BUILDING BLOCK WHITE PAPER

DERIVED PERSONAL IDENTITY VERIFICATION (PIV) CREDENTIALS

Murugiah Souppaya
Mike Bartock
Jeff Cichonski

Information Technology Laboratory
National Institute of Standards and Technology

DRAFT
June 18, 2015
piv-nccoe@nist.gov

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

NCCoE building blocks address technology gaps that affect multiple industry sectors.

ABSTRACT

Federal Information Processing (FIPS) Standards Publication 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," establishes a standard for a PIV system based on secure and reliable forms of identity credentials issued by the federal government to its employees and contractors. These credentials are intended to authenticate individuals who require access to federally controlled facilities, information systems, and applications. In 2005, when FIPS 201 was first published, logical access was geared toward traditional computing devices (i.e., desktop and laptop computers) where the PIV card provides common authentication mechanisms through integrated smart card readers across the federal government. With the emergence of computing devices such as tablets, convertible computers, and in particular mobile devices, the use of PIV cards has proved challenging. Mobile devices lack the integrated smart card readers found in laptop and desktop computers and require separate card readers attached to devices to provide authentication services. In addition, some of the modern use case scenarios require the devices to be "on" all the time and for the user to quickly authenticate to the system using a personal identification number. Derived PIV credentials represent one possible way to PIV-enable a mobile device. The document specifies the use of tokens on mobile devices in which derived PIV credentials 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 information technology resources. The National Institute of Standards and Technology (NIST) has developed a proof-of-concept prototype platform for use of derived identity credentials in a mobile environment. Although the PIV program and the proof-of-concept focus on federal credentials, personal identity verification and identity-based security in mobile environments are important in both public and private sectors. The NCCoE is initiating a building block effort to develop and demonstrate extensions from the current platform to a platform that supports both government and private sector applications. The goal of the building block effort is a feasible security platform based on Federal PIV standards that can support operations in federal (PIV), non-federal critical infrastructure (PIV-Interoperable or PIV-I), and general business (PIV-Compatible or CIV) environments. This project will result in a freely available NIST Cybersecurity Practice Guide.

KEYWORDS

authentication; credentials; derived PIV credentials; electronic authentication; electronic credentials; devices; personal identity verification; PIV

DISCLAIMER

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

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

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

Public comment period: June 18, 2015 to August 14, 2015

Table of Contents

Abstract ii
Keywords iii
Disclaimer iii
Comments on NCCoE Documents iii
1. Description 2
Goal 2
Background 3
2. Scenarios 3
Usage Scenario 1 3
Usage Scenario 2 4
3. Security Characteristics 5
4. Implementation Challenges 14
5. Relevant Standards and References 14
6. High-Level Architecture 15
Components 16
Appendix A - Acronyms and Abbreviations 17

1. Description

Goal

Organizations protect their information systems, in part, by limiting access to the minimum set of users required to perform a function. This principle of "least privilege" requires both authentication and authorization processes. Federal Information Processing Standards Publication 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," recommends using smart cards with user data in conjunction with passwords 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 (i.e., 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 a smart card on the various mobile devices due to their form factor. Attaching or tethering a separate external smart card reader to the mobile phones or tablets creates usability and portability challenges and makes the card an impractical authentication token.

This building block will demonstrate, using smart cards (initially PIV cards), how derived smart card credentials can be added to mobile devices so that they may be used for remote authentication to information technology (IT) systems in operational environments. The National Institute of Standards and Technology (NIST) Information Technology Laboratory's Computer Security Division has developed an initial derived credentials proof-of-concept platform. Personal identification in mobile device environments is important in Federal (PIV), critical infrastructure (PIV-Interoperable [PIV-I]), and general business (PIV-Compatible [PIV-C or CIV]) environments. The goal of the building block effort is a feasible security platform based on Federal PIV standards and a NCCoE-developed demonstration prototype that can support operations in PIV, PIV-I, and PIV-C or CIV environments. This building block will use commercially available technologies to build on the proof of concept to demonstrate a public key infrastructure (PKI) with credentials derived from a PIV card, adhering to the requirements in NIST Special Publication (SP) 800-157, "Guidelines for Derived Personal Identity Verification (PIV) Credentials." The derived PIV X.509-based credentials 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 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 SIM cards), or Universal Serial Bus (USB) token.

