyID will communicate with the DPC-issuing CA, submitting the PKCS #10 to the CA along with various configurable attributes such as email address and UPN. The CA will return a PKCS #7 and MyID will pass the certificate to the mobile device to be stored securely.

The enrollment process completes. MyID Identity Agent provides a graphical representation of the Subscriber's PIV credential as shown in Figure 20.

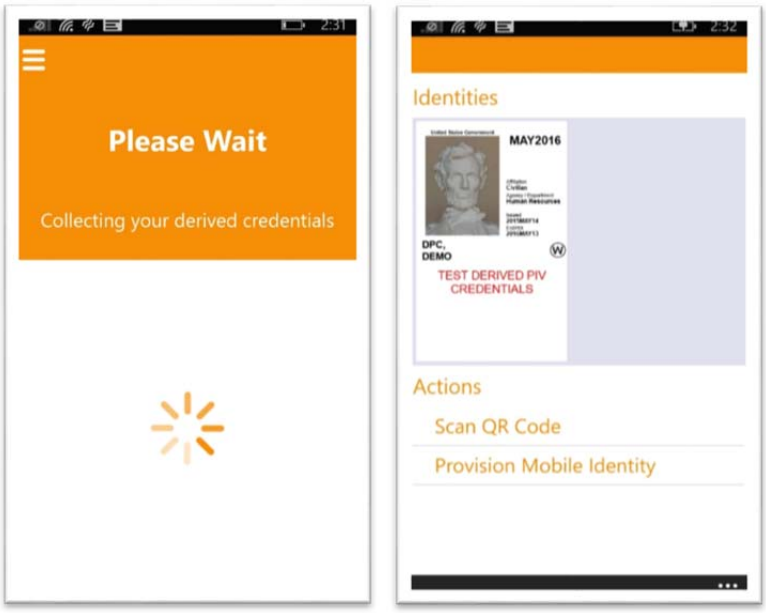


Figure 20: MyID Identity Agent DPC Key Generation and Certificate Issuance

5.2.1 Revocation of Applicant's PIV Card within Seven Days of DPC Issuance

The revocation status of the Applicant's PIV Authentication certificate should be rechecked seven calendar days following issuance of the DPC; this step can detect the use of a compromised PIV Card to obtain a DPC. When the MyID CMS system issues the DPC, a job is queued to check the certificate revocation status of the enrollee's PIV Authentication certificate during the seven days after the DPC issuance. If the Primary PIV credential is revoked any time within the seven-day period for any reason, the newly-issued DPC will be automatically revoked.

To demonstrate this scenario using one of MyID's several mechanisms to revoke credentials, the primary PIV Card was revoked after the DPC was issued. The PIV certificate was issued on Tuesday, May 26, 2015. The Subscriber's PIV Authentication certificate's serial number is shown in Figure 21.

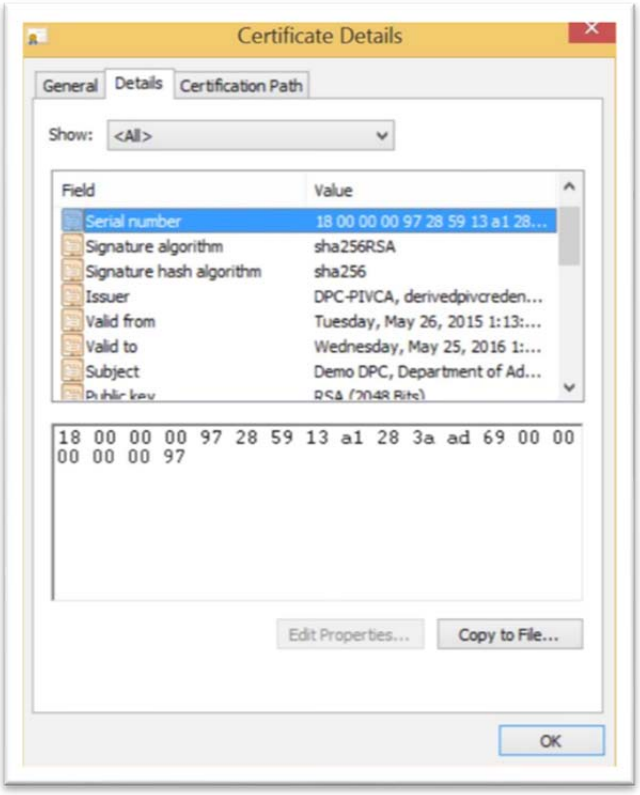


Figure 21: Subscriber's PIV Authentication Certificate's Serial Number

The Subscriber's PIV certificate was revoked on the same day as the issuance of the DPC. The PIV CA CRL contains the serial number of the PIV certificate. The Subscriber's PIV Authentication certificate serial number within the CRL is shown in Figure 22.

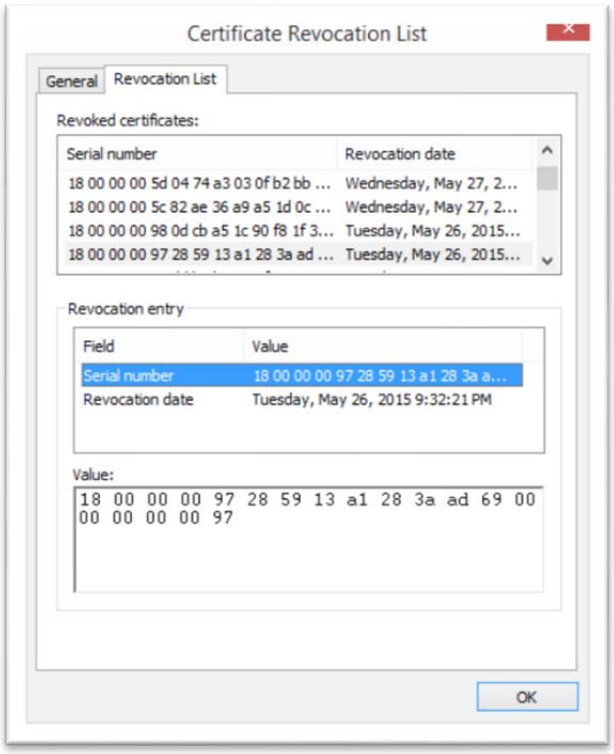


Figure 22: Subscriber's PIV Authentication Certificate Serial Number within CRL

The Subscriber's DPC certificate was issued on Tuesday, May 26, 2015. The Subscriber's Derived PIV Authentication certificate serial number is shown in Figure 23.

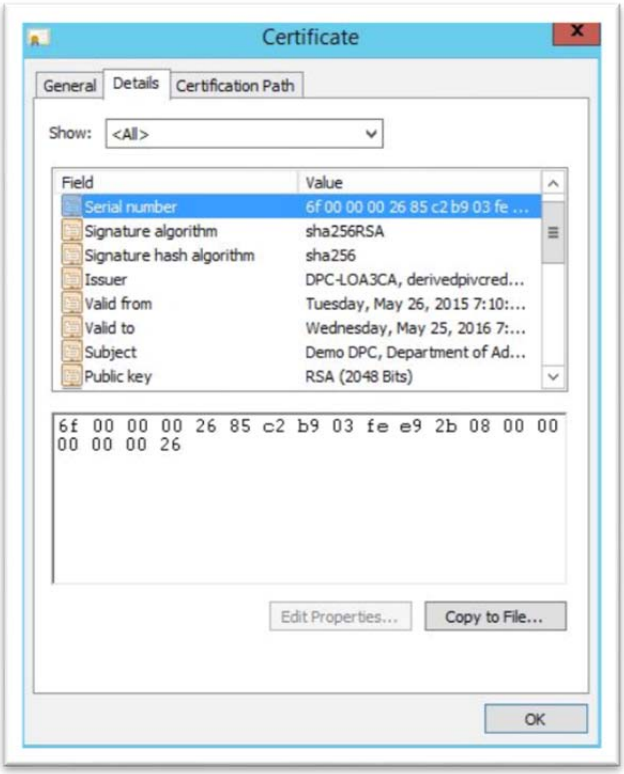


Figure 23: Subscriber's Derived PIV Authentication Certificate Serial Number

The MyID CMS automatically revokes the issued DPC based upon the revocation of the Subscriber's corresponding PIV credential within the seven-day period after issuance. The LOA-3 CA CRL contains the serial number of the DPC certificate as shown in Figure 24. The revocation date was two days after the revocation of the Subscriber's PIV credential.

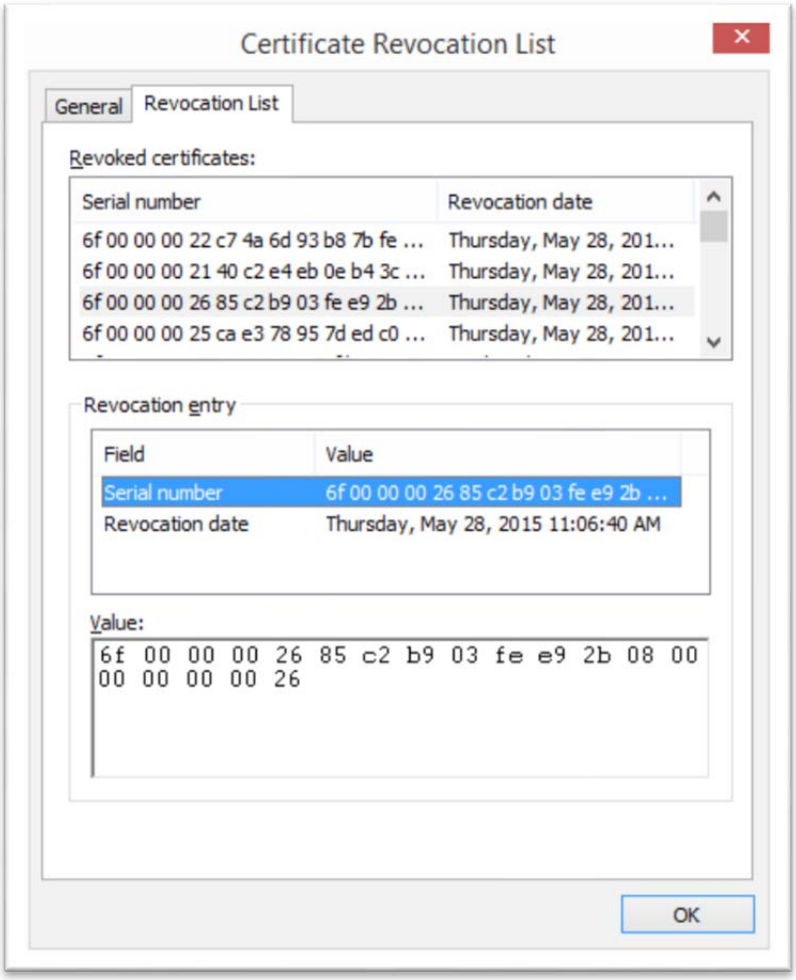


Figure 24: Subscriber's Derived PIV Authentication Certificate Serial Number within CRL

5.3 MyID LOA-3 Remote Issuance by the Organization

In addition to the MyID self-service kiosk, Intercede has developed a mechanism to remotely request a compliant LOA-3 DPC via email enrollment for Applicants who cannot access a self-service kiosk. This workflow is intended to be a complement to the self-service kiosk for those organizations that have business requirements that do not suit the in-person self-service collection. For example, an organization may have employees who are remote from a field office and do not have access to a self-service kiosk. Another use case would be organizations that do not allow mobile devices to use the camera on the phone for the QR scan. The MyID Identity Agent application is also required for this type of issuance, as it was for the self-service kiosk model. This process requires two electronic transactions and based upon the requirement for an LOA-3 DPC, the Applicant must identify himself/herself in each new encounter by presenting a temporary secret that was issued in a previous transaction.

The Applicant browses to the MyID CMS web site and selects Smart Card Logon, as shown in Figure 25.

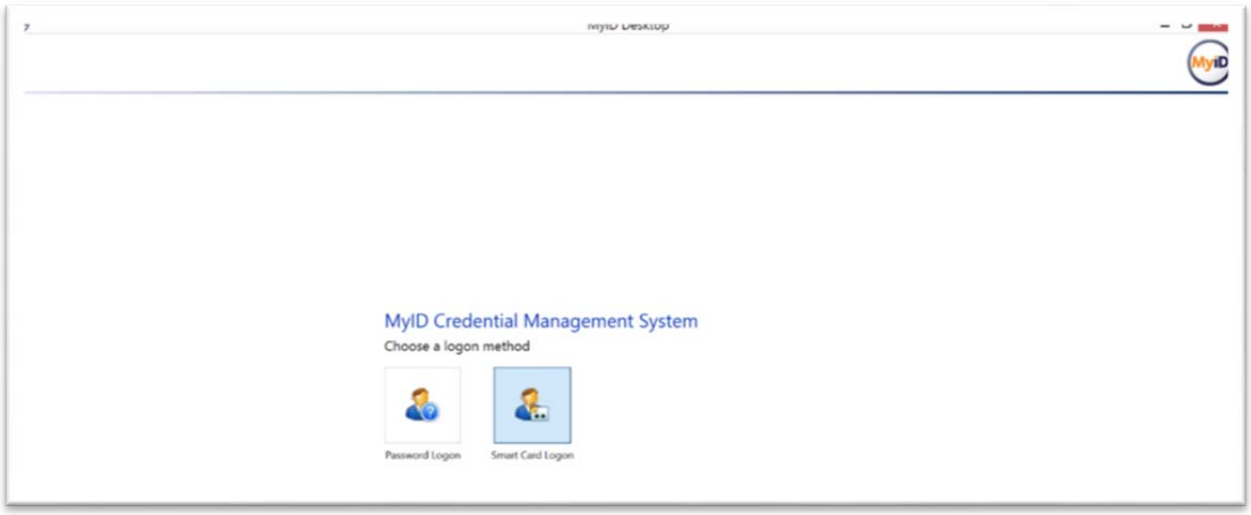


Figure 25: MyID Smart Card Logon

The user enters the PIN to unlock the PIV Client Authentication certificate, proving ownership of the PIV Card and also allowing MyID to validate the user's PIV Client Authentication certificate as shown in Figure 26.

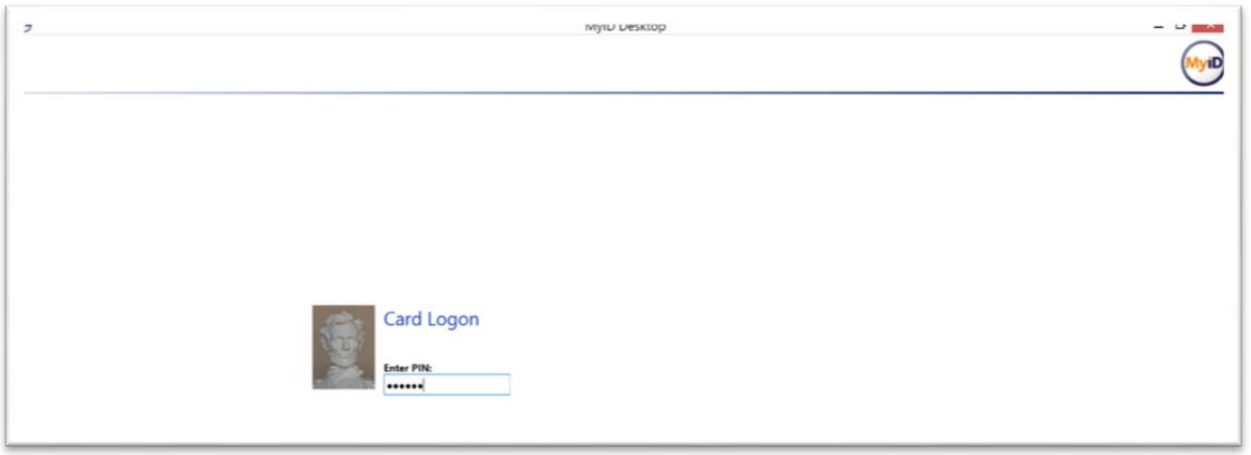


Figure 26: MyID Smart Card Authentication

The MyID CMS is configured based on the user's role to allow Applicants the ability to initiate remote DPC issuance. The Applicant navigates to Select Mobile Devices → Request My ID as shown in Figure 27. MyID can associate the mobile device with the Applicant through an MDM solution. The MDM can be used to enforce which device can receive a DPC.

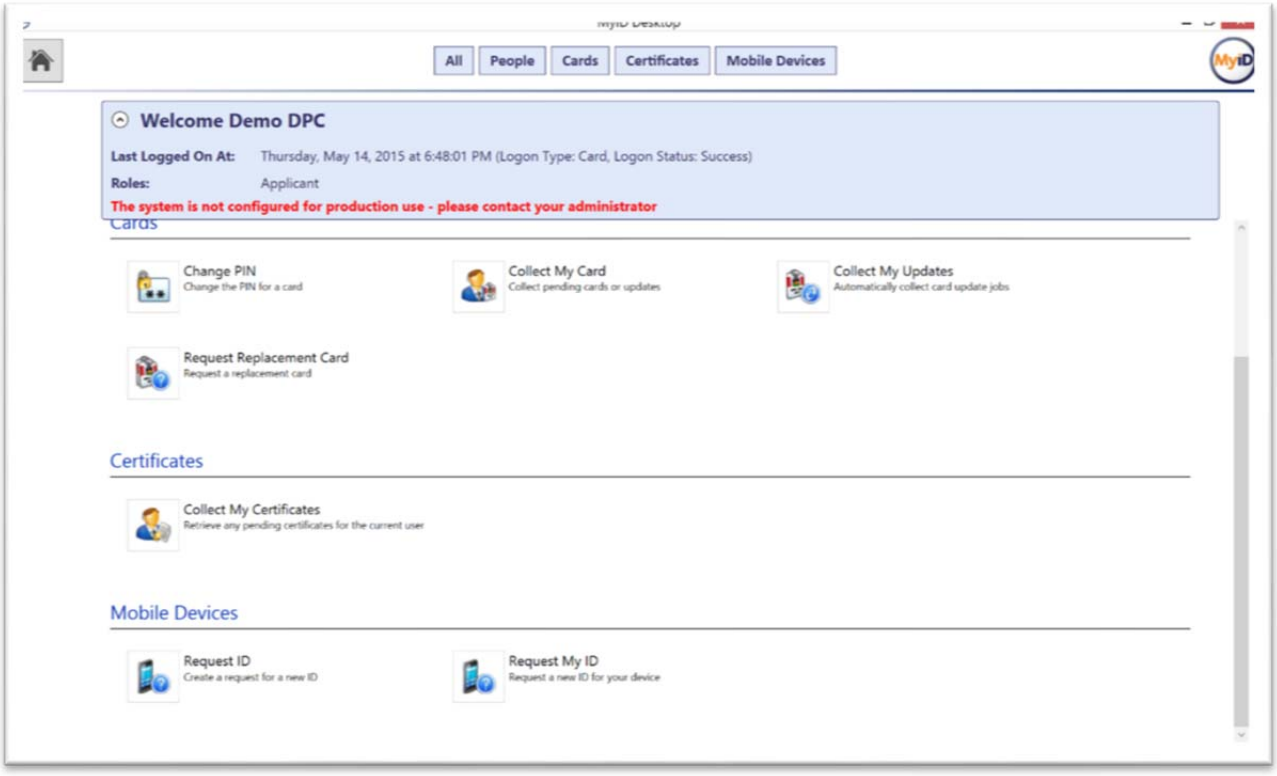


Figure 27: MyID Applicant Console

The Applicant selects the mobile derived credential profile as shown in Figure 28.

