NIST SPECIAL PUBLICATION 1800-12A

# Derived Personal Identity Verification (PIV) Credentials

**Volume A:**
**Executive Summary**

**William Newhouse**
National Cybersecurity Center of Excellence
Information Technology Laboratory

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

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

September 2017

DRAFT

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


# Executive Summary

- In response to the 9/11 attacks, the Department of Homeland Security directed the development of a mandatory, government-wide standard for forms of personal identification. These standards were to offer a secure and reliable way to authenticate and verify the identity of government employees and contractors to access federal facilities and information systems (Homeland Security Presidential Directive-12 (HSPD-12)).
- To satisfy the requirements of this mandate, the National Institute of Standards and Technology (NIST) developed a common identification standard, Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors. This standard created requirements for PIV systems that are interoperable and specified an agreed-upon set of credentials contained in a PIV Card – also known as a "smart card." These cards contain identifying information about the cardholder that grants them access.
- To extend the value of PIV systems into mobile devices that do not have PIV Card readers, NIST developed technical guidelines on the implementation of identity credentials that are standards-based, secure, reliable, interoperable based on public key infrastructure (PKI) and are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV card. These NIST guidelines, published in 2014, describe Derived PIV Credentials (DPCs) which leverage identity proofing and vetting results of current and valid PIV credentials.
- To demonstrate the DPCs guidelines, the National Cybersecurity Center of Excellence (NCCoE) at NIST built in its laboratory a security architecture using commercial technology to manage the lifecycle of DPCs demonstrating the process that enables a PIV Card holder to establish DPCs in a mobile device which then can be used to allow the PIV Card holder to access websites that require PIV authentication.
- This practice guide demonstrates the laboratory security architecture which shows how an organization can continue to provide two-factor authentication for users with a mobile device that leverages the strengths of the PIV standard.
- Although the PIV program and the NCCoE Derived PIV Credentials project are primarily aimed at the federal sector's needs, both are relevant to mobile device users in the commercial sector using smart card-based credentials or other means of authenticating identity.

## CHALLENGE

The Federal Government utilizes PIV cards to securely authenticate and identify employees and contractors when granting access to federal facilities and information systems. PIV cards require the use of a smart card reader that is typically integrated in desktop and laptop computers. Increasingly, users are performing their work on mobile devices, such as cell phones and tablets, which lack smart card readers needed to authenticate users. External readers are available, but they are an additional cost and cumbersome to use. As a result, the mandate to use PIV systems has pushed for new means to extend into mobile devices to enforce the same security policies as on desktop and laptop computers.

Previously, NIST published guidance on DPC including documenting a proof of concept research paper. The challenge is how to expand upon this work to demonstrate the use of Derived PIV Credentials on mobile devices in a manner that meets security policies.

## SOLUTION

The NCCoE developed a Derived Personal Identify Verification (PIV) Credentials solution that demonstrates how PIV credentials can be added to mobile devices to enable two factor authentication to information technology systems while meeting policy guidelines. Although the PIV program and the NCCoE Derived PIV Credentials project are primarily aimed at the federal sector's needs, both are relevant to mobile device users in the commercial sector using smart card-based credentials or other means of authenticating identity.

The NCCoE identified an architecture that use common mobile device families to demonstrate the use of Derived PIV Credentials in a manner that meets security policies. With experts from the federal sector and technology collaborators that provided the requisite equipment and services, we developed a representative use-case scenario to describe user access security challenges based on normal day-to-day business operations. This use case includes issuance, maintenance, and termination of the credential.

To that end, the example solution in the reference build is based on standards and best practices and derives from a simple scenario that informs the basis of an architecture tailored to either the public or private sector, or both.

The NCCoE reference design includes the following capabilities:

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

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

## BENEFITS

The NCCoE's practice guide to Derived PIV Credentials can help your organization:

- meet authentication standards requirements for protected websites and information across all devices, both traditional and mobile
- provide users access to the information they need using the devices they want
- extend authentication measures to mobile devices without having to purchase cumbersome external smart card readers
- manage expenses by reducing integration efforts associated with implementing the Derived PIV Credentials through the use of an Enterprise Mobility Management system

## SHARE YOUR FEEDBACK

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

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

## TECHNOLOGY PARTNERS/COLLABORATORS

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


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

---

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology.

**LEARN MORE**

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