Background

Federal Information Processing Standards (FIPS) Publication 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors,"[1] establishes a standard for a PIV system based on secure and reliable forms of identity credentials issued by the federal government to its employees and contractors. These credentials are intended to authenticate individuals who require access to federally controlled facilities, information systems and applications. The standard addresses requirements for initial identity proofing, infrastructures to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV credentials. In 2005, when FIPS 201 was first published, logical access was geared toward traditional computing devices (i.e., desktop and laptop computers), where the PIV card provides common authentication mechanisms through integrated smart card readers across the federal government. With the emergence of a newer generation of computing devices such as tablets, convertible computers, and in particular with mobile devices, the use of PIV cards has proved challenging. Mobile devices lack the integrated smart card readers found in laptop and desktop computers and require separate card readers attached to devices to provide authentication services from the device. In addition, some of the modern use case scenarios require the devices to be "on" all the time and the user to quickly authenticate to the system using a personal identification number (PIN).

NIST SP 800-157 defines the use of a derived PIV credential as one possible way to PIV-enable a mobile device. It specifies the use of tokens on mobile devices in which derived PIV credentials 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[2] for common identification that is secure, reliable, and interoperable government-wide.

2. Scenarios

This section proposes some high-level usage scenarios that support various characteristics and requirements that will be described in detail in the next section.

Usage Scenario 1

An organization provisions PIV credentials using a local enterprise PIV Card Management System (CMS). The organization is deploying modern client devices such as smart phones, tablets, and ultra-lightweight general-purpose computing devices that do not have built-in or contactless PIV card readers. However, these devices provide an

[1] http://dx.doi.org/10.6028/NIST.FIPS.201-2

[2] 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

embedded hardware token or software token that supports derived PIV credentials. In addition, the enterprise CMS system and internal PKI are capable of supporting the issuance, maintenance, use, and termination of derived PIV X.509-based credentials. The derived PIV credentials are used to authenticate and access resources hosted on a secure website, email messages hosted in the cloud, and the like.

For example, NIST SP 800-157 describes in detail an informative[3] issuance process of derived PIV credentials at Level of Identity Assurance 3 as follows:

> An employee requires a mobile device for work. The mobile device is ordered and a request for the issuance of a Derived PIV Credential is submitted to the agency's approval authority.
>
> Once the employee has received the device and the request has been approved the employee starts the issuance process by visiting a Web site operated by a registration authority (RA) that is associated with the certification authority (CA) that will issue the Derived PIV Credential. The Web site requires TLS [Transport Layer Security] client authentication using the PIV Authentication certificate on the employee's PIV Card. Since the employee cannot use the PIV Card with the mobile device the employee performs this step from a desktop computer. By requiring the use of the PIV Authentication certificate when connecting to the Web site and by validating the certificate, the server not only authenticates the employee, but also verifies that the employee is still eligible to possess a PIV credential. If the employee successfully authenticates to the server then the RA issues the employee a one-time password (OTP).
>
> The employee then runs a provisioning application on the mobile device. The application asks the employee to enter the OTP that was previously provided and to create a password, which will subsequently be used to authenticate to the cryptographic module. The application generates a key pair within the device's cryptographic module and submits the OTP and newly generated public key to the RA as part of a certificate request. The RA authenticates the employee by verifying that the OTP in the certificate request matches the one that it previously issued, signs the certificate request, and forwards it to the CA, which issues the Derived PIV Credential (i.e., the Derived PIV Authentication certificate). The provisioning application loads the Derived PIV Authentication certificate on the mobile device.

Usage Scenario 2

An organization wants to leverage shared service provider-provisioned PIV credentials to generate derived PIV credentials to be used on various computing devices. A local

[3] This represents an illustrative example provided in SP 800-157; it does not reflect a specific issuance process requirement.

CMS system and PKI will support the issuance, maintenance, use, and termination of the derived PIV X.509-based credentials. The derived PIV credentials are used to authenticate and access resource hosted on a secure website, email messages hosted in the cloud, and the like.