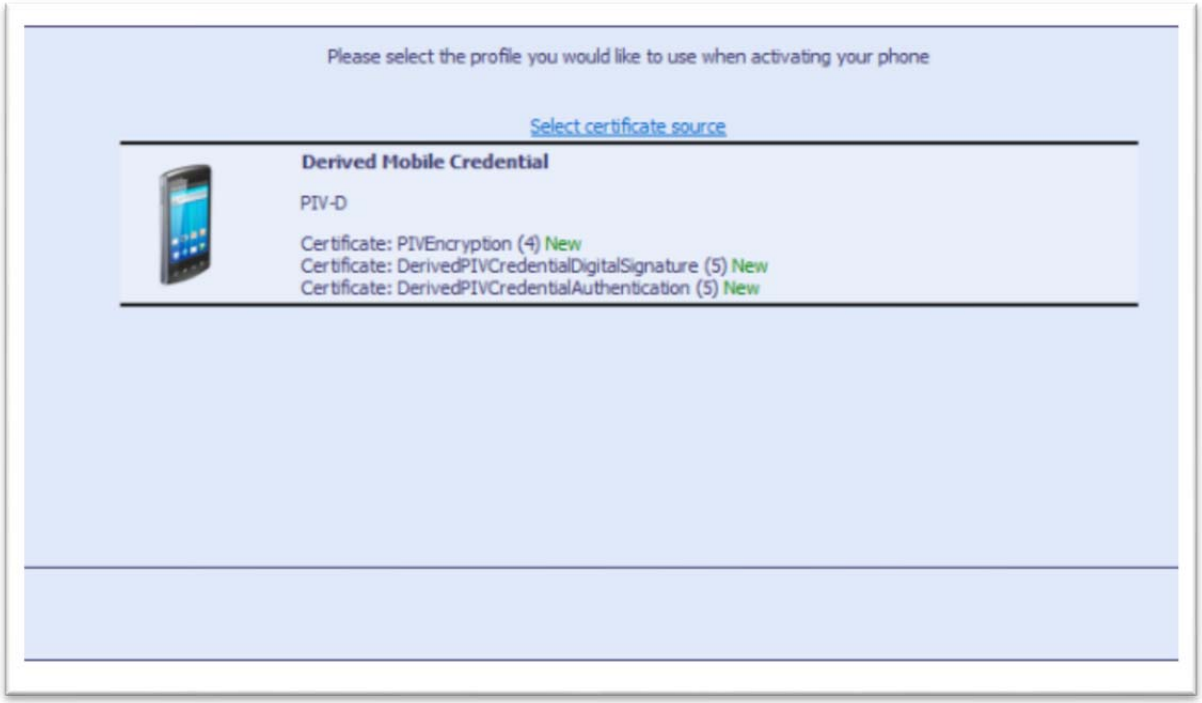


Figure 28: MyID Mobile Device Profile

A one-time passcode is generated as required for enrollment processes that require more than two or more electronic transactions, as shown in Figure 29. The Applicant will be provided this one-time access code through an out-of-band method. It is not recommended to use the same delivery method for the one-time passcode and the MyID Identity Agent registration message (email or Short Message Service (SMS)).

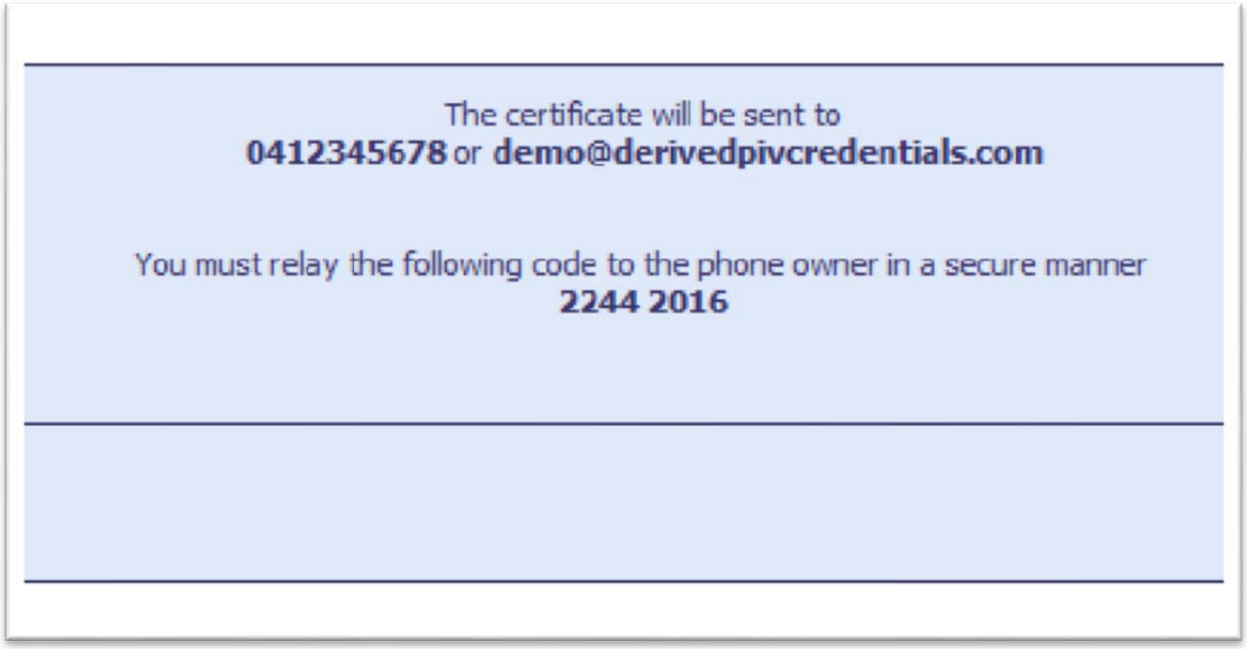


Figure 29: MyID Mobile Enrollment One-Time Access Code

The Applicant also selects the method by which the issuance notification will be delivered to the device. Options for this are also to deliver via email or SMS as shown in Figure 30.

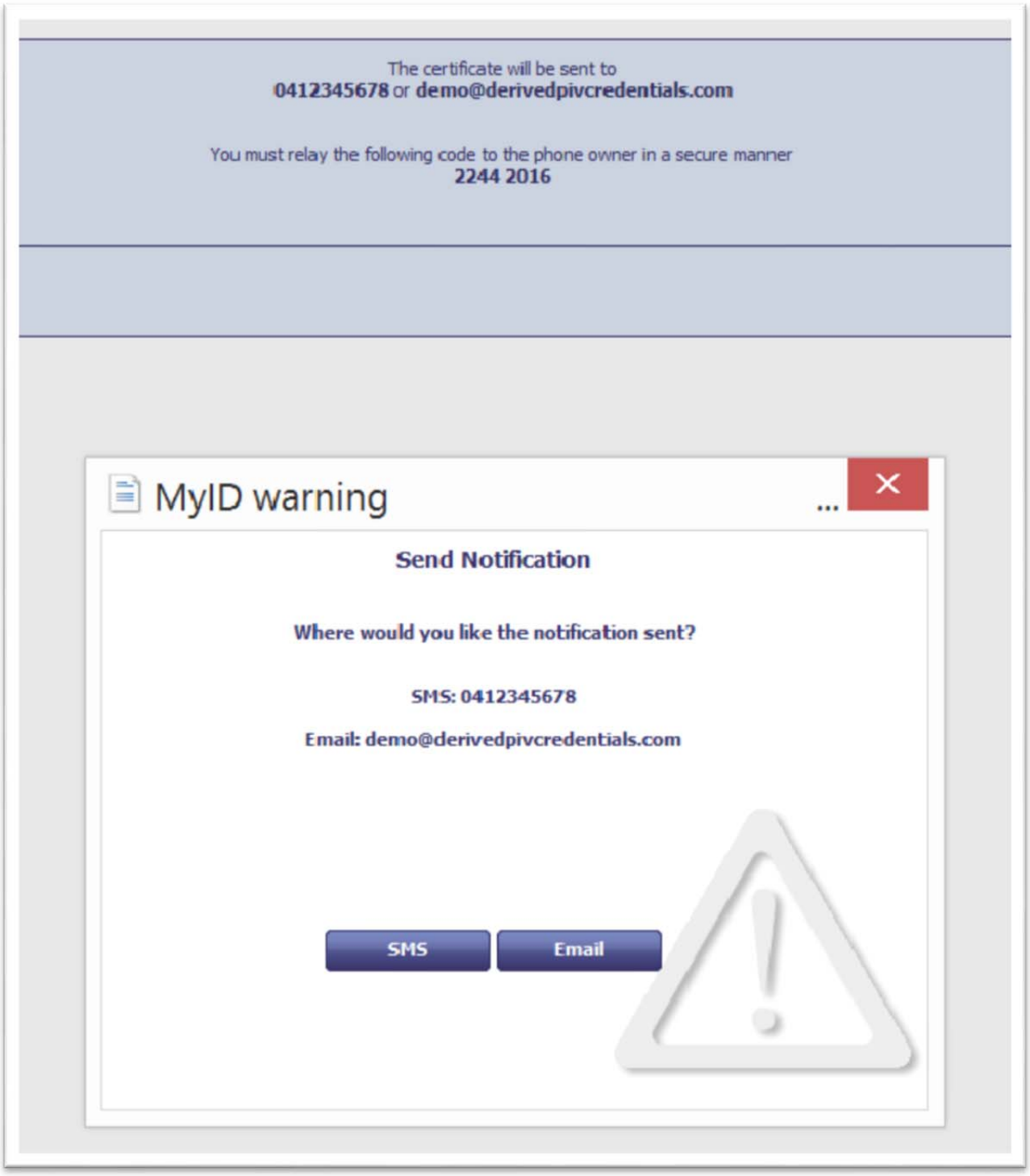


Figure 30: MyID Mobile Enrollment Notification Selection

The Applicant receives an email on the mobile device that will be the target for the DPC, as shown in Figure 31.

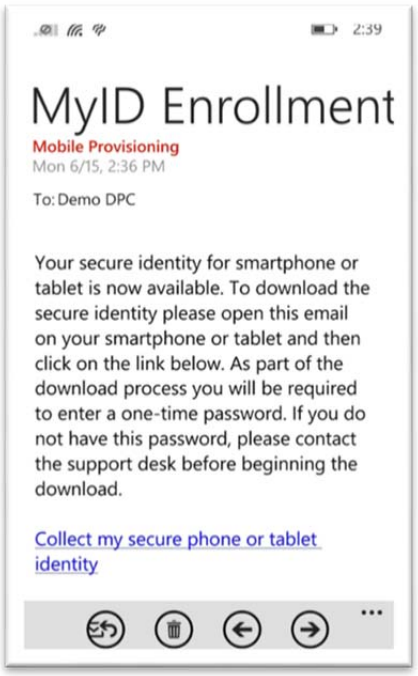


Figure 31: MyID Mobile Enrollment Email Notification

Within the email is the link that states, “collect my secure phone or tablet identity.” This links to the MyID Identity Agent, which will initiate the issuance process. The link also contains similar elements as above to uniquely identity the job that is intended for the respective user.

The Identity Agent connects to the MyID CMS web service over TLS 1.2. The job identifier and enrollment unique identifier are presented to the MyID CMS automatically once the user clicks the link. The Applicant is prompted to enter the one-time passcode for the associated enrollment record, which the Applicant received out of band. Once all values are confirmed, the process continues as shown in Figure 32.

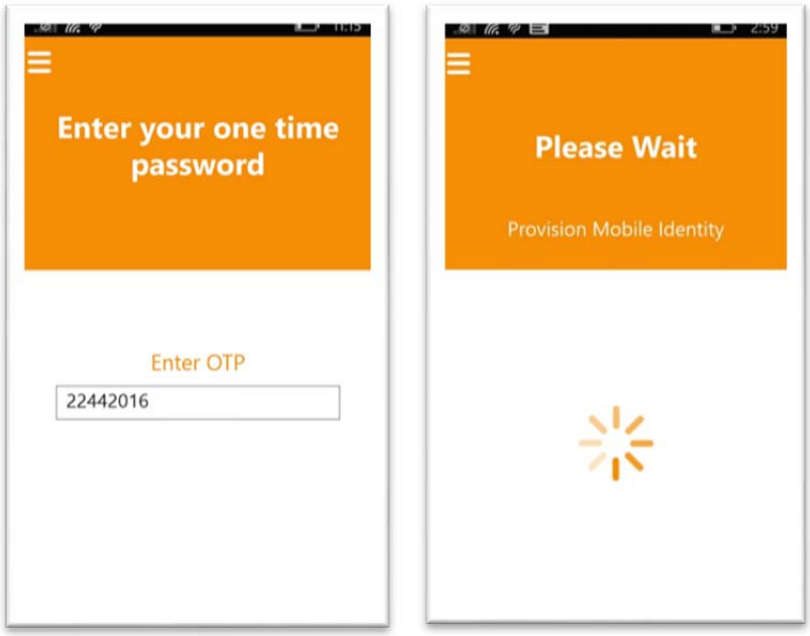


Figure 32: MyID Mobile Agent One-Time Passcode Entry

On the mobile device the user is prompted to set the PIN for private key access as shown in Figure 33. The PIN Policy is enforced within the MyID CMS.

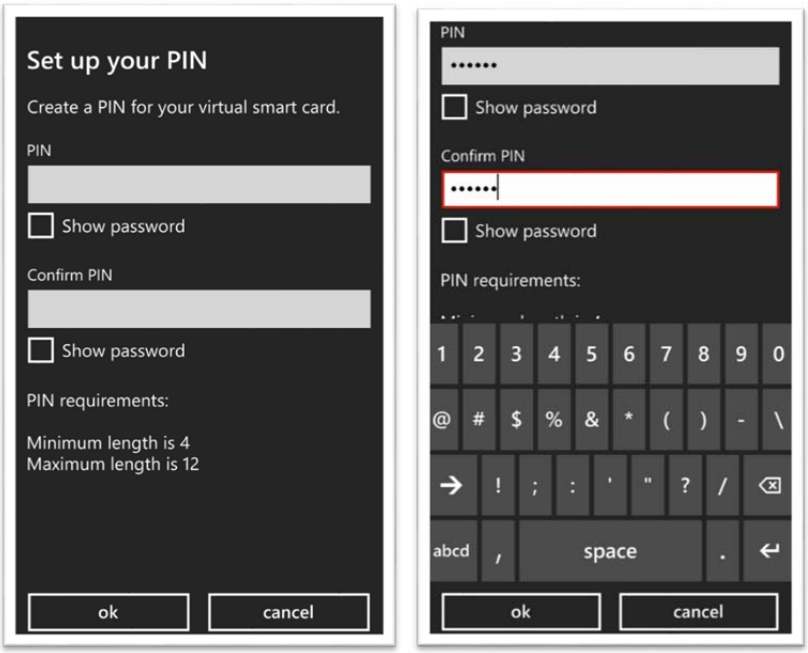


Figure 33: MyID Identity Agent PIN Creation

MyID Identity Agent now communicates with the MyID CMS to perform certificate issuance. The associated key pairs (i.e., client authentication and digital signature) are generated on the mobile device.

The enrollment process completes. MyID Identity Agent provides a graphical representation of the Subscriber's DPC as shown in Figure 34.

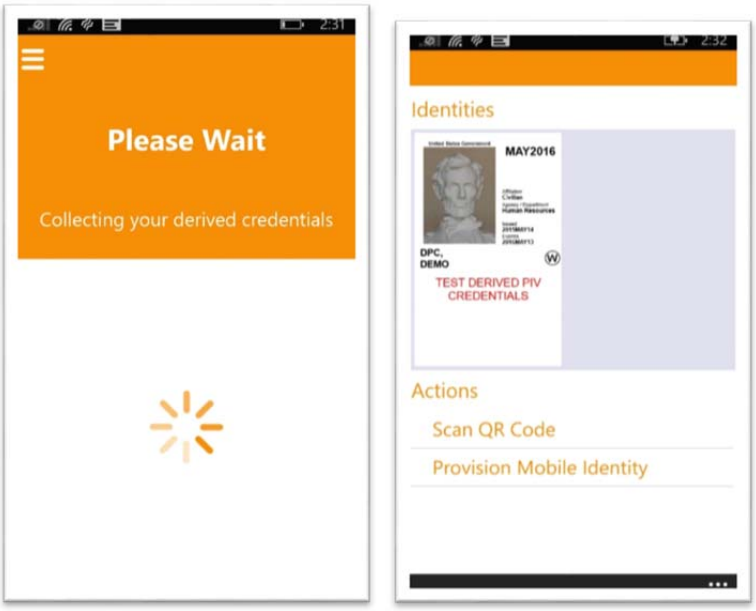


Figure 34: MyID Identity Agent DPC Key Generation and Certificate Issuance

5.4 Windows 8.1 Workstation – MyID Self-Service Enrollment

The MyID CMS can issue Windows 8.1 OS VSCs protected by the TPM. This method of enrollment requires that the MyID CMS and the device to be issued the DPC are joined to the same AD domain. The Azure IaaS Point-to-Site VPN allows for AD Kerberos communications to occur. The device's TPM must be enabled within the system's BIOS and ownership taken from within the TPM.MSC snap-in. The MyID service account must have administrative rights to the workstation and able to communicate via the Windows Management Instrumentation (WMI) for the remote issuance of commands to create a VSC. The following Windows Firewall settings must be applied to the workstation to allow remote enrollment as shown in Table 3.

Table 3: Workstation Group Policy Settings

Group Policy Name	Path	State
Windows Firewall Remote Management (RPC-EPMAP)	Computer Configuration\ Windows Settings\ Security Settings\ Windows Firewall with Advanced Security\ Inbound Rules	Enabled
Windows Firewall Remote Management (RPC)	Computer Configuration\ Windows Settings\ Security Settings\ Windows Firewall with Advanced Security\ Inbound Rules	Enabled

There are multiple methods to deploy a VSC to a domain-joined system. In this demonstration the Subscriber will initiate a DPC request on his or her domain-joined Windows 8.1 device. The MyID Self-Service App is required for this process.

The Applicant logs on to the Windows 8.1 device using his or her PIV smart card, then establishes the Azure Point to Site VPN session and launches the MyID Self-Service App as shown in Figure 35.

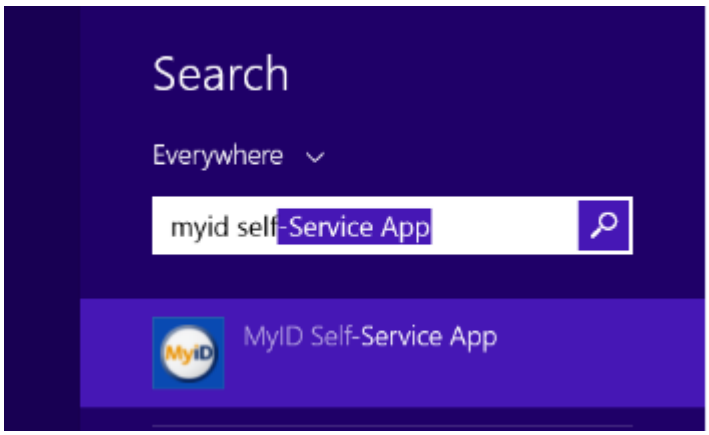


Figure 35: Windows 8.1 MyID Self-Service App

The MyID Self-Service App communicates with the Azure IaaS-based MyID CMS and a notification window appears in the task tray as shown in Figure 36.

