NIST SPECIAL PUBLICATION 1800-12A

Derived Personal Identity Verification (PIV) Credentials

Volume A:
Executive Summary

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

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

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

August 2018

SECOND DRAFT

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

Executive Summary

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

CHALLENGE

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

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

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

SOLUTION

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

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

The NCCoE sought existing technologies that provided the following capabilities:

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

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

BENEFITS

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

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

SHARE YOUR FEEDBACK

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

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

TECHNOLOGY PARTNERS/COLLABORATORS

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

intel Entrust Datacard intercede MobileIron verizon✓

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