3. Security Characteristics

This building block will demonstrate capabilities throughout the primary life-cycle activities for the derived PIV credential as described in NIST SP 800-157. To achieve interoperability with the PIV infrastructure and its applications, this building block will use PKI technology as the basis for the derived PIV credential. An X.509 public key certificate that the CMS has 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 (FPKIPA) will serve as the derived PIV authentication certificate. The proposed approach outlines general security characteristics for stages within the PIV management life cycle.

General Characteristics:

1. A derived PIV credential 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. Tokens are used with alternative form factors to the PIV card that may be inserted into mobile devices, such as microSD tokens, USB tokens, or universal integrated circuit cards, or that are embedded in the mobile or computing device.

3. The PKI-based derived PIV credentials specified in this document are issued at levels of assurance (LOAs) 3 and 4.

4. Derived PIV credentials 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.

5. Applicant's proof of possession of a valid PIV card is required to receive a derived PIV credential.

6. The derived PIV authentication certificate is an X.509 public key certificate issued in accordance with the requirements of SP 800-157 and the X.509 Certificate Policy for the FPKIPA.[4]

[4] http://www.idmanagement.gov/documents/common-policy-framework-certificate-policy

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

Initial Issuance Characteristics:

1. A derived PIV credential 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 per Section 6.2.3.1 of FIPS 201-2.

2. The revocation status of the applicant's PIV authentication certificate should be rechecked seven calendar days following issuance of the derived PIV credential.

3. A derived PIV credential may be issued at identity assurance LOA-3 or LOA-4.

4. An LOA-3 derived PIV credential may be issued remotely or in person, while an LOA-4 derived PIV credential is issued in person in accordance with SP 800-63.

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

6. If the issuance process involves two or more electronic transactions for an LOA-3 derived PIV credential, 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.

7. The applicant shall identify him- or herself using a biometric sample that can be verified against the applicant's PIV card when enrolling for an LOA-4 derived PIV credential.

8. If there are two or more transactions during the issuance process, the applicant shall identify him- or 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 a LOA-4 derived PIV credential.

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

10. Issuance of multiple derived PIV credentials to the same applicant on the basis of the same PIV card is not precluded.

Maintenance Characteristics:

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

3. The initial issuance process shall be followed for re-key of an expired or compromised derived PIV credential.

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

5. The derived PIV authentication certificate shall be revoked or the token containing the corresponding private key shall be either zeroized[5] or destroyed when one of these circumstances occurs:

    a. The token containing the private key corresponding to the derived PIV credential is lost, stolen, damaged, or compromised.

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

    c. 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).

    d. The department or agency that issued the credential determines that the subscriber no longer requires a derived PIV credential, 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 derived PIV credential.

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

[5] If the derived PIV authentication private key was created and stored on a hardware cryptographic token that does not permit export of the private key and the token was collected and either zeroized or destroyed, then revocation of the derived PIV authentication certificate is optional. In all other cases, revocation of the derived PIV authentication certificate is mandatory.

certificate, a new Derived PIV Authentication certificate with the new name will also need to be issued.

Linkage with PIV Card Characteristics:

1. A derived PIV credential issuer shall issue a derived PIV credential to an applicant only if it has access to information about the applicant's PIV card from the issuer of the PIV card.

2. The derived PIV credential 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 derived PIV credential (e.g., name) has changed, as these would require revocation or modification of the derived PIV credential.

3. The derived PIV credential issuer should check every 18 hours on the termination status. The periodic checking requirement can also be met if:

    a. A notification mechanism is in place between the PIV card issuer and derived PIV credential issuer or

    b. The PIV card record and the derived PIV credential record are stored in the same system and termination of the PIV card automatically triggers termination of the derived PIV credential.