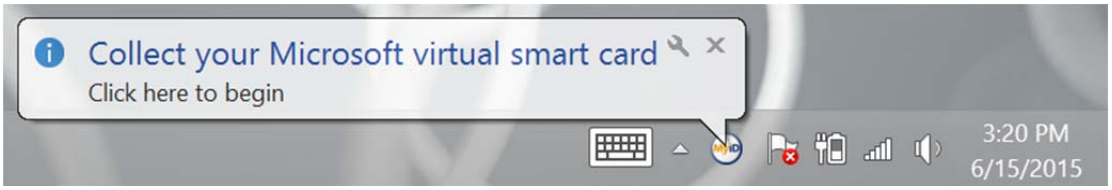


Figure 36: MyID Self-Service App Notification

The process initiates. The Applicant is required to provide the answers to two security questions that the Applicant has pre-registered with MyID as shown in Figure 37. The security questions could be imported via the application programming interface (API) when the user account is created. The use of Active Directory Authentication Mechanism Assurance (AMA)[36] can restrict the launching of the MyID Self-Service App. AMA can be configured to add users, who have authenticated with a PIV smart card, to a dynamic AD-controlled security group. The user's Kerberos ticket will contain the AMA group's identifier, and membership is only valid for the current Kerberos session. The user would have to re-authenticate to AD using his or her PIV smart card to be re-added to the group. The MyID Self-Service App executable can have an access control list applied to only allow members of the AMA group to launch the application, thus proving the user has authenticated using his or her PIV smart card.

[36] https://technet.microsoft.com/en-us/library/dd378897(v=ws.10).aspx

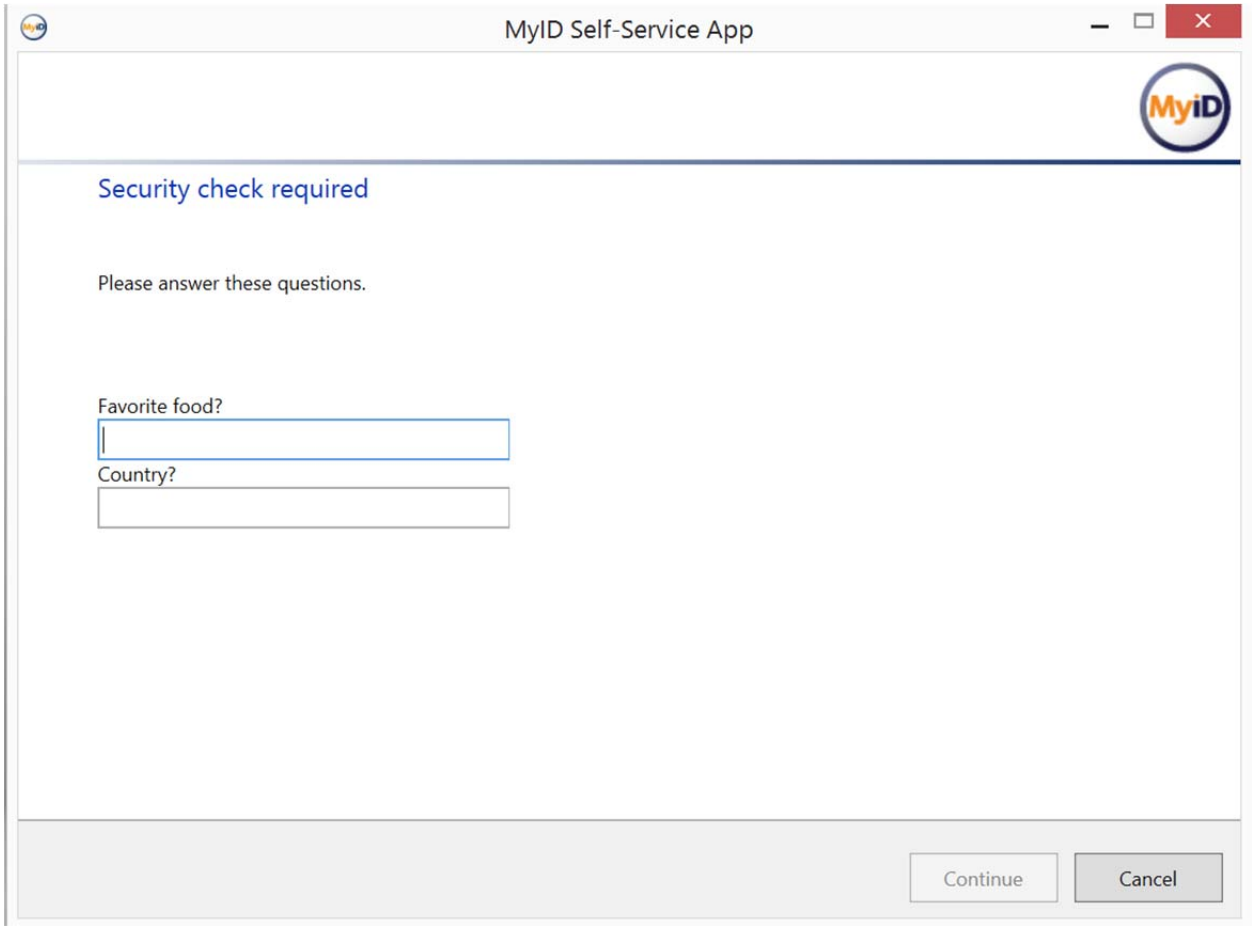


Figure 37: MyID Applicant Challenge Questions

The Subscriber enters the PIN for the DPC as shown in Figure 38. The PIN Policy is enforced within the MyID CMS.

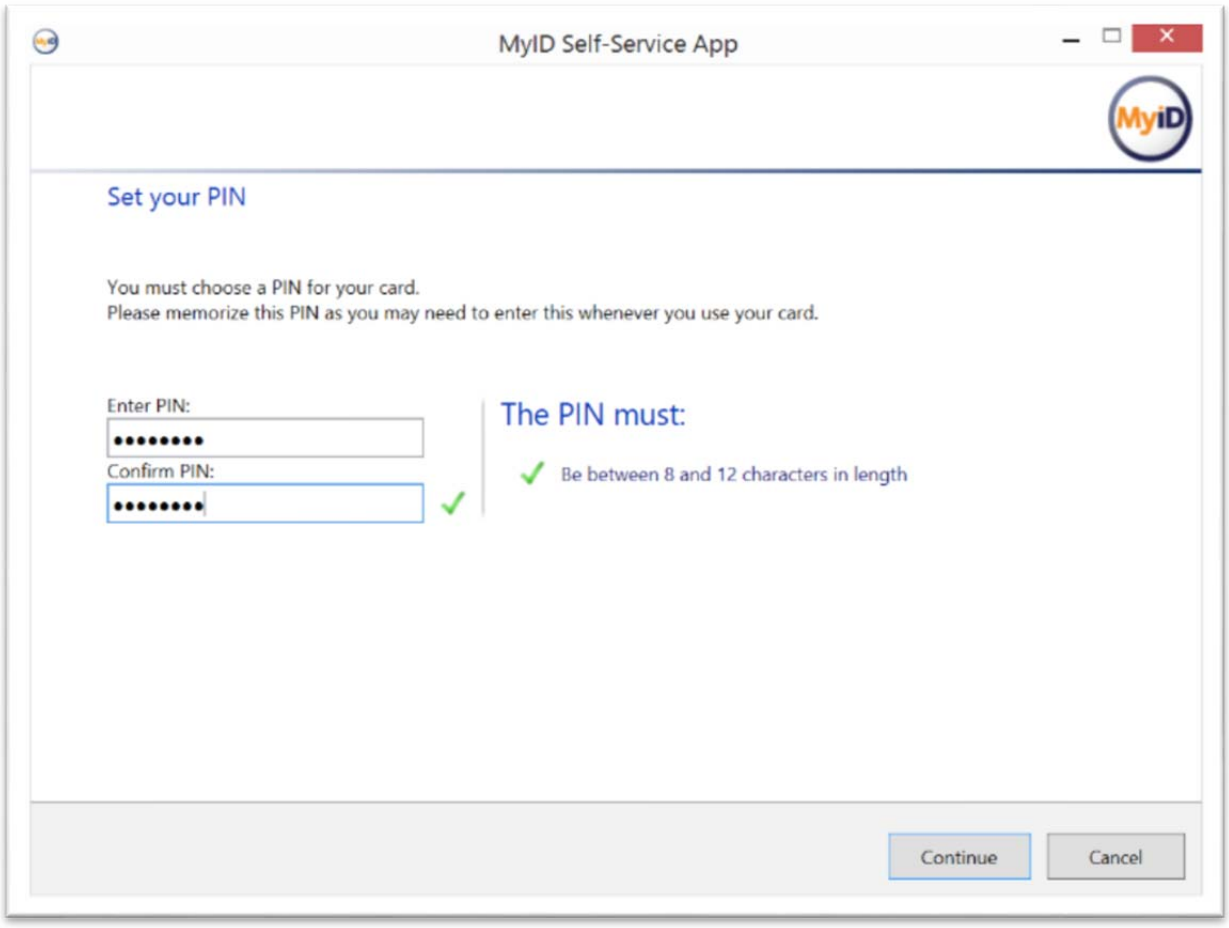


Figure 38: PIN Creation

MyID Self-Service App now communicates with the MyID CMS to perform certificate issuance. The associated key pairs (i.e., client authentication and digital signature) are generated by the TPM as shown in Figure 39. The TPM protects the access to the private key that is associated with the certificate. All cryptographic functions occur in the TPM, e.g., key generation. The certificates are stored in the OS key store and protected by the private key.

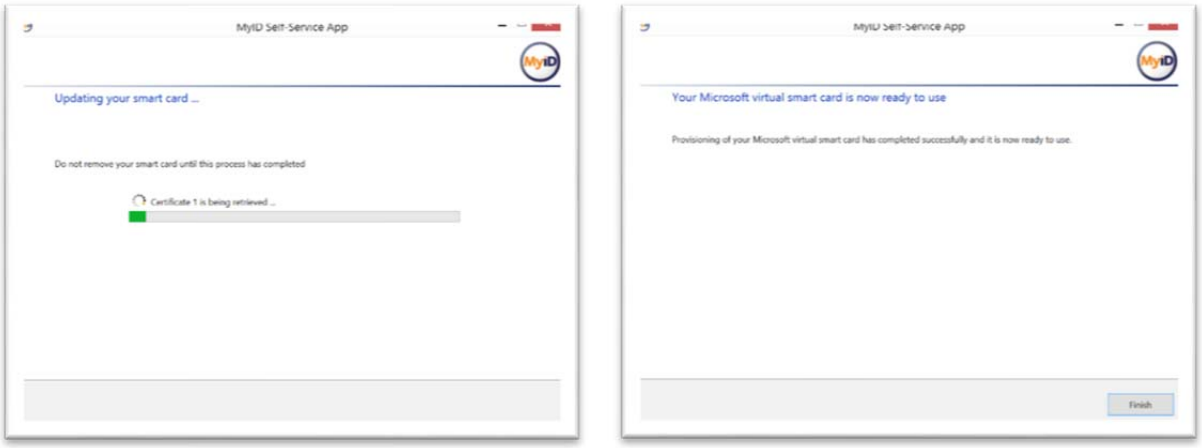


Figure 39: Key Pair Generation and Certificate Issuance

6 DPC Maintenance

The MyID CMS supports the maintenance of DPCs. This section addresses two aspects of maintenance: DPC reissuance and PIN unblocking.

6.1 Reissuance

For many of the lifecycle management usage scenarios accounted for in NIST SP 800-157, the outcome is for the credential to be reissued. That is specifically the case for both name changes and the loss of a mobile device. In the event of a Subscriber name change, the existing DPC should be canceled and a new DPC issued to the mobile device. In this scenario, using the MyID CMS, the existing DPC will be submitted to the CA for revocation and a job for the new DPC will be queued. Since the new device that will contain the DPC is still possessed by the Applicant, the MyID Identity Agent will zeroize the old credential and then write the newly-issued DPC.

In the event of a lost device, the DPC is also required to be reissued, but first MyID must make sure that the lost credential is unusable. Using MyID's ability to remotely cancel devices, the MyID Operator can login to the system and select a device to be revoked. MyID will post any active certificates associated with that device to the CRL, causing them to be unusable. Once the revocation is completed, either the Applicant can report to the kiosk in order to get a new DPC, or an operator can queue up a job for that user in order to perform a remote DPC issuance.

6.2 PIN Unblock

For non-domain-joined devices, reissuance is required when a PIN lockout occurs. For example, the Windows Phone 8.1 VSC will permanently lock after five failed PIN attempts and the VSC will have to be reissued. The scenario is represented in Figure 40.

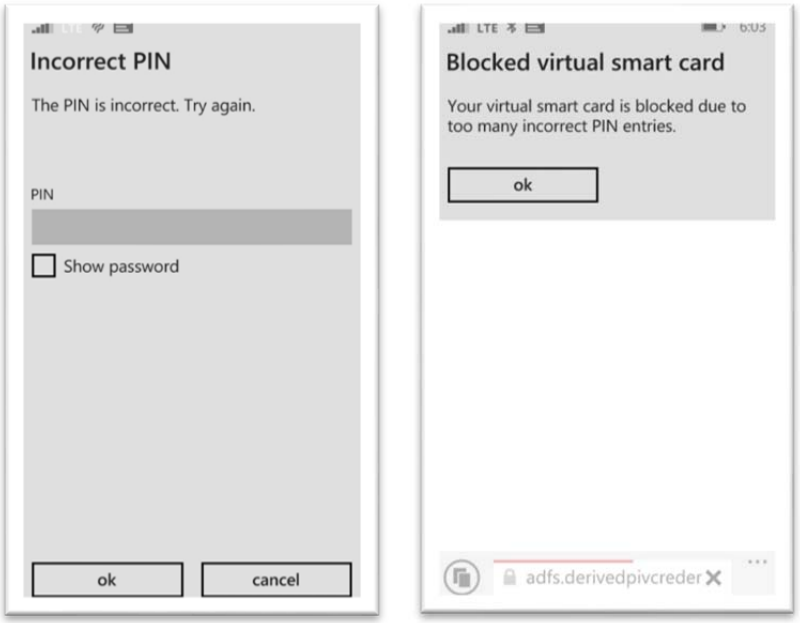


Figure 40: Windows Phone 8.1 PIN Block

For domain-joined Windows 8.1 devices, a challenge/response exchange between the MyID CMS and the device remotely unblocks the Subscriber's DPC as shown in Figure 41. The Subscriber must register two security questions/answers with the MyID CMS as a prerequisite for this process.

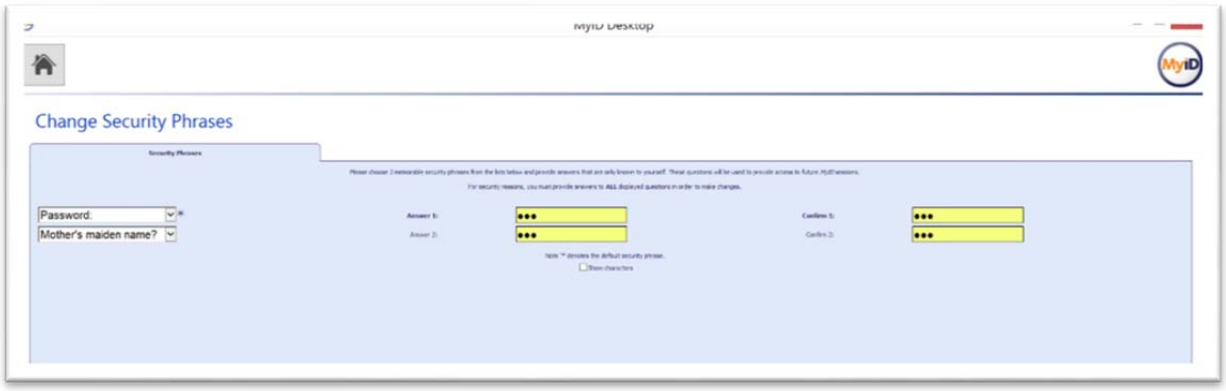


Figure 41: Subscriber's MyID Security Question Registration

Two group policy settings are applied to the workstation to instruct the Subscriber on whom to contact and the challenge phrase, as shown in Table 4.

Table 4: Smart Card Group Policy Settings

Group Policy Name	Path	State
Allow integrated unblock screen to be displayed at the time of logon	Computer Configuration\ Administrative Templates\ Windows Components\ Smart Cards	Enabled
Display string when smart card is blocked	Computer Configuration\ Administrative Templates\ Windows Components\ Smart Cards	Enabled (e.g. "Contact the helpdesk at x5555")

When the Windows 8 VSC is blocked, the Subscriber will be presented a similar screen that instructs him or her to contact the MyID Operators and provides a challenge string that will be given to the Operators as shown in Figure 42.

Figure 42: Windows 8.1 PIN Unblock Challenge Response Screen

The MyID Operator launches the Remote Unlock workflow and searches for the Subscriber's record, then selects the Subscriber's device with the associated blocked DPC. The Subscriber reads the challenge passphrase to the MyID Operator and enters the security question answer. The MyID Remote Unlock screen is shown in Figure 43.

Figure 43: MyID Remote Unlock

MyID produces the unlock response as shown in Figure 44.

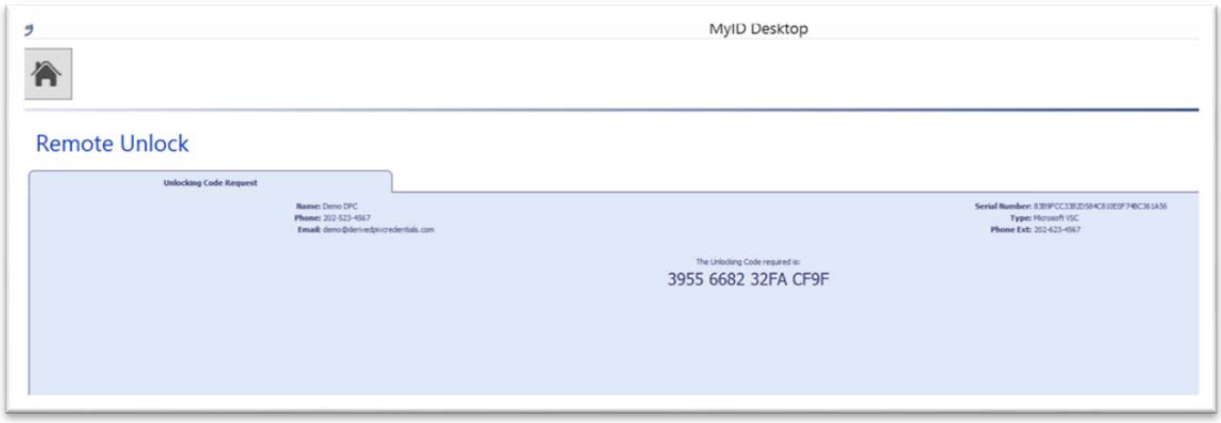


Figure 44: MyID Remote Unlock Response

The MyID Operator reads the response code and password back to the Subscriber. The code and a new PIN is entered by the Subscriber. The PIN is now unblocked as shown in Figure 45.

