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

- Authentication is the process of verifying the identity of a user, often as a prerequisite to allowing access to a system's resources.
- Physical and logical access to federal information systems relies on the authentication of the user through the use of a Personal Identity Verification (PIV) card. These "smart cards" contain identifying information about the cardholder to authenticate them to federal facilities, information systems, and applications.
- To create interoperable PIV Systems and eliminate wide variations in the quality and security of authentication mechanisms, the National Institute of Standards and Technology (NIST) developed a common identification standard known as Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, which specifies an agreed-upon set of credentials contained in a smart card form factor (PIV Card).
- Extending the value of PIV systems to mobile devices is described in NIST technical guidelines on the implementation of identity credentials which can be implemented and deployed directly with mobile devices (such as smart phones and tablets) where those credentials are issued by federal departments and agencies to individuals who possess, and prove control over, a valid PIV Card. The guidelines describe Derived PIV Credentials, which leverage identity proofing and vetting results of current and valid PIV credentials.
- The National Cybersecurity Center of Excellence (NCCoE) at NIST built a laboratory environment to explore the development of a security architecture that uses commercial technology to manage the life cycle of derived PIV credentials.
- This NIST Cybersecurity Practice Guide demonstrates how organizations can provide two-factor authentication for users to access websites and exchange secured emails, from mobile devices that lack PIV-card readers, by leveraging a user's previously established PIV-card credentials to create a derived PIV credential.

CHALLENGE

PIV systems were first mandated as a response to Homeland Security Presidential Directive (HSPD-12) to enhance national security by providing common authentication mechanisms to provide logical access to federal systems on desktop and laptop computers with PIV card readers. With the federal government's increased reliance on mobile computing devices that lack PIV card readers, the mandate to use PIV systems has pushed for new means to extend the value of PIV by deriving the credentials on a PIV card into mobile devices in a manner that enforces the same security policies for the life cycle of a PIV card.

NIST has published guidance on derived PIV credentials, including documenting a proof-of-concept research paper. Expanding upon this work, the NCCoE identified an architecture that utilizes common mobile device families available in the market today, to demonstrate the use of derived PIV credentials in a manner that meets security policies. The flexibility of the technologies that underpin PIV, along with a growing understanding of the value of strong digital authentication practices, have developed an ecosystem of technology providers able to provide digital authentication solutions that may follow the policies outlined in NIST guidance for Derived PIV Credentials.

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

SOLUTION

The NCCoE has developed a Derived PIV Credentials solution that demonstrates how derived 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 who use smart card–based credentials or other means of authenticating identity.

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 sought existing technologies that provided the following capabilities:

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

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

BENEFITS

The NCCoE's practice guide titled 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 with access to the information that they need, using the devices that they want to use
- extend authentication measures to mobile devices without having to purchase expensive and cumbersome external smart card readers
- manage the Derived PIV Credentials centrally through an Enterprise Mobility Management system, reducing integration efforts and associated costs

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 as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

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

TECHNOLOGY PARTNERS/COLLABORATORS

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

Entrust Datacard MobileIron

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

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

LEARN MORE

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