4. The issuer of the derived PIV credential 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.

5. Additional methods must be employed for obtaining information about the PIV card from the PIV card issuer, such as:

    a. If the derived PIV credential is issued by the same agency or issuer that issued the subscriber's PIV card, then the derived PIV credential issuer may have direct access to the Identity Management System database implemented by the issuing agency that contains the relevant information about the subscriber.

    b. When the issuer of the derived PIV credential is different from the PIV card issuer, the following mechanisms may be applied:

        i. 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.

ii. The issuer of the derived PIV credential notifies the original PIV issuer when a derived PIV credential is created. The issuer of the PIV card maintains a list of corresponding derived PIV credential 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.

iii. If a Uniform Reliability and Revocation Service (URRS) is implemented in accordance with Section 3.7 of NIST IR 7817*, A Credential Reliability and Revocation Model for Federated Identities*, the issuer of a derived PIV credential may obtain termination status of the subscriber's PIV card through the URRS.

Technical Characteristics:

1. Certificate Policies

   a. 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 "X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework."[6]

   b. 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) Profile for the Shared Service Providers (SSP) Program."[7]

   c. The expiration date of the derived PIV authentication certificate is based on the issuer's certificate policy. 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 life-cycle management.

2. Cryptographic Specifications

[6] The relevant versions of these documents will come once FPKIPA approves the changes required to support derived PIV credentials.

[7] The profile for derived PIV authentication certificates does not appear in the January 2008 version of the profile. A proposal for the new worksheet has been submitted to FPKIPA, but it has not yet been approved.

a. 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 SP 800-78.

b. 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 Federal Information Processing Standard 140-2 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.

c. 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 [FIPS140] Level 1 or higher.

3. Cryptographic Token Types

a. Removable (Non-Embedded) Hardware Cryptographic Tokens

i. 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 that the derived PIV credential interface is aligned with the interface of the PIV card.

ii. The form factor supports a secure element, a tamper-resistant cryptographic component that provides security and confidentiality.

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

iv. As described in Appendix B of 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.

v. SD Card with Cryptographic Module

1. A derived PIV application may reside on an SD card implementation that includes an onboard secure element or security system.

2. The secure element used for the derived PIV application shall support an interface with the card commands specified in Appendix B of SP 800-157.

vi. Removable Universal Integrated Circuit Card with Cryptographic Module

1. The derived PIV application shall be installed in a security domain that is separate from other security domains, dedicated to the derived PIV credential, and under the explicit control of the issuing agency.

2. The APDUs as specified in Appendix B of SP 800-157 shall be used with this secure element containing the PIV derived application.

3. A UICC used to host a derived PIV credential shall implement the GlobalPlatform Card Secure Element Configuration v1.0.

vii. USB Token with Cryptographic Module

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

2. The APDUs for the derived PIV application as specified in Appendix B of 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.

3. USB tokens with cryptographic modules that support a derived PIV application shall also be compliant with the specifications in SP 800-96 for APDU support for contact card readers.

b. Embedded Cryptographic Tokens

i. A derived PIV credential 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 of a software cryptographic module that runs on the device.

ii. Software-based derived PIV credentials cannot be issued at LOA-4.

iii. 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.

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

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

4. Activation Data

a. Use of the derived PIV authentication private key, or access to the plain text or wrapped private key, shall be blocked prior to password-based subscriber authentication.

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

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

d. 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.

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

f. 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.

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

h. 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:

    i. The subscriber's PIV card shall be used to authenticate the subscriber (via PKI-AUTH mechanism per Section 6.2.3.1 of FIPS 201) prior to password reset. The issuer shall verify that the derived PIV credential is for the same subscriber who authenticated using the PIV card.

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

i. When password reset is performed remotely, it shall follow the processes below:

    i. The subscriber's PIV card shall be used to authenticate the subscriber (via PKI-AUTH authentication mechanism per Section 6.2.3.1 of FIPS 201) prior to password reset.

    ii. 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.

    iii. The issuer shall verify that the derived PIV credential is for the same subscriber who authenticated using the PIV card.

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

j. Removable hardware tokens shall support the password reset functionality per Appendix B of SP 800-157. 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.

4. Implementation Challenges

We foresee the following challenges for the implementation of derived PIV credentials:

- a combination of technological and procedural requirements for the assertion of e-authentication LOA[8] of the derived PIV credential,
- enrollment processes both remote and in-person and issuance of derived PIV credential to known device and cryptographic container,
- credential life-cycle management; for example, PIN unlock process for corresponding LOA, subscriber's PIV card event that triggers derived PIV credential updates,
- derived PIV credential zeroing and/or revocation based upon method of termination, credential container, and design consideration for the support public key infrastructure,
- disparate PIV CMS interfaces and information exchange requirements for the issuance, maintenance, and termination of derived PIV credentials from a CMS that is not authoritative for the enrollee's PIV enrollment record.