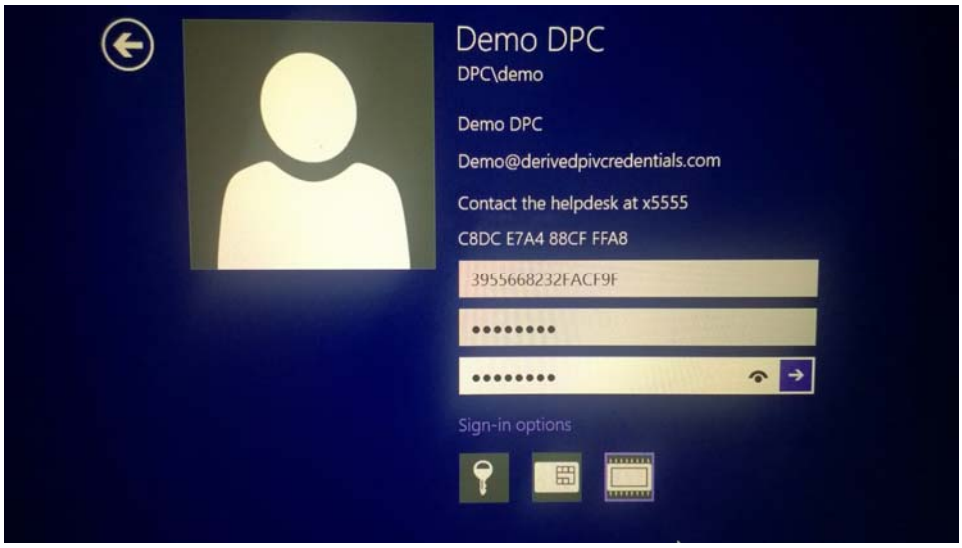


Figure 45: Windows 8.1 PIN Unblock Response and PIN Entry

7 DPC Termination

When a Subscriber is deemed no longer allowed to possess a PIV and DPC, the MyID CMS can terminate the credentials immediately. Since it is unlikely that the MyID Operator will have access to the Subscriber's mobile device to zeroize the token containing the DPC, MyID will revoke all certificates. In this scenario, using one of MyID's several mechanisms to revoke credentials, an operator can use the Remove Person workflow. The Remove Person workflow will revoke all active credentials and associated certificates immediately.

The MyID Operator removes a Subscriber by using the People → Remove Person workflow as shown in Figure 46.

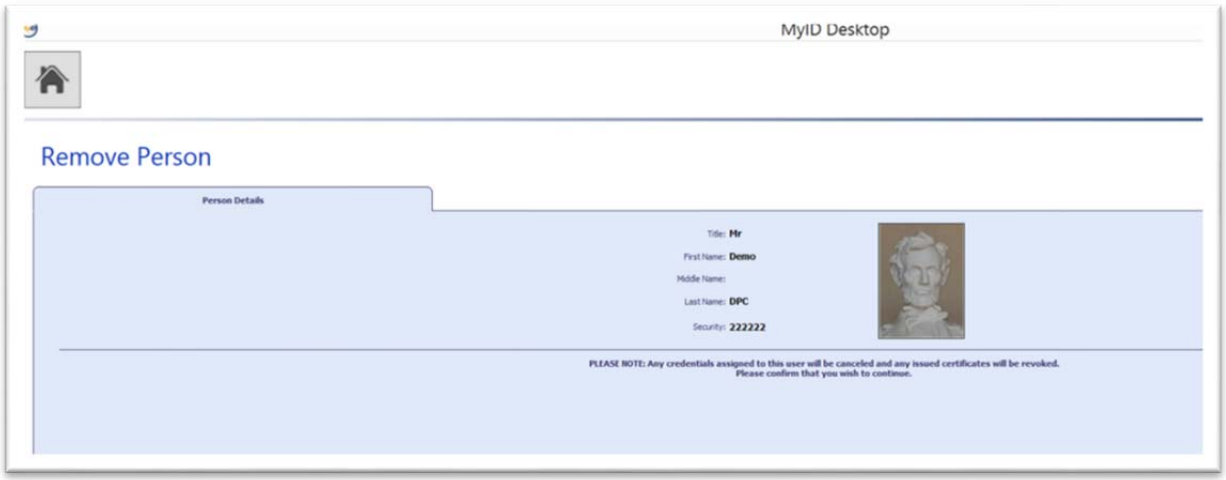


Figure 46: MyID Remove Person

The MyID Operator selects the reason for termination as shown in Figure 47.

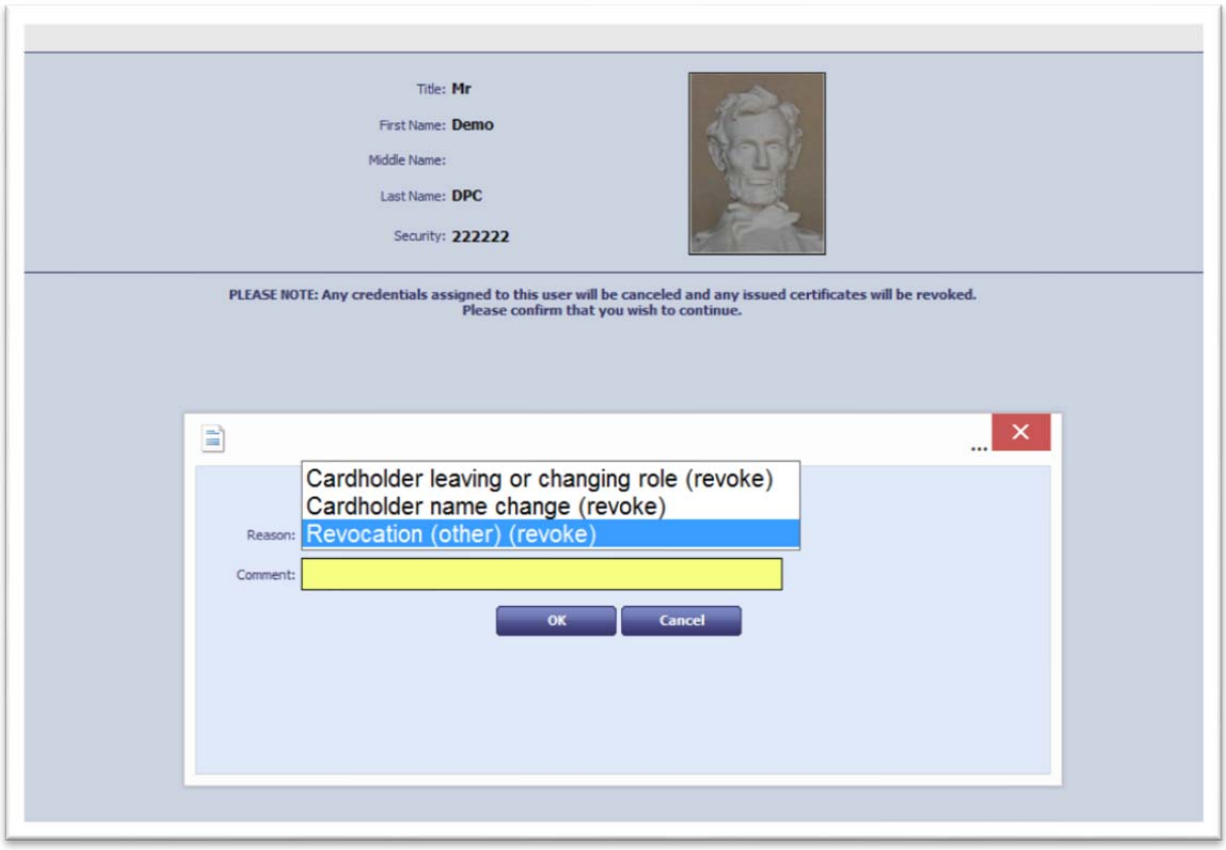


Figure 47: MyID Remove Person Reason Selection

The MyID CMS will revoke all certificates associated with the Subscriber's record. The serial numbers of the certificates will appear in the next DPC PIV CA and DPC LOA-3 CA CRL publications as shown in Figures 48 and 49.

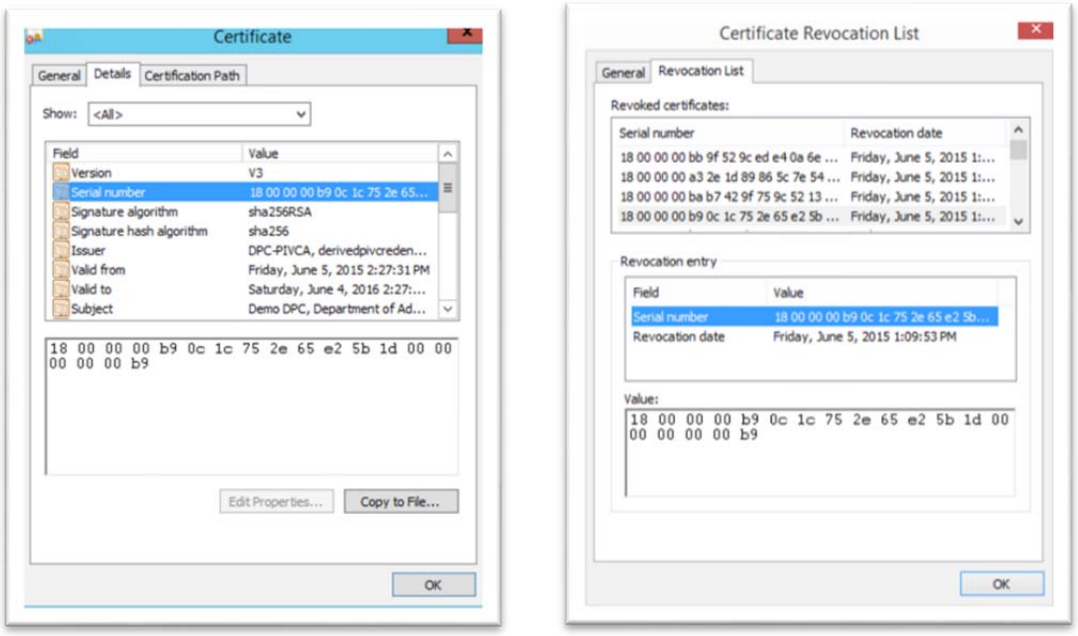


Figure 48: Subscriber's PIV Authentication Certificate and CRL Entry

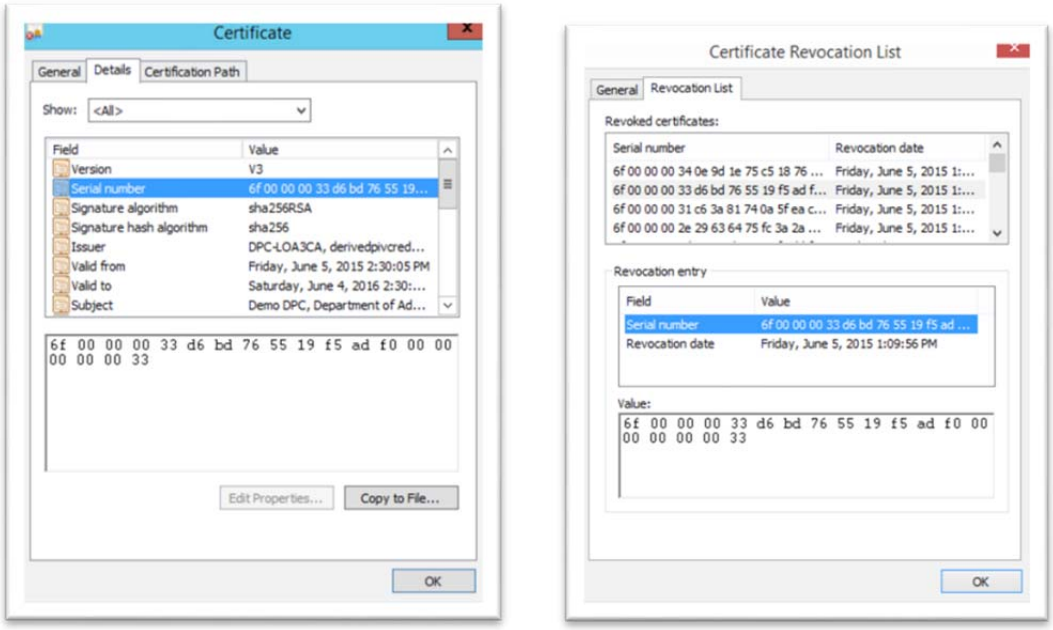


Figure 49: Subscriber's Derived PIV Authentication Certificate and CRL Entry

8 Usage of Cloud-Based Services Via DPCs

Section 4.3 of this report describes the services that the user will be accessing using their DPCs. Microsoft Office 365 "single sign-on" allows customers to use their organization credentials to access Office 365 services. This capability is provided through ADFS or third-party single sign-on providers.[37]

At the time of this report's publication, the various Office 365 services use different protocols. For the user to be prompted for his or her X.509-based credential at time of authentication, the Web Services Federation (WS-Federation) passive requester profile[38] is used. Office 365 Outlook Web Access, SharePoint, and OneDrive use WS-Federation.

The ADFS Identity Provider Security Token Service (IdP STS) authenticates the user to AD and generates a SAML token asserting the user's identity. Within this token is the authenticating user's AD UserPrincipalName (UPN) and ObjectGUID, a unique AD object. These values must match the associated Azure AD user object's UPN and ImmutableID, a unique identifier in Azure AD. These values are synchronized to Azure AD using the Azure AD Synchronization tool described in Section 4.2 of this report. ADFS supports X.509-based authentication. The authenticating user's DerivedPIVCredential.com UPN must match the id-fpki-common-pivAuth-derived certificate's Subject Alternate Name, PrincipalName value as shown in Figure 50.

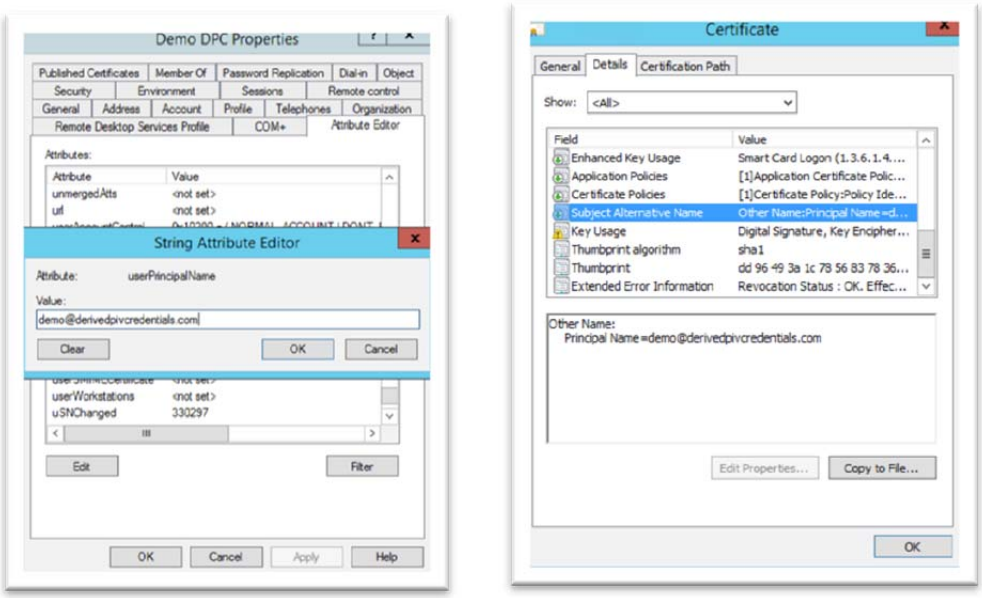


Figure 50: AD UPN to Certificate SubjectAlternativeName PrincipalName Values

It is recommended that the UPN contain a unique, Internet-routable domain suffix (e.g., @derivedpivcredentials.com). The domain suffix is registered as a federated, custom domain

[37] https://technet.microsoft.com/en-us/library/jj679342.aspx
[38] http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf

with Azure AD. When a user attempts to access an Office 365 resource, the Azure federation endpoint, "EvoSTS," determines the URL for the user's IdP STS. This is known as the home realm discovery process. The user's browser is redirected to the organization's IdP STS and is prompted for authentication. This is where the user is prompted for his or her X.509 credential. The user PINs the DPC, and ADFS validates the certificate and authenticates the user to AD. ADFS then generates a SAML access token, which is returned to the user's browser with a redirection to the Office 365 service endpoint. The user is given an access token in the form of an Office 365 access session-based non-persistent cookie to access his or her Office 365 resource.

8.1 Office 365 Outlook Web Access (OWA)

Office 365 Outlook Web Access (OWA) uses claims-based authentication for mailbox access. The WS-Federation passive workflow for X.509-based authentication to an Office 365 OWA mailbox is shown in Figure 51.

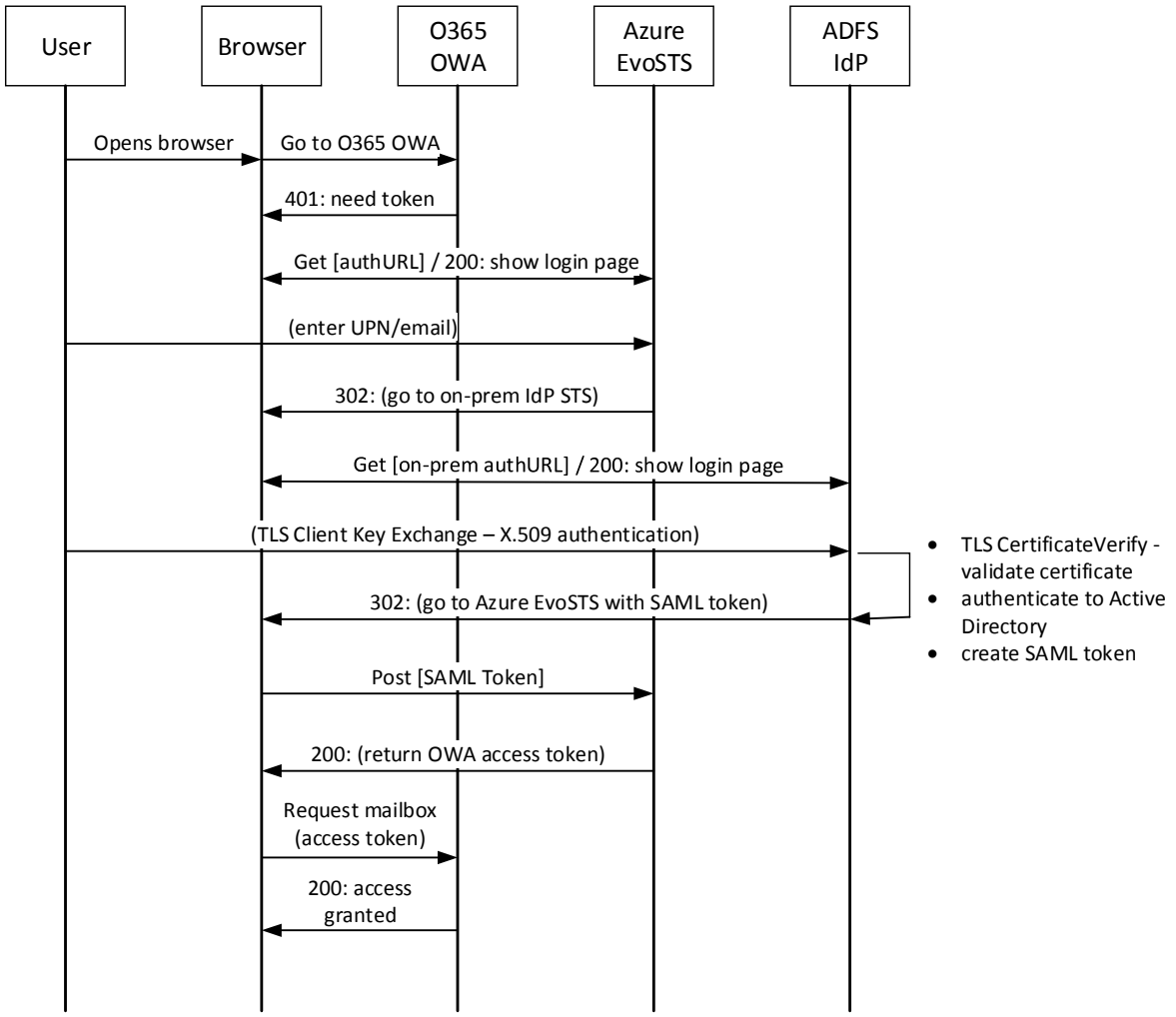


Figure 51: Office 365 OWA WS-Federation Workflow

The user opens his or her browser and enters the https://outlook.office365.com URL. The Azure EvoSTS renders a logon screen. The user enters his or her UPN into the first text box as shown in Figure 52.