5. Relevant Standards and References

- *Backend Attribute Exchange (BAE) v2.0 Overview*, January 2012 http://idmanagement.gov/sites/default/files/documents/BAE_v2_Overview_Document_Final_v1.0.0.pdf
- Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors*, February 25, 2005 http://www.dhs.gov/homeland-security-presidential-directive-12
- [id] Management.Gov, *Common Policy Framework Certificate Policy*, May 7, 2015 http://www.idmanagement.gov/documents/common-policy-framework-certificate-policy
- Universal Serial Bus Alliance, DWG Smart-Card USB Integrated Circuit(s) Card Devices, *Universal Serial Bus Device Class: Smart Card ICCD, Specification for USB Integrated Circuit(s) Card Devices*, Revision 1.0, April 22, 2005. http://www.usb.org/developers/docs/devclass_docs/DWG_Smart-Card_USB-ICC_ICCD_rev10.pdf
- *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Version 1.21, December 2012[9]

[8] NIST Special Publication 800-63-2, "Electronic Authentication Guideline," http://dx.doi.org/10.6028/NIST.SP.800-63-2

[9] The relevant versions of these documents will come once FPKIPA approves the changes required to support derived PIV credentials.

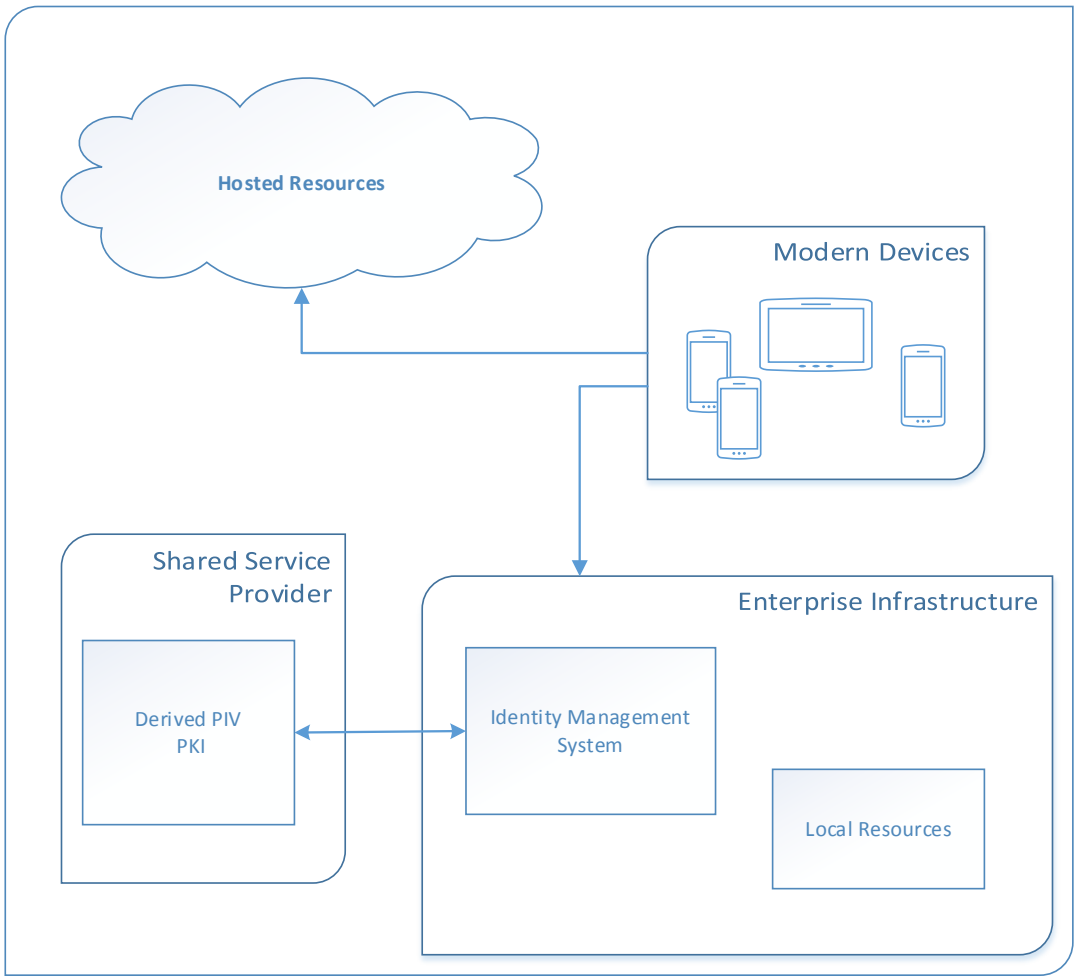
http://www.idmanagement.gov/documents/common-policy-framework-certificate-policy