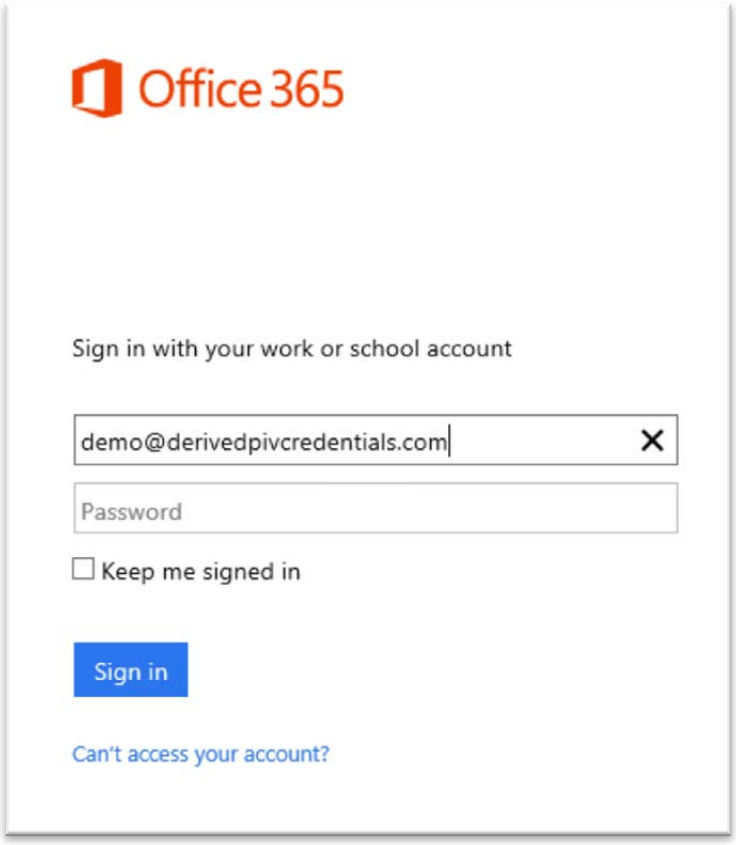


Figure 52: EvoSTS Authentication Page

The Azure EvoSTS performs home realm discovery on the supplied UPN (@derivedpivcredentials.com). Azure EvoSTS determines that this domain is federated and redirects the user's browser to the registered on-premises federation IdP STS (https://adfs.derivedpivcredentials.com/adfs/ls). The logon name field is populated with the value that was entered at the Azure EvoSTS as shown in Figure 53.

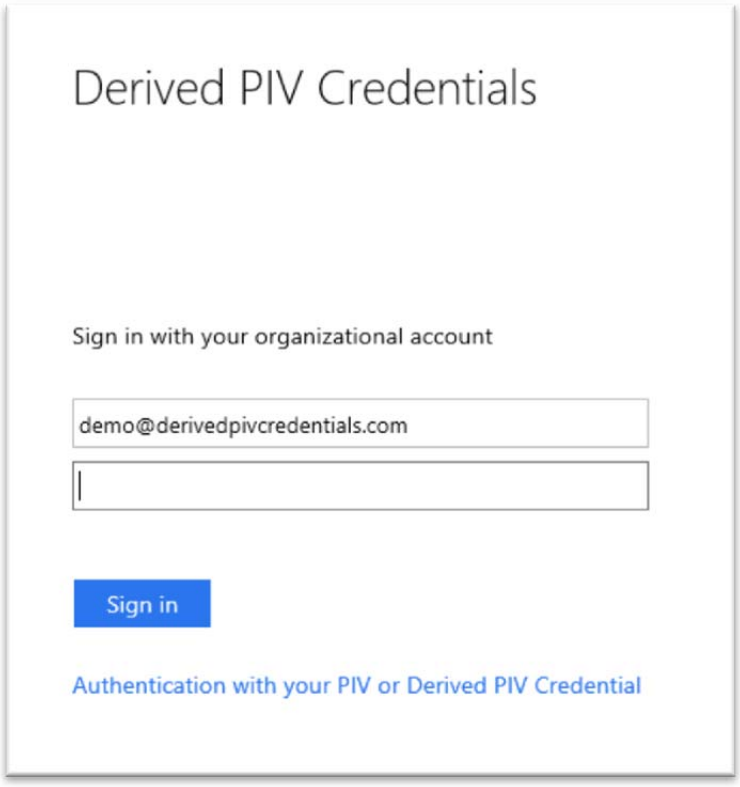
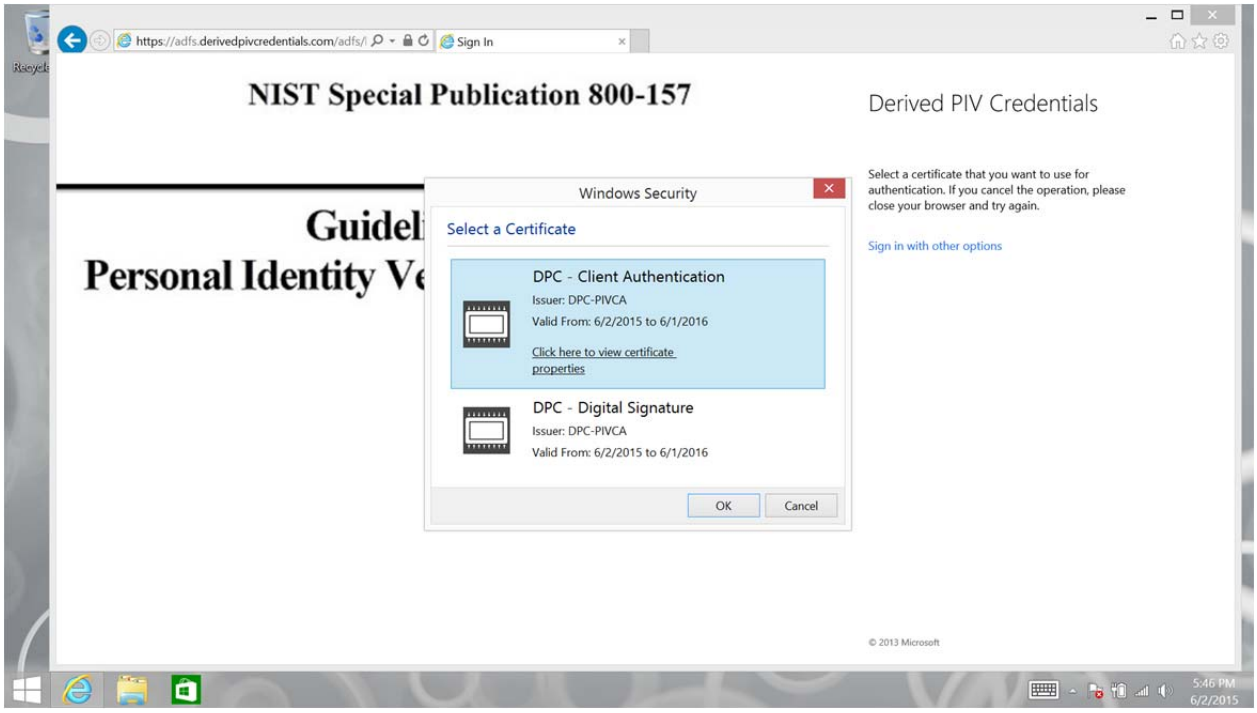


Figure 53: DerivedPIVCredentials.com ADFS Authentication Page

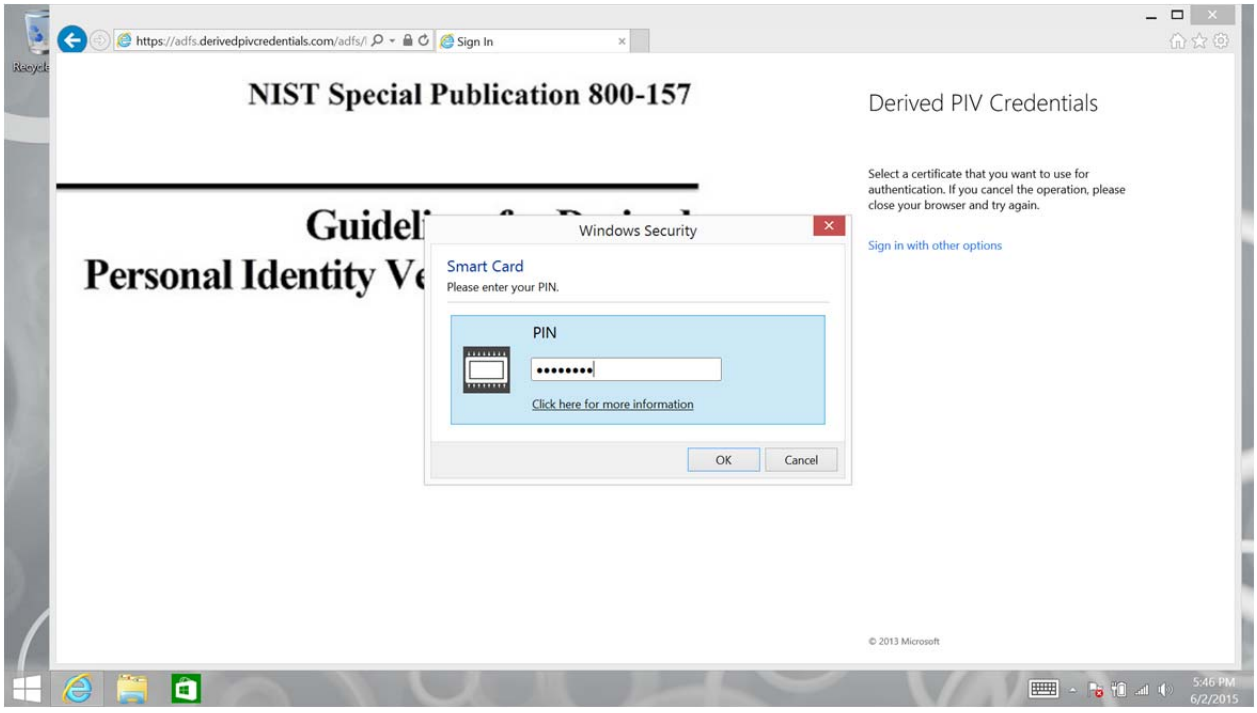
The user then selects "Authentication with your PIV or Derived PIV Credential" as shown in Figure 53.

Next, the user selects the Derived PIV Authentication certificate, as shown in Figure 54, to perform the TLS Client Key Exchange process, which starts after the user enters the PIN as shown in Figure 55.



1371

1372 **Figure 54: Certificate Selection**



1373

1374 **Figure 55: Derived PIV Authentication PIN**

1375 The DerivedPIVCredentials.com ADFS validates the DPC certificate (TLS CertificateVerify)
1376 and authenticates the user to the DerivedPIVCredentials.com AD domain. A SAML token is

returned to the Azure EvoSTS. The EvoSTS returns an OWA access token to the user's browser and it is presented to the Office 365 OWA endpoint. The user is now authenticated into his or her Office 365 mailbox as shown in Figure 56.

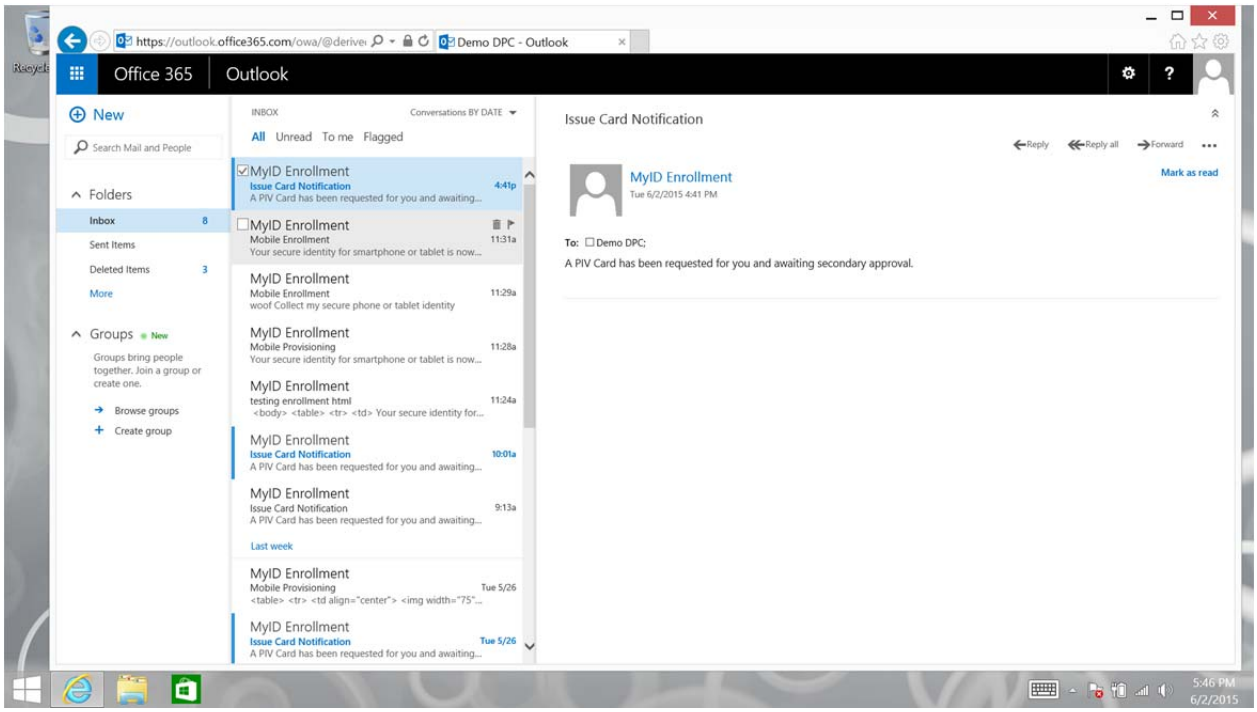


Figure 56: Office 365 Mailbox Outlook Web Access

The user can now use his or her Derived PIV End Entity Signature Certificate for S/MIME digital signature as shown in Figures 57 through 59. OWA S/MIME[39] requires the use of Internet Explorer 9 or higher, installation of the owasmime.msi ActiveX control available from outlook.office365.com, and the Derived PIV End Entity Signature Certificate described in Section 4.8.2 of this report.

[39] http://blogs.technet.com/b/exchange/archive/2014/12/15/how-to-configure-s-mime-in-office-365.aspx