- *X.509 Certificate and Certificate Revocation List (CRL) Profile for the Shared Service Providers (SSP) Program, Version 1.5,* January 2008[10] http://idmanagement.gov/sites/default/files/documents/CertCRLprofileForCP.pdf
- Federal Information Processing Standards (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, NIST, August 2013 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf.
- NIST Special Publication 800-63-2, *Electronic Authentication Guideline*, NIST, August 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf
- NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification (3 Parts)*, May 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf
- NIST Special Publication 800-76-2, *Biometric Specifications for Personal Identity Verification*, July 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf
- NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, May 2014, or as http://csrc.nist.gov http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf
- NIST Special Publication 800-79 2, *DRAFT Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, June 2, 2014 http://csrc.nist.gov/publications/drafts/800-79-2/sp800_79-2_draft.pdf
- NIST Special Publication 800-96, *PIV Card to Reader Interoperability Guidelines*, September, 2006 http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf
- NIST Special Publication 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials, December 2014 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf
- NIST Interagency Report 7817, *A Credential Reliability and Revocation Model for Federated Identities*, November 2012 http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7817.pdf

6. HIGH-LEVEL ARCHITECTURE

The figure below depicts the proposed environment and architecture for the derived PIV credentials proof of concept:

[10] The relevant versions of these documents will come once FPKIPA approves the changes required to support derived PIV credentials.



475

476 **Figure 1. Proposed Derived PIV Credentials Environment**

477 ## Components

478 Components needed to implement the proposed Derived PIV Credentials building block
479 include, but are not limited to the following:

480 • Client systems
481 • Server systems
482 • Cloud computing services
483 • DNS/DNSSEC services
484 • Removable MicroSD tokens
485 • Removable USB security tokens
486 • Removable UICC tokens
487 • Embedded Mobile Device Software tokens

- Embedded Hardware
- Virtual private network service
- Domain name services
- Windows domain controllers
- Active Directory Federation Servers
- Identity management system
- Cards management system
- Certificate authorities for PIV and Derived PIV Credentials
- Application Proxy Servers
- PIV/PIV-I/ CIV Card Management Systems
- PIV/PIV-I/ CIV smart card writers and printer
- PIV/PIV-I/ CIV compliant smart card readers
- PIV/PIV-I/ CIV compliant Smart cards
- Mobile devices
- Operating Systems
- Laptop computer

APPENDIX A - ACRONYMS AND ABBREVIATIONS

APDU	Application Protocol Data Unit
BAE	Backend Attribute Exchange
CA	Certification Authority
CIV	Personal Identity Verification-Compatible
CMS	Card Management System
FIPS	Federal Information Processing Standards
FPKIPA	Federal PKI Common Policy Framework
ICC	Integrated Circuit Card
ICCD	Integrated Circuit(s) Card Device

IT	Information Technology
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
OTP	One-Time Password
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-C	Personal Identity Verification-Compatible
PIV-I	Personal Identity Verification-Interoperable
PKI	Public Key Infrastructure
RA	Registration Authority
SD	Secure Digital
SP	Special Publication
TLS	Transport Layer Security
UICC	universal integrated circuit card
URRS	Uniform Reliability and Revocation Service
USB	Universal Serial Bus

505