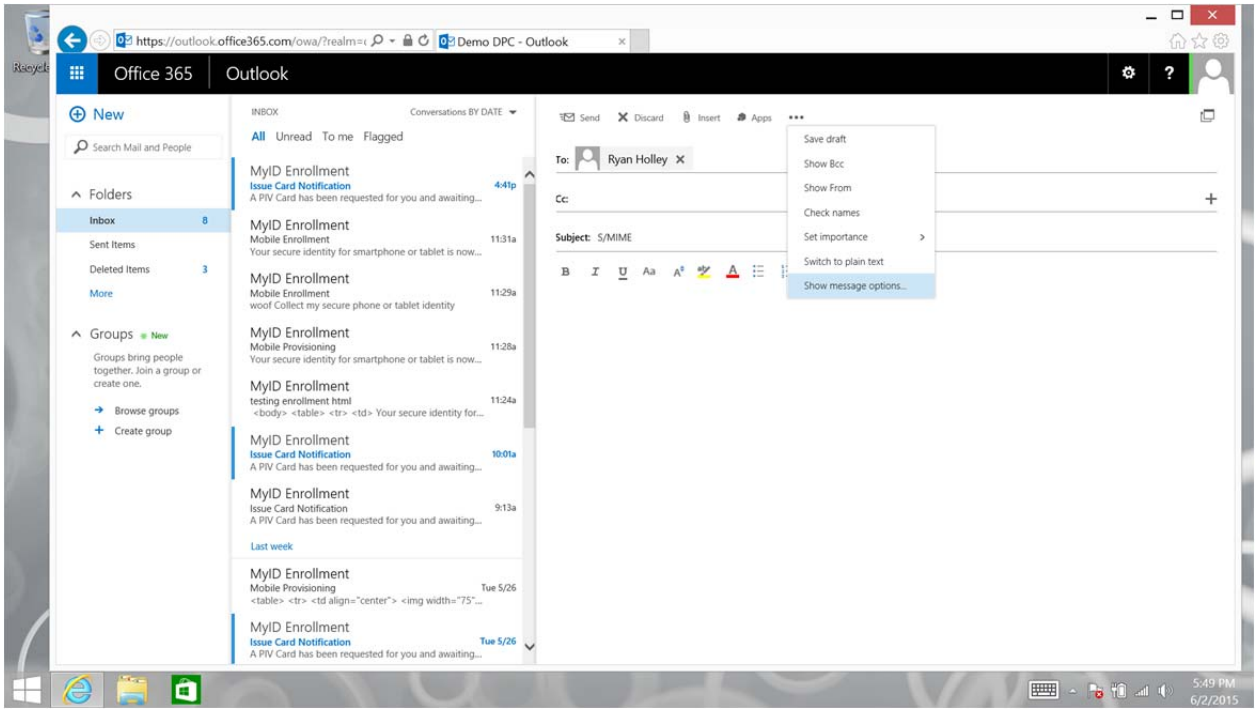


Figure 57: OWA S/MIME

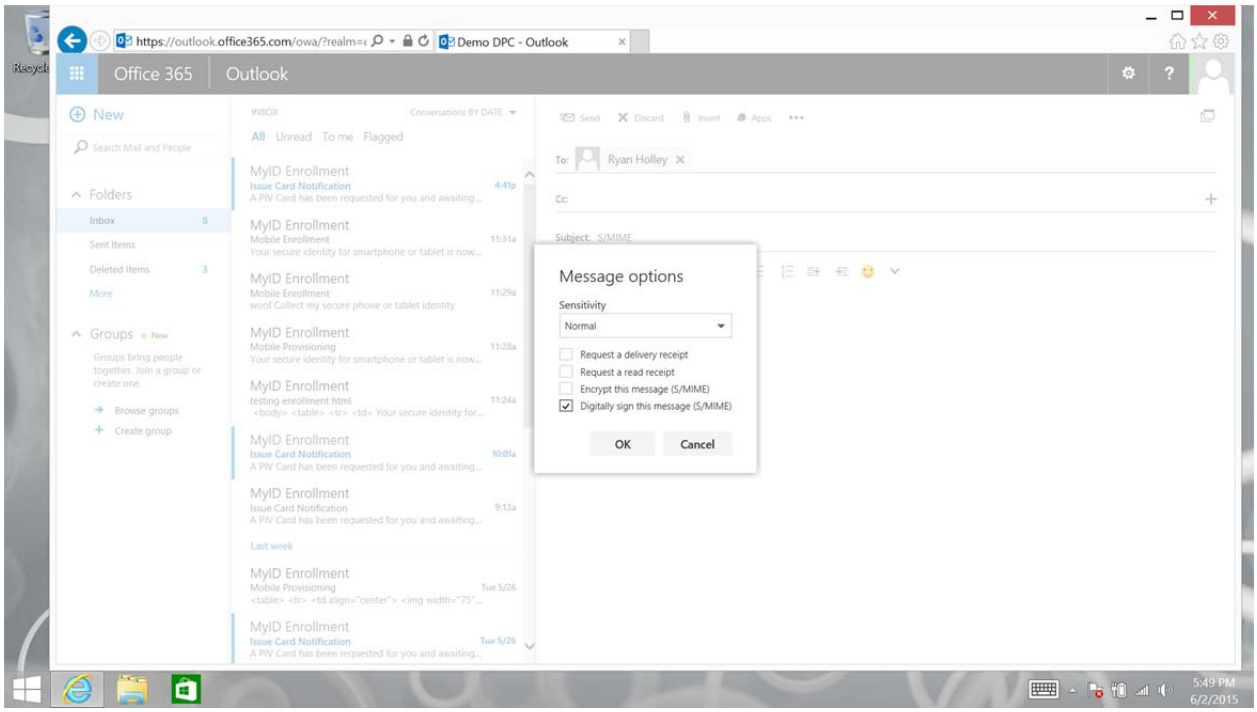


Figure 58: OWA S/MIME Digital Signature

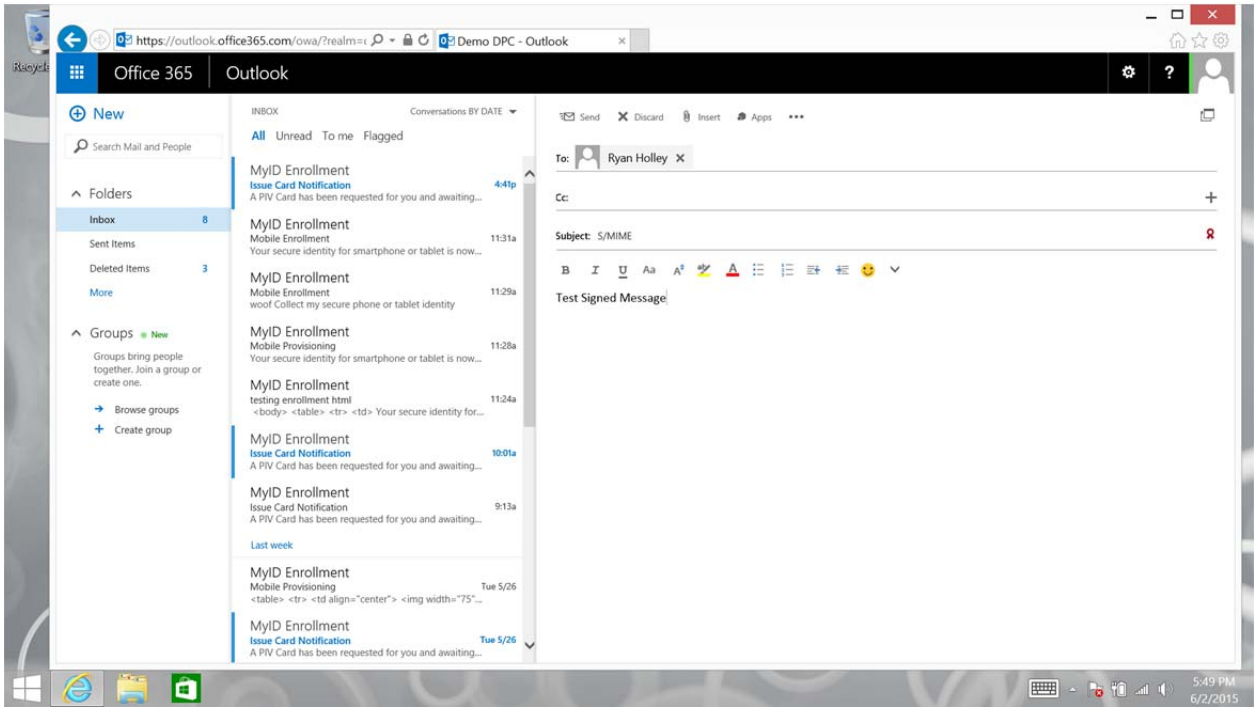


Figure 59: Digitally Signed Message

The recipient validates the signed message as shown in Figure 60.

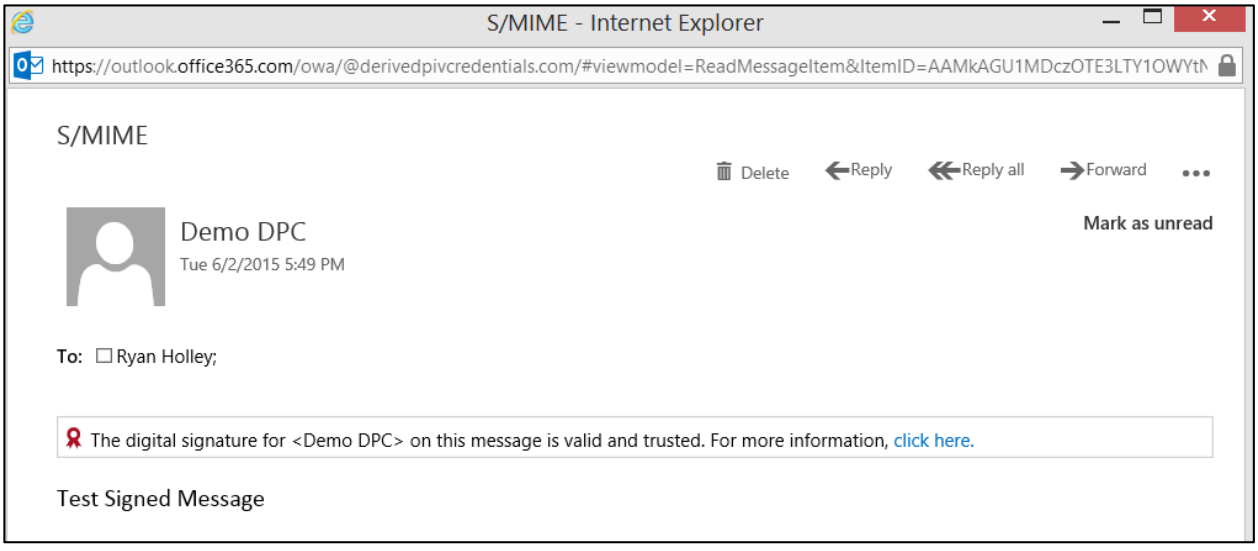


Figure 60: Validated Digitally Signed Message

8.2 Office 2013 Modern Authentication

Modern authentication[40] is Microsoft's implementation of the SAML 2.0 and OAuth 2.0 protocols for rich applications (non-browser-based) using the Microsoft Azure Active Directory Authentication Library (ADAL). ADAL is available on different platforms and allows client application developers to authenticate users to both on-premises AD and cloud-based resources.[41] ADAL is provided as an open source implementation.[42] The OAuth-based authentication stack used by new Office applications includes cross-platform support (e.g., iOS, Mac OS X, Android, Windows). The March 2015 update to Office 2013 includes production-ready ADAL functionality. With this update, Outlook 2013 can perform X.509 authentication to its Office 365 mailbox. At the time of this report, the associated Office 365 Exchange tenant must be enabled[43] for modern authentication, and the Outlook client must be configured to use modern authentication protocols.[44] The Outlook 2013 authentication workflow to an Office 365 mailbox is represented in Figure 61.

[40] https://blogs.office.com/2015/03/23/office-2013-modern-authentication-public-preview-announced/
[41] https://msdn.microsoft.com/en-us/library/azure/dn151135.aspx
[42] https://github.com/AzureAD
[43] http://aka.ms/publicpreview
[44] http://aka.ms/authadminhowto

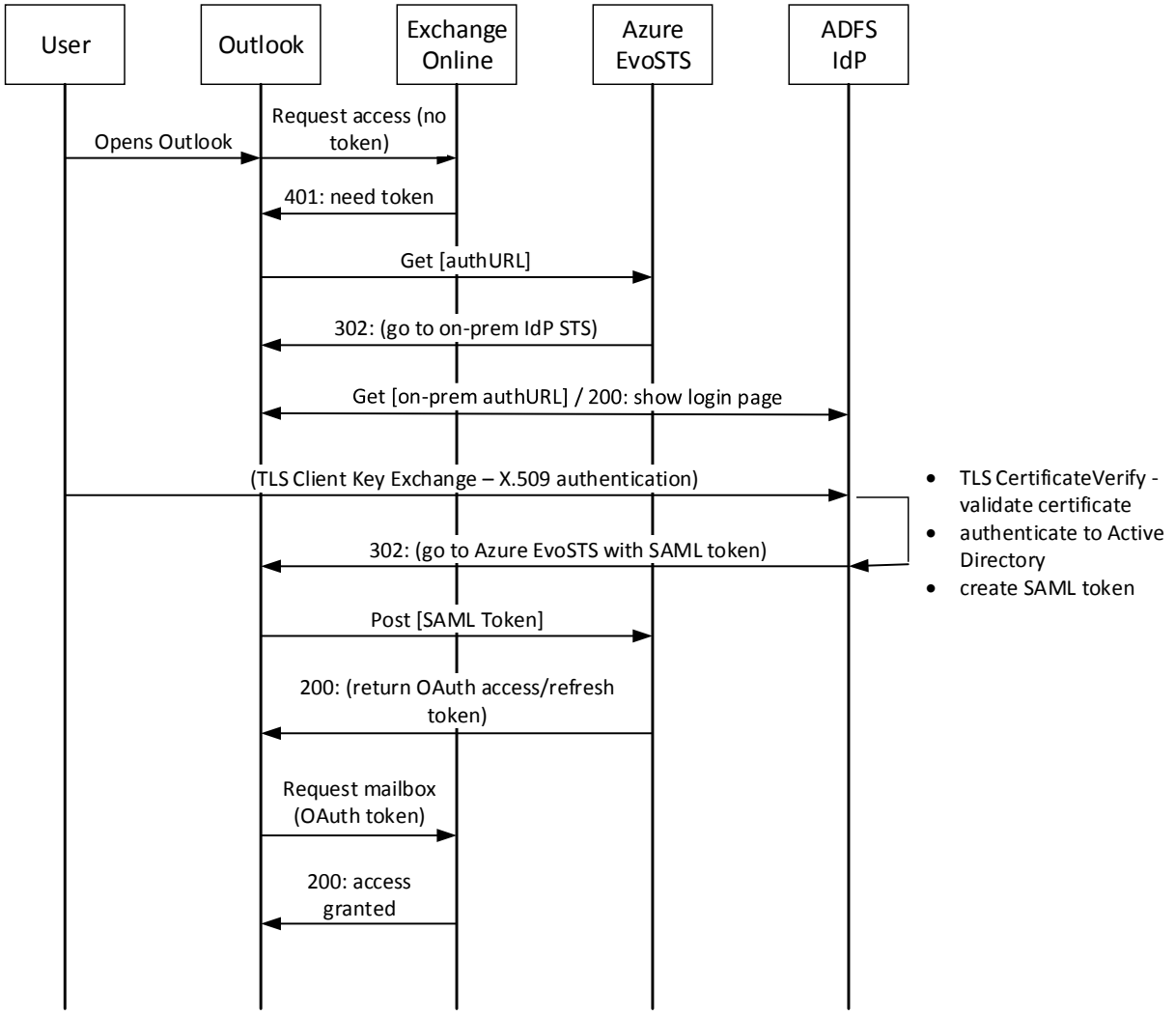
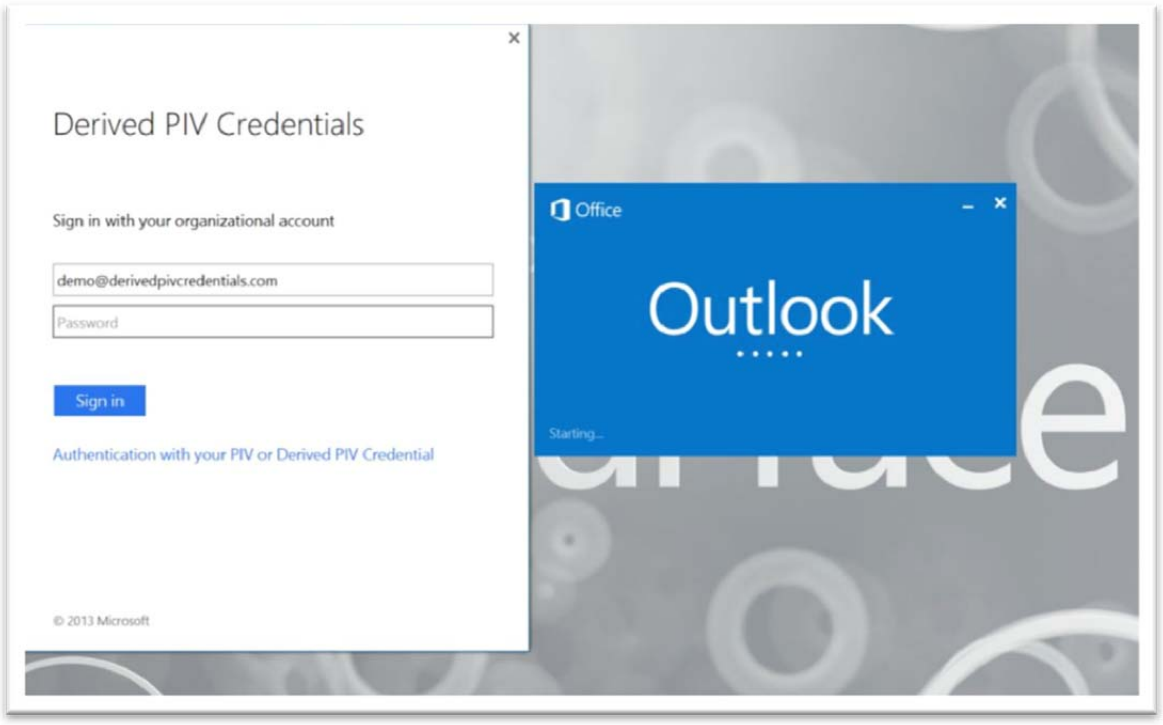


Figure 61: Office 365 / Outlook 2013 Modern Authentication Workflow

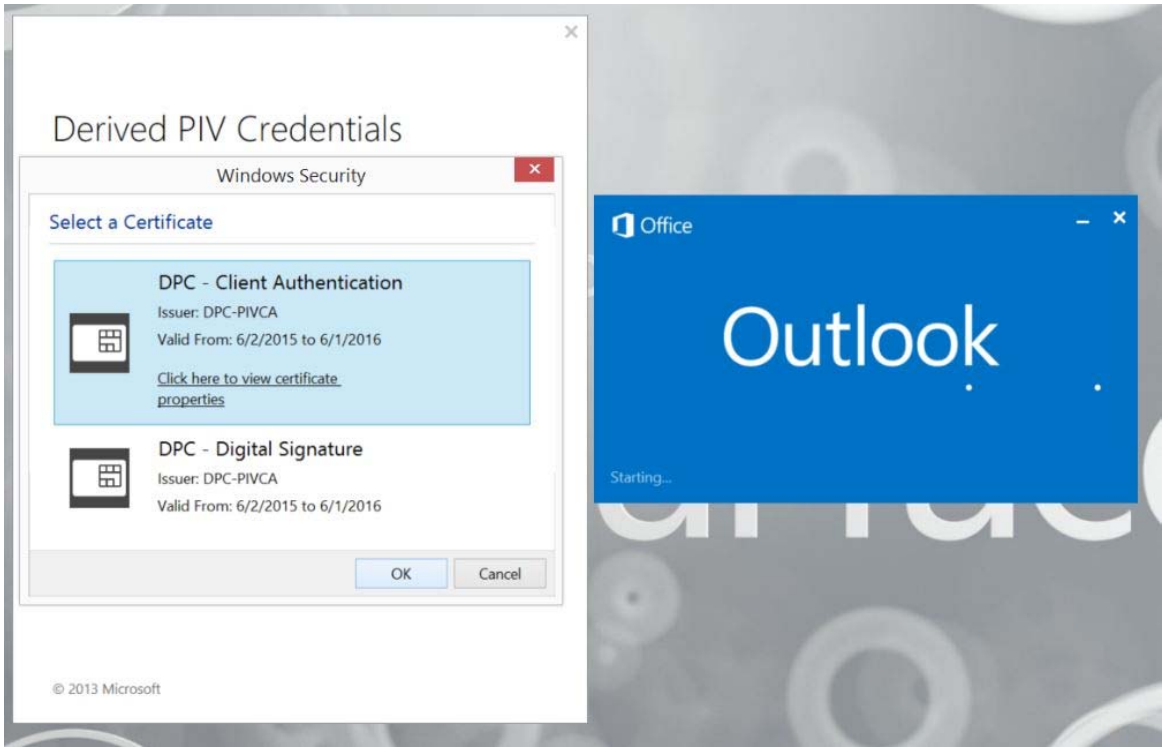
When the user starts a modern authentication-enabled Outlook client and Exchange auto-discovery has already been performed, the user's Outlook client is redirected to the on-premise IdP STS. The user selects "Authentication with your PIV or Derived PIV Credential" as shown in Figure 62.



1418

1419 **Figure 62: Office 365 / Outlook 2013 Modern Authentication Federation Logon**

1420 The user selects the Derived PIV Authentication certificate as shown in Figure 63.



1421

1422 **Figure 63: Office 365 / Outlook 2013 Modern Authentication Certificate Selection**

The user enters the PIN to perform the TLS Client Key Exchange process as shown in Figure 64.

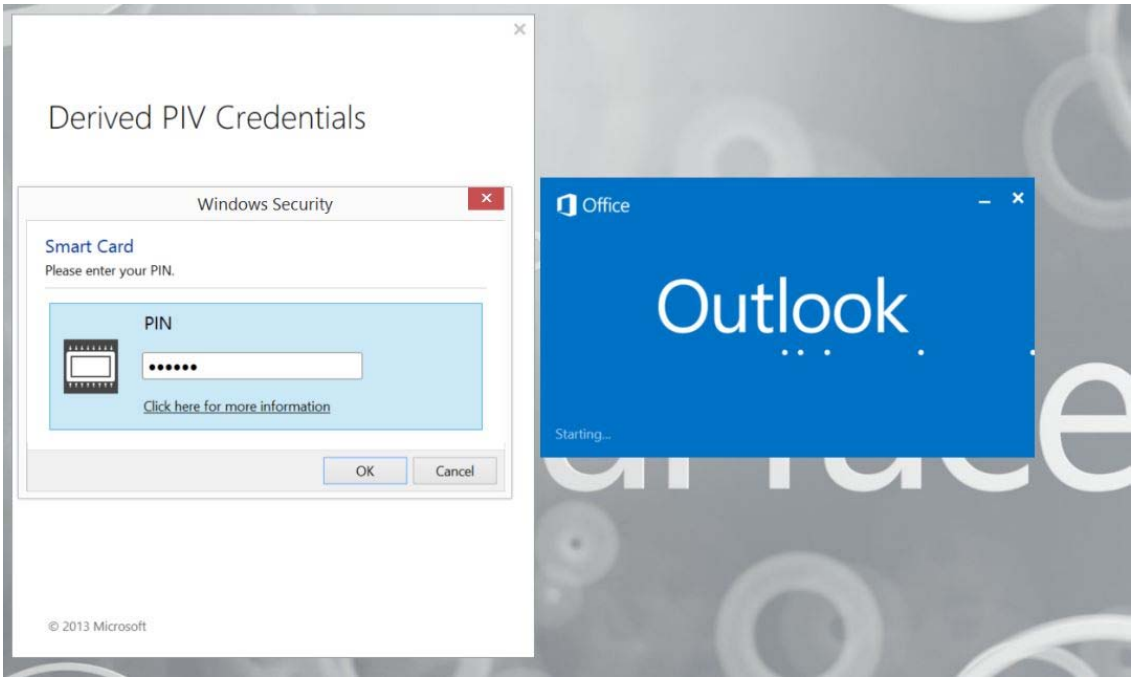


Figure 64: Office 365 / Outlook 2013 Modern Authentication PIN

The DerivedPIVCredentials.com ADFS validates the DPC certificate (TLS CertificateVerify) and authenticates the user to the DerivedPIVCredentials.com AD domain. A SAML 2.0 token is returned to the Azure EvoSTS. The EvoSTS returns an OAuth 2.0 access and refresh token to the user's Outlook client. The OAuth 2.0 access token is presented to the Office 365 Exchange Online mailbox endpoint. The user is now authenticated into his or her Office 365 mailbox as presented in Figure 65.

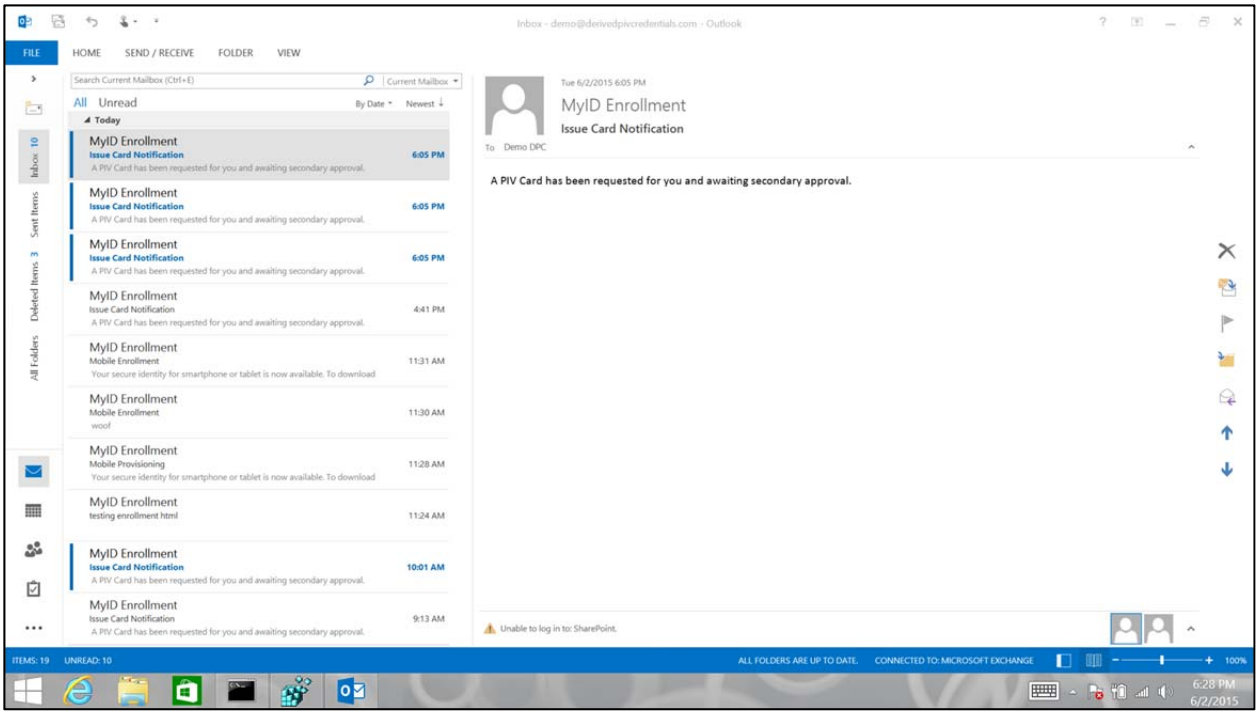


Figure 65: Office 365 / Outlook 2013 Modern Authentication Mailbox Access

The user's Outlook client can be configured to send S/MIME digitally signed and encrypted messages. The Outlook signature/encryption settings are configured in File \ Options \ Trust Center \ Trust Center Settings \ E-mail Security \ Encrypted e-mail, Default Settings \ Settings. For the Signature certificate, select the Derived PIV End Entity Signature Certificate, and set the Hash Algorithm to SHA256 as shown in Figure 66.

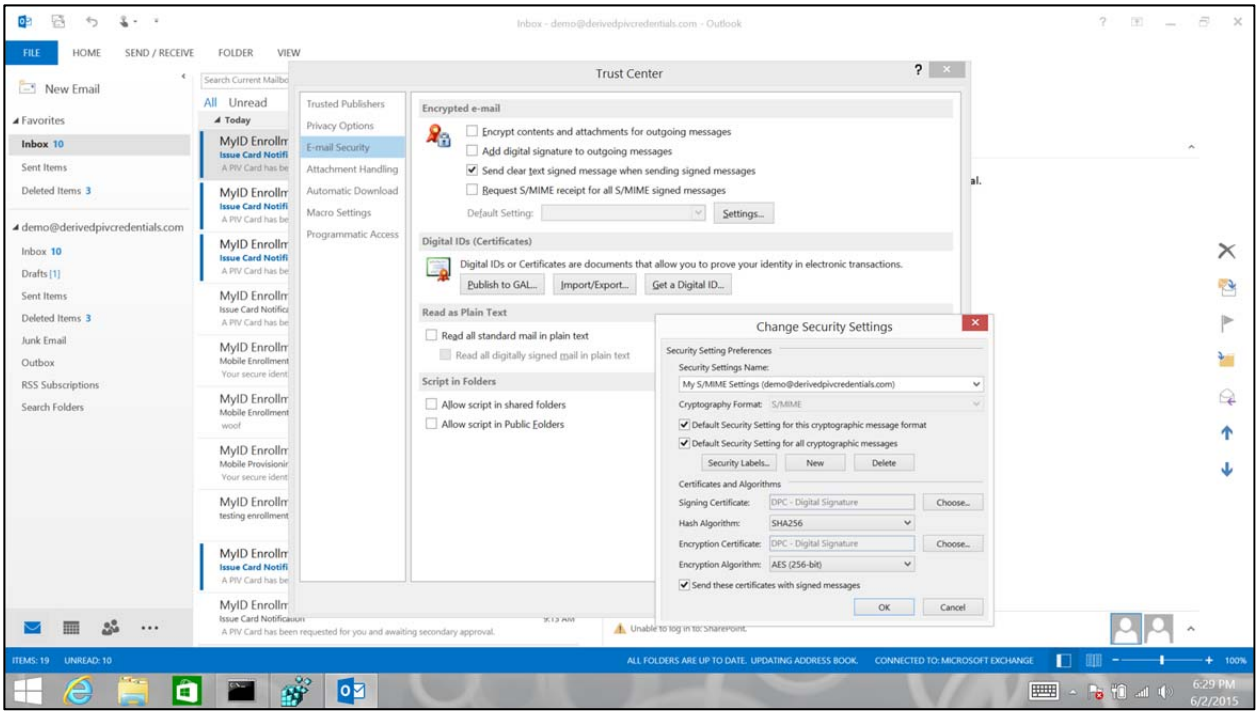


Figure 66: Outlook 2013 S/MIME Configuration

To sign a new message within the message, select Options, then Permission, and click “Sign” as shown in Figure 67.

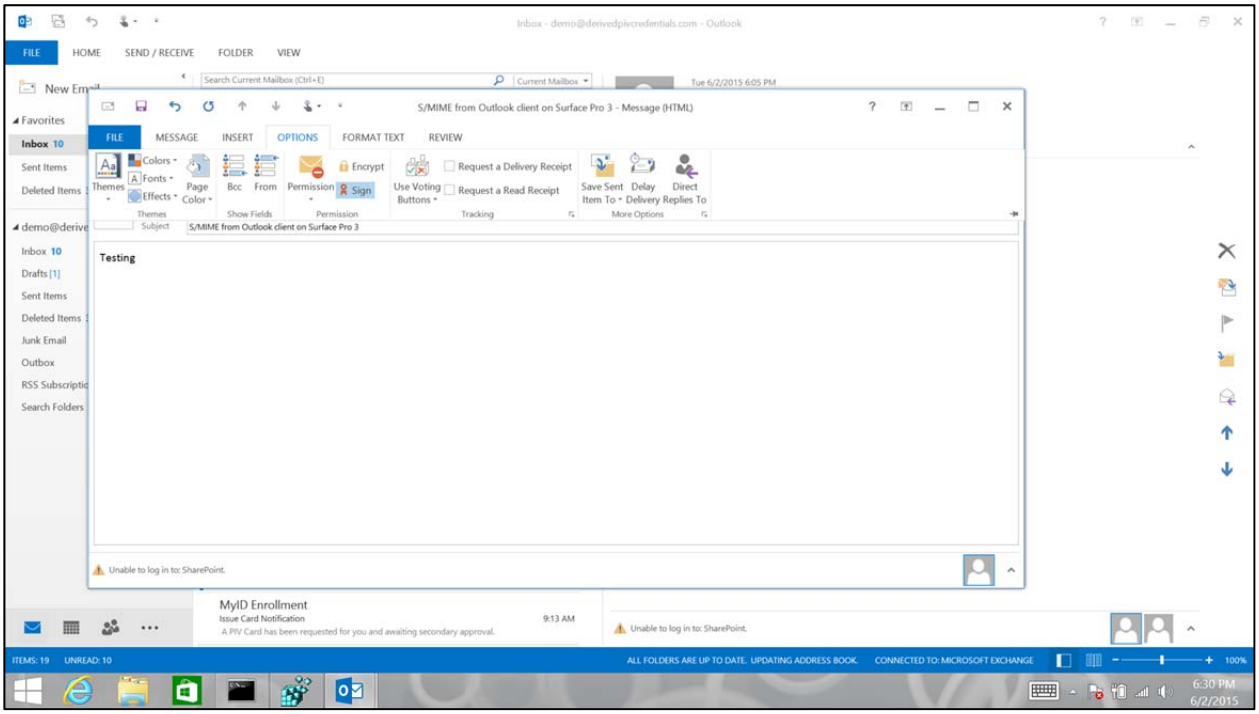


Figure 67: Outlook 2013 S/MIME Digitally Signed Message

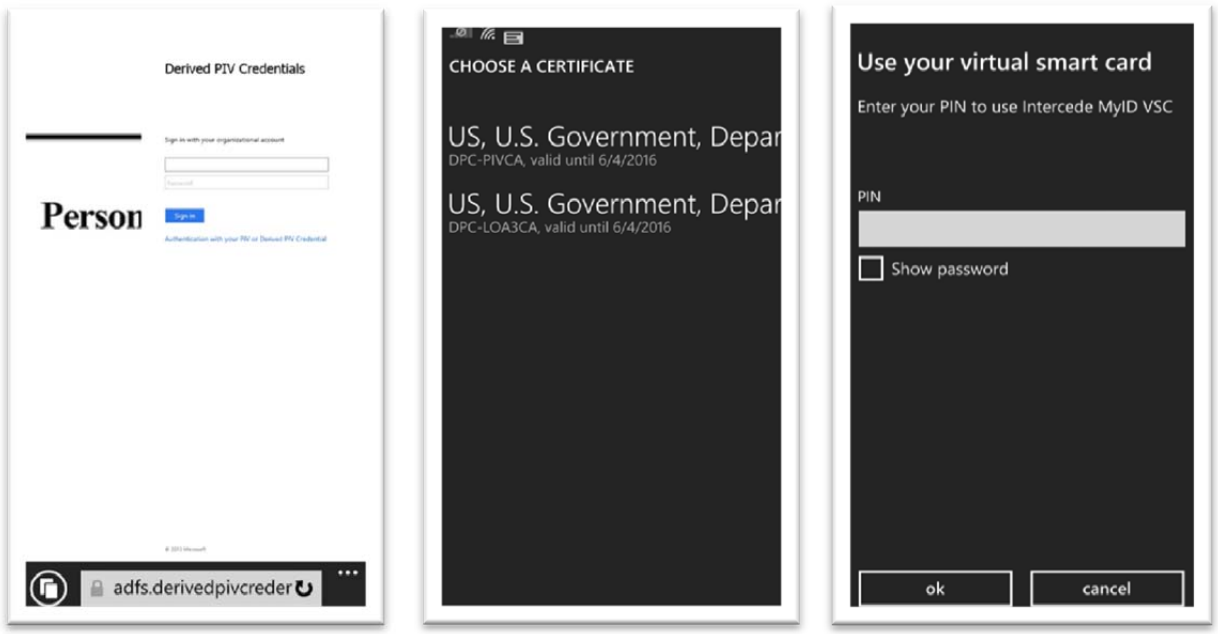
8.3 ASP.NET Claim Application

A sample claims-based application is published through the DerivedPIVCredentials.com ADFS Web Application Proxy. This sample application is available in the Windows Identity Foundation SDK[45] and is configured as a Relying Party on the DerivedPIVCredentials.com ADFS. The application uses the WS-Federation passive profile and renders all claims that are returned within the SAML token. The Windows Server 2012R2 ADFS includes new claim values that can be used to ensure the methods of authentication.[46] In this scenario the user will use the Windows Phone 8.1, LOA-3, Derived PIV authentication VSC for authentication. The authentication certificate contains the OID 2.16.840.1.101.3.2.1.48.173 within the policyIdentifier extension to signify it as an id-fpki-common-pivAuth-derived (LOA-3) credential. When the user authenticates to the ADFS IdP using this credential, the SAML token will contain the claim http://schemas.microsoft.com/2012/12/certificatecontext/extension/certificatepolicy with the value of 2.16.840.1.101.3.2.1.48.173. Other certificate extension values can be returned as claims (e.g., Enhanced Key Usage, Key Usage, Subject Name, Authority Key Identifier). The claims within the SAML token are rendered within the user's browser.

On the Windows 8.1 phone, the user starts Internet Explorer and goes to https://claimapp.derivedpivcredentials.com/claimapp. The user's browser is redirected to the DerivedPIVCredentials.com ADFS IdP STS and is presented with the logon page. The user selects "Authentication with your PIV or Derived PIV Credential." The user selects the Derived PIV Authentication certificate and enters the PIN to perform the TLS Client Key Exchange process. Figure 68 shows this scenario.

[45] http://www.microsoft.com/download/details.aspx?id=4451

[46] http://blogs.msdn.com/b/ramical/archive/2014/01/30/under-the-hood-tour-on-multi-factor-authentication-in-ad-fs-part-1-policy.aspx



1468

1469 **Figure 68: Windows Phone DPC Certificate Selection and PIN**

1470 The ADFS server validates the certificate (TLS CertificateVerify), authenticates the user to the
1471 DerivedPIVCredentials.com AD domain, and generates a SAML token that is returned to the
1472 application. The contents are rendered within the browser as shown in Figure 69.

1473

Figure 69: Claims Generated by ADFS IdP

Access can be based upon the enforcement of the requirement of specific claim values. This determination can be made by the IdP STS Issuance Authorization Claim rule or within the application's logic.

9 Next Steps

This report represents a reference implementation developed as part of the experimental research performed during the development of NIST SP 800-157 using commercially available technologies that were available to the NIST Computer Security Division. It showed the issuance, usage, maintenance, and termination of LOA-3 DPCs for cloud-based authentication and S/MIME digital signatures using embedded software and hybrid software/hardware tokens.

Additional research will be performed to support the following capabilities and usage scenarios in order to help organizations deploy DPC in operational environments:

- LOA-4 DPC FIPS 140-2 validated tokens
- S/MIME encryption
- Leveraging other hardware cryptographic modules such as Trusted Execution Environment and Intel Identity Protection Technology
- SSP-provisioned PIV credentials and DPCs issued using a different IDMS and PKI
- BAE to support DPC issuance to PIV cardholder Applicants from another issuer
- Usability of the DPC by providing consistent user experience across devices
- Sample assessment and authorization procedure

The National Cybersecurity Center of Excellence (NCCoE) has created a Building Block[47] for entities that want to demonstrate their capabilities in compliance with NIST SP 800-157 guidance. The practice guides that are developed as an outcome of the Building Block will support a diverse set of technologies and IT products, and they will provide greater details for organizations to adopt and build DPC pilots in different operational environments.

[47] http://nccoe.nist.gov/derivedcredentials

Appendix A—DPC Requirement Mappings

This appendix contains mappings between the DPC requirements from this report and requirements from other federal government standards and guidelines.

A.1 NISTIR 8055 Requirements Enumeration and Implementation Mappings

Table 5 enumerates the requirements presented in Section 2.3, assigning each a requirement number, and maps these requirements to their implementations in Sections 4 through 7.

Table 5: NISTIR 8055 Requirements Definition and Implementation Mappings

Requirement Category	Req. Number	Req. Section Number	Requirement Name	NISTIR 8055 Implementation Mapping
RC1 - Device and Cryptographic Token	RC1.1	2.3.1.1	Private key in cryptographic module	Windows Virtual Smart Card protected by TPM (section 4.8.5) Android and iOS protected by MyID Identity Agent (section 4.8.6)
	RC1.2	2.3.1.2	Alternative tokens	N/A
	RC1.3	2.3.1.7	Digital signature and key management keys on the device	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	Termination (section 7)
	RC1.5	2.3.3.5.2	Zeroize or destroy the token due to transfer of token or device to another individual	Termination (section 7)
	RC1.6	2.3.3.5.3	Zeroize or destroy the token due to no longer being eligible to have a PIV Card	Termination (section 7)
	RC1.7	2.3.3.5.4	Zeroize or destroy the token due to no longer being eligible to have a DPC	Termination (section 7)
	RC1.8	2.3.5.3.1.1	Removable hardware cryptographic tokens: interface of PIV Card	N/A
	RC1.9	2.3.5.3.1.2	Removable hardware cryptographic tokens: secure element	N/A
	RC1.10	2.3.5.3.1.3	Removable hardware cryptographic tokens: NIST SP 800-157 Appendix B APDU command interface	N/A
	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	N/A
	RC1.12	2.3.5.3.1.5.1	Removable hardware cryptographic tokens: SD card with cryptographic module: on-board secure element or security system	N/A
	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	N/A
	RC1.14	2.3.5.3.1.6.1	Removable hardware cryptographic tokens: UICC: separate security domain for Derived PIV Application	N/A

Requirement Category	Req. Number	Req. Section Number	Requirement Name	NISTIR 8055 Implementation Mapping
	RC1.15	2.3.5.3.1.6.2	Removable hardware cryptographic tokens: UICC: NIST SP 800-157 Appendix B APDU command interface	N/A
	RC1.16	2.3.5.3.1.6.3	Removable hardware cryptographic tokens: UICC: *GlobalPlatform Card Secure Element Configuration v1.0*	N/A
	RC1.17	2.3.5.3.1.7.1	Removable hardware cryptographic tokens: USB token with cryptographic module: integrated secure element with *Smart Card ICCD Specification for USB Integrated Circuit Card Devices*	N/A
	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	N/A
	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	N/A
	RC1.20	2.3.5.3.2.1	Embedded cryptographic tokens: Hardware or software cryptographic module	Windows Virtual Smart Card protected by TPM (section 4.8.5) Android and iOS protected by MyID Identity Agent (section 4.8.6)
	RC1.21	2.3.5.3.2.2	Embedded cryptographic tokens: Software cryptographic module at LOA-3	Token descriptions (section 4.8.4)
	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	Token descriptions (section 4.8.4)
	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	Certificate profiles assert test OIDs (section 4.8.2)
	RC1.24	2.3.5.3.2.5	Embedded cryptographic tokens: Other keys stored in the same cryptographic module	Windows Virtual Smart Card protected by TPM (section 4.8.5) Android and iOS protected by MyID Identity Agent (section 4.8.6)
	RC1.25	2.3.5.4.6	Embedded cryptographic tokens: authentication mechanism implemented by hardware or software mechanism outside of cryptographic boundary at LOA-3	Windows Virtual Smart Card protected by TPM (section 4.8.5) Android and iOS protected by MyID Identity Agent (section 4.8.6)
	RC1.26	2.3.5.4.7	Implementation and enforcement of authentication mechanism by cryptographic module at LOA-4	N/A
	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	PIN unblock (section 6.2)
RC2 - PIV Card	RC2.1	2.3.1.4	Identity proofing	PIV already issued by MyID CMS (section 5)
	RC2.2	2.3.1.5	Proof of possession of a valid PIV Card	MyID self-service kiosk issuance (section 5.2)

Requirement Category	Req. Number	Req. Section Number	Requirement Name	NISTIR 8055 Implementation Mapping
				MyID LOA-3 remote issuance (section 5.3)
	RC2.3	2.3.2.1	Verification of Applicant's PIV authentication for issuance	MyID self-service kiosk issuance (section 5.2) MyID LOA-3 remote issuance (section 5.3)
	RC2.4	2.3.2.2	Revocation status of PIV authentication certificate checked after seven days of issuance	Revocation of Applicant's PIV Card within seven days of kiosk-based DPC issuance (section 5.2.1)
	RC2.5	2.3.2.10	Issuance of multiple DPCs	Issuance (section 5)
RC3 - PKI	RC3.1	2.3.1.3	PKI-based DPCs at LOA-3 and LOA-4	PKI (section 4.4)
	RC3.2	2.3.1.6	X.509 public key certificate	Issuance (section 5)
	RC3.3	2.3.3.6	Issuance of Derived PIV Authentication certificate as a result of Subscriber name change	Reissuance (section 6.1)
	RC3.4	2.3.5.1.2	Worksheet 10: Derived PIV Authentication Certificate Profile found in *X.509 Certificate and Certificate Revocation List (CRL) Profile for the Shared Service Providers (SSP) Program*	*X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program* (section 4.8.2)
	RC3.5	2.3.5.1.3	No dependency with expiration date of the Derived PIV Authentication certificate with PIV Card	Expiration date based upon certificate profiles
	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	Certificate profiles based upon *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program* (section 4.8.2)
RC4 - Level of Assurance	RC4.1	2.3.2.3	LOA-3 or LOA-4	Only LOA-3 issuance, maintenance, termination and usage demonstrated within this report
	RC4.2	2.3.2.4	LOA-3 DPC issued in person or remotely	MyID self-service kiosk issuance (section 5.2) MyID remote issuance (section 5.3)
	RC4.3	2.3.2.5	Authenticated and protected channel for remote issuance	MyID self-service kiosk issuance (section 5.2) MyID remote issuance (section 5.3)
	RC4.4	2.3.2.6	Identification of each encounter in issuance process involving two or more electronic transactions	MyID remote issuance (section 5.3)
	RC4.5	2.3.2.7	Identification of Applicant using biometric sample for LOA-4	N/A
	RC4.6	2.3.2.8	Identification of each encounter in issuance process involving two or more electronic transactions of Applicant using biometric sample for LOA-4	N/A
	RC4.7	2.3.2.9	Retain biometric sample of Applicant for LOA-4	N/A
	RC4.8	2.3.3.1	Communication over mutually authenticated secure sessions between issuer and cryptographic module for LOA-4	N/A

Requirement Category	Req. Number	Req. Section Number	Requirement Name	NISTIR 8055 Implementation Mapping
	RC4.9	2.3.3.2	Encrypted and integrity checks for data transmitted between issuer and cryptographic module for LOA-4	N/A
	RC4.10	2.3.3.3	Re-key of and expired or compromised DPC	Reissuance (section 6.1)
	RC4.11	2.3.3.4	Re-key of and expired or compromised DPC to new hardware token at LOA-4	N/A
	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	*X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program* for LOA-3 (section 4.8.2)
	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	N/A
	RC4.14	2.3.5.2.3	Key pair generated in cryptographic module validated to FIPS 140 level 1 or higher for LOA-3	Windows Virtual Smart Card protected by TPM (section 4.8.5) Android and iOS protected by MyID Identity Agent (section 4.8.6)
RC5 - Credential Management System	RC5.1	2.3.4.1	Issuance of a DPC based on information of Applicant's PIV Card	DPC Initial Issuance (section 5)
	RC5.2	2.3.4.2	Periodically check the status of the PIV Card	PIV and DPC tied to the same Subscriber record within MyID
	RC5.3	2.3.4.3.1	Termination status of PIV Card checked every 18 hours via notification system	Termination (section 7)
	RC5.4	2.3.4.3.2	Termination of the PIV and DPC record on an integrated management system	Termination (section 7)
	RC5.5	2.3.4.4	Track beyond the revocation of the PIV Authentication certificate	Both PIV card and DPC are provisioned by the same CMS
	RC5.6	2.3.4.5.1	Direct access to the PIV Card information for integrated PIV and DPC system	Both PIV card and DPC are provisioned by the same CMS
	RC5.7	2.3.4.5.2.1	Access to the BAE	N/A
	RC5.8	2.3.4.5.2.2	Notification of DPC system issuer with Issuer of PIV Card	N/A
	RC5.9	2.3.4.5.2.3	Access to the URRS for termination status	N/A
	RC5.10	2.3.5.4.1	Password-based Subscriber authentication for Derived PIV Authentication private key	PIN required for private key access
	RC5.11	2.3.5.4.2	Password is not guessable or individually identifiable	MyID enforced PIN policy
	RC5.12	2.3.5.4.3	Minimum password length of six characters	MyID enforced PIN policy
	RC5.13	2.3.5.4.4	Block use of Derived PIV Authentication key after a number of consecutive failed activation attempts	Windows virtual smart card blocks PIN after five failed PIN attempts
	RC5.14	2.3.5.4.5	Limit number of attempts over period of time with throttling mechanisms	Windows Virtual Smart Card protected by TPM (section 4.8.5)

Requirement Category	Req. Number	Req. Section Number	Requirement Name	NISTIR 8055 Implementation Mapping
	RC5.15	2.3.5.4.8.1	Password reset in-person: Authentication via PKI-AUTH mechanism with Subscriber's PIV Card	PIN unblock (section 6.2)
	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	N/A
	RC5.17	2.3.5.4.9.1	Password reset remotely: Authentication via PKI-AUTH mechanism with Subscriber's PIV Card	PIN unblock (section 6.2)
	RC5.18	2.3.5.4.9.2	Password reset remotely: Strong linkage between the PKI-AUTH session and reset session	PIN unblock (section 6.2)
	RC5.19	2.3.5.4.9.3	Password reset remotely: Same Subscriber for the DPC and the PIV Card	PIN unblock (section 6.2)
	RC5.20	2.3.5.4.9.4	Password reset remotely: Reset completed over a protected session	PIN unblock (section 6.2)

A.2 LOA Mapping to Cryptographic Tokens for the POC

Table 6 summarizes the DPC proof of concept implementation LOA and associated cryptographic tokens.

Table 6: LOA Mapping to Cryptographic Tokens

NIST SP 800-63-2 Assurance Level	PIV Assurance Level	Target Guidance: M-06-16 /M-07-16 for Separate Tokens	Target Guidance: Future Alternate OMB Guidance for Integrated Tokens	Cryptographic Token FIPS 140-2 Validation Level	Cryptographic Token Type	PIV Derived Authentication Certificate Policy	Enrollment Method
LOA-3	Very High	No	✓	FIPS 140-2 Level 1	Hybrid hardware/software token • Windows 8.1 • TPM • Microsoft CSP	id-fpki-common-pivAuth-derived	Remote enrollment
LOA-3	High	No	✓	FIPS 140-2 Level 1	Software token • Android/iOS • MyID Identity Agent	id-fpki-common-pivAuth-derived	Remote enrollment

A.3 Supporting NIST SP 800-53 Security Controls and Publications

The major controls in the NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*[48] control catalog that affect the DPC proof of concept research are:

AC-7, Unsuccessful Logon Attempts

Related controls: AC-2, AC-9, AC-14, IA-5

AC-19, Access Control for Mobile Devices

Related controls: AC-3, AC-7, AC- 18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4

References: OMB M-06-16; NIST SPs 800-114, 800-124, and 800-164

CM-3, Configuration Change Control

Related controls: CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12

References: NIST SP 800-128

IA-2, Identification and Authentication (Organizational Users)

Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8

References: HSPD-12; OMB M-04-04, 06-16, 11-11; FIPS 201; NIST SPs 800-63, 800-73, 800-76, 800-78; Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance; idmanagement.gov

IA-4, Identifier Management

Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37

References: FIPS 201; NIST SPs 800-73, 800-76, 800-78

IA-5, Authenticator Management

Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28

References: OMB M-04-04, 11-11; FIPS 201; NIST SPs 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; idmanagement.gov

[48] *Security and Privacy Controls for Federal Information Systems and Organizations*, http://dx.doi.org/10.6028/NIST.SP.800-53r4

SC-8, Transmission Confidentiality and Integrity
Related controls: AC-17, PE-4
References: FIPS 140-2, 197; NIST SPs 800-52, 800-77, 800-81, 800-113; Committee on National Security Systems (CNSS) Policy 15; National Security Telecommunications and Information Systems Security (NSTISSI) No. 7003

SC-12, Cryptographic Key Establishment and Management
Related controls: SC-13, SC-17
References: NIST SPs 800-56, 800-57

SC-13, Cryptographic Protection
Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7
References: FIPS 140-2; csrc.nist.gov/cryptval, www.cnss.gov

SC-17, Public Key Infrastructure Certificates
Related control: SC-12
References: OMB M-05-24; NIST SPs 800-32, 800-63

Information on these controls and guidelines on possible implementations can be found in the following publications:

- *Committee on National Security Systems (CNSS) Policy 15*
- *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0*
- *FIPS 140-2, Security Requirements for Cryptographic Modules*
- *FIPS 197, Advanced Encryption Standard*
- *FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors*
- *HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors*
- *National Security Telecommunications and Information Systems Security (NSTISSI) No. 7003, Protective Distribution Systems (PDS)*
- *SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure*
- *SP 800-52 Rev. 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*

- *SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations*
- *SP 800-53A Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations*
- *SP 800-63-2, Electronic Authentication Guideline*
- *SP 800-73-4, Interfaces for Personal Identity Verification*
- *SP 800-76-2, Biometric Specifications for Personal Identity Verification*
- *SP 800-77, Guide to IPsec VPNs*
- *SP 800-78-4, Cryptographic Algorithms and Key Sizes for Personal Identity Verification*
- *SP 800-81-2, Secure Domain Name System (DNS) Deployment Guide*
- *SP 800-113, Guide to SSL VPNs*
- *SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access*
- *SP 800-124 Rev. 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise*
- *SP 800-128, Guide for Security-Focused Configuration Management of Information Systems*
- *SP 800-164 (Draft), Guidelines on Hardware-Rooted Security in Mobile Devices*
- *OMB M-04-04, E-Authentication Guidance for Federal Agencies*
- *OMB M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
- *OMB M-06-16, Protection of Sensitive Agency Information*
- *OMB M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*

A.4 Cybersecurity Framework Subcategory Mappings

Major security features of the DPC proof of concept research map to the following subcategories from the Cybersecurity Framework:[49]

- PR.AC-1: Identities and credentials are managed for authorized devices and users
- PR.AC-3: Remote access is managed
- PR.DS-2: Data-in-transit is protected

[49] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, NIST, February 12, 2014. http://www.nist.gov/cyberframework/index.cfm

1612 • PR.DS-5: Protections against data leaks are implemented

1613 • PR.IP-3: Configuration change control processes are in place

1614

Appendix B—Acronyms and Abbreviations

Acronyms and abbreviations used in this report are defined below.

AD	Active Directory
ADAL	Active Directory Authentication Library
ADCS	Active Directory Certificate Services
ADDS	Active Directory Domain Services
ADFS	Active Directory Federation Services
AMA	Authentication Mechanism Assurance
APDU	Application Protocol Data Unit
API	Application Programming Interface
BAE	Backend Attribute Exchange
CA	Certificate Authority
CHUID	Card Holder Unique Identifier
CMS	Credential Management System
CNSS	Committee on National Security Systems
CRL	Certificate Revocation List
CSOR	Computer Security Objects Register
CSP	Cryptographic Service Provider
DN	Distinguished Name
DNS	Domain Name System
DPC	Derived PIV Credential
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard
HSPD	Homeland Security Presidential Directive
IaaS	Infrastructure as a Service
ICC	Integrated Circuit Card
ICCD	Integrated Circuit Card Device
IDMS	Identity Management System
IdP	Identity Provider
IdP STS	Identity Provider Security Token Service
IP	Internet Protocol
IR	Interagency Report or Internal Report
IT	Information Technology
ITL	Information Technology Laboratory
KDC	Key Distribution Center
LOA	Level of Assurance
MAG	Microsoft Azure Government
MDM	Mobile Device Management
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSTISSI	National Security Telecommunications and Information Systems Security
OID	Object Identity
OMB	Office of Management and Budget
OS	Operating System

OWA	Outlook Web Access
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
QR	Quick Response
RA	Registration Authority
RRAS	Routing and Remote Access Service
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAML	Security Assertion Markup Language
SD	Secure Digital
SDK	Software Development Kit
SE	Secure Element
SIM	Subscriber Identity Module
SMS	Short Message Service
SP	Special Publication
SSP	Shared Service Provider
TLS	Transport Layer Security
TPM	Trusted Platform Module
UICC	Universal Integrated Circuit Card
UPN	UserPrincipalName
URL	Uniform Resource Locator
URRS	Uniform Reliability and Revocation Service
USB	Universal Serial Bus
VNet	Virtual Network
VPN	Virtual Private Network
VSC	Virtual Smart Card
WAP	Web Application Proxy
WMI	Windows Management Instrumentation
WS-Federation	Web Services Federation

1617

Appendix C—Bibliography

This appendix lists all the sources of information used to develop this report.

About Virtual Network Secure Cross-Premises Connectivity. https://msdn.microsoft.com/en-us/library/azure/dn133798.aspx

Atmel Trusted Platform Module AT97SC3204/AT97SC3205 Security Policy. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2014.pdf

Azure Active Directory (GitHub). https://github.com/AzureAD

Azure Active Directory Authentication Libraries. https://msdn.microsoft.com/en-us/library/azure/dn151135.aspx

"Authentication Mechanism Assurance for AD DS in Windows Server 2008 R2 Step-by-Step Guide." https://technet.microsoft.com/en-us/library/dd378897(v=ws.10).aspx

"Azure Active Directory federation compatibility list: third-party identity providers that can be used to implement single sign-on." https://technet.microsoft.com/en-us/library/jj679342.aspx

Azure Active Directory Sync Services. http://www.microsoft.com/en-us/download/details.aspx?id=44225

Computer Security Objects Register (CSOR) Public Key Infrastructure (PKI) Objects Registration. http://csrc.nist.gov/groups/ST/crypto_apps_infra/csor/pki_registration.html

Derived Personal Identity Verification (PIV) Credentials Building Block. https://nccoe.nist.gov/sites/default/files/Derived_PIV_Credentials-Building_Block_final.pdf

"DirSync: List of attributes that are synced by the Azure Active Directory Sync Tool." http://social.technet.microsoft.com/wiki/contents/articles/19901.dirsync-list-of-attributes-that-are-synced-by-the-azure-active-directory-sync-tool.aspx

Enable Modern Authentication for Office 2013 on Windows devices. https://support.office.com/en-us/article/Enable-Modern-Authentication-for-Office-2013-on-Windows-devices-7dc1c01a-090f-4971-9677-f1b192d6c910?ui=en-US&rs=en-US&ad=US

FIPS 140 Validation. https://technet.microsoft.com/en-us/library/security/cc750357.aspx

FIPS 140-2, *Security Requirements for Cryptographic Modules*, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS 140-2 Security Policy for Nuvoton Cryptographic Module. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2023.pdf

FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. http://dx.doi.org/10.6028/NIST.FIPS.201-2

Framework for Improving Critical Infrastructure Cybersecurity.
http://www.nist.gov/cyberframework/index.cfm

GlobalPlatform Card Secure Element Configuration v1.0.
https://www.globalplatform.org/specificationscard.asp

"How to Configure S/MIME in Office 365."
http://blogs.technet.com/b/exchange/archive/2014/12/15/how-to-configure-s-mime-in-office-365.aspx

HSPD-12, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*. http://www.dhs.gov/homeland-security-presidential-directive-12

HSPD-12 Logical Access Authentication and Active Directory Domains.
http://www.microsoft.com/en-us/download/details.aspx?id=9427

IETF RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2."
tools.ietf.org/html/rfc5246

"Making Windows 10 More Personal and More Secure with Windows Hello."
http://blogs.windows.com/bloggingwindows/2015/03/17/making-windows-10-more-personal-and-more-secure-with-windows-hello/

Microsoft Azure Cloud Services Documentation. http://azure.microsoft.com/en-us/documentation/services/cloud-services/

Microsoft Azure Government Infrastructure as a Service. http://azure.microsoft.com/en-us/features/gov/

Microsoft Azure IaaS VNet. https://msdn.microsoft.com/en-us/library/azure/jj156007.aspx

Microsoft Office 365 Enterprise E3 Services. http://products.office.com/en-us/business/office-365-enterprise-e3-business-software

NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*.
http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

NIST IR 7817, *A Credential Reliability and Revocation Model for Federated Identities*.
http://dx.doi.org/10.6028/NIST.IR.7817

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST SP 800-63-2, *Electronic Authentication Guideline*. http://dx.doi.org/10.6028/NIST.SP.800-63-2

NIST SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification.* http://dx.doi.org/10.6028/NIST.SP.800-78-4

NIST SP 800-96, *PIV Card to Reader Interoperability Guidelines.* http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf

NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials.* http://dx.doi.org/10.6028/NIST.SP.800-157

"Office 2013 modern authentication public preview announced." https://blogs.office.com/2015/03/23/office-2013-modern-authentication-public-preview-announced/

OMB M-04-04, *E-Authentication Guidance for Federal Agencies*. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

OpenSSL FIPS Object Module. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf

Reset the TPM Lockout. https://technet.microsoft.com/en-us/library/dd851452.aspx

TPM Key Attestation. https://technet.microsoft.com/en-us/library/dn581921.aspx

Trusted Platform Module. http://www.trustedcomputinggroup.org/developers/trusted_platform_module

"Under the hood tour on Multi-Factor Authentication in ADS – Part 1: Policy." http://blogs.msdn.com/b/ramical/archive/2014/01/30/under-the-hood-tour-on-multi-factor-authentication-in-ad-fs-part-1-policy.aspx

Understanding and Evaluating Virtual Smart Cards. https://www.microsoft.com/en-us/download/details.aspx?id=29076

Universal Serial Bus Device Class: Smart Card ICCD Specification for USB Integrated Circuit(s) Card Devices. http://www.usb.org/developers/docs/devclass_docs/DWG_Smart-Card_USB-ICC_ICCD_rev10.pdf

"Walkthrough Guide: Connect to Applications and Services from Anywhere with Web Application Proxy." https://technet.microsoft.com/en-us/library/dn280943.aspx

Web Services Federation Passive Requester Profile. http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf

Windows Identity Foundation SDK. https://www.microsoft.com/en-us/download/details.aspx?id=4451

X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program.
http://idmanagement.gov/sites/default/files/documents/CertCRLprofileForCP.pdf

X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.
http://www.idmanagement.gov/sites/default/files/documents/commonpolicy.pdf