BUILDING BLOCK

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DERIVED PIV CREDENTIALS

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of derived Personal Identity Verification (PIV) credentials through collaboration with members of the information technology (IT) community, including vendors of cybersecurity solutions. This sheet provides an overview of the challenge, solution, and benefits of NIST Cybersecurity Practice Guide SP 1800-12, *Derived Personal Identity Verification (PIV) Credentials*. The example solution proposed by this effort is not the only one available in the fast-moving cybersecurity technology market. Please email us at piv-nccoe@nist.gov with suggestions and comments.

BACKGROUND

The deployment of PIV Cards and their supporting infrastructure was initiated in 2004 by Homeland Security Presidential Directive-12 (HSPD-12) with a directive to eliminate the wide variations in the quality and security of authentication mechanisms used across Federal agencies. The mandate called for a common identification standard to promote interoperable authentication mechanisms at graduated levels of security based on the environment and the sensitivity of data. In response, the 2005 Federal Information Processing Standard (FIPS) 201 specified a common set of credentials in a smart card form factor, known as the Personal Identity Verification (PIV) Card, which is currently used government-wide, as intended, for both physical access to government facilities and logical access to Federal information systems.

CHALLENGE

At the time that FIPS 201 was first published, logical access was geared towards traditional computing devices (i.e., desktop and laptop computers) where the PIV Card provides common authentication mechanisms through integrated readers across the federal government. With the emergence of a newer generation of computing devices and with mobile devices in particular, the use of PIV Cards has proved challenging. Mobile devices lack 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.

SOLUTION

The NCCoE has developed cybersecurity guidance, NIST Special Publication 1800-12 *Derived PIV Credentials*, using standards-based commercially available technologies and best practices to help government agencies and other organizations extend the value of PIV systems into mobile devices that do not have PIV Card readers. This NIST cybersecurity publication provides detailed guidance on how to develop a security architecture using commercial and open source technology based on Federal PIV standards. The Derived PIV Credentials project builds on NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, and NISTIR 8055, *Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research* to demonstrate the use of Derived PIV Credentials on mobile devices in a manner that meets security policies. Although the PIV program and the The NCCoE Derived PIV Credentials project is primarily aimed at the Federal sector's needs, it will still be relevant to mobile device users with smart card based credentials in the private sector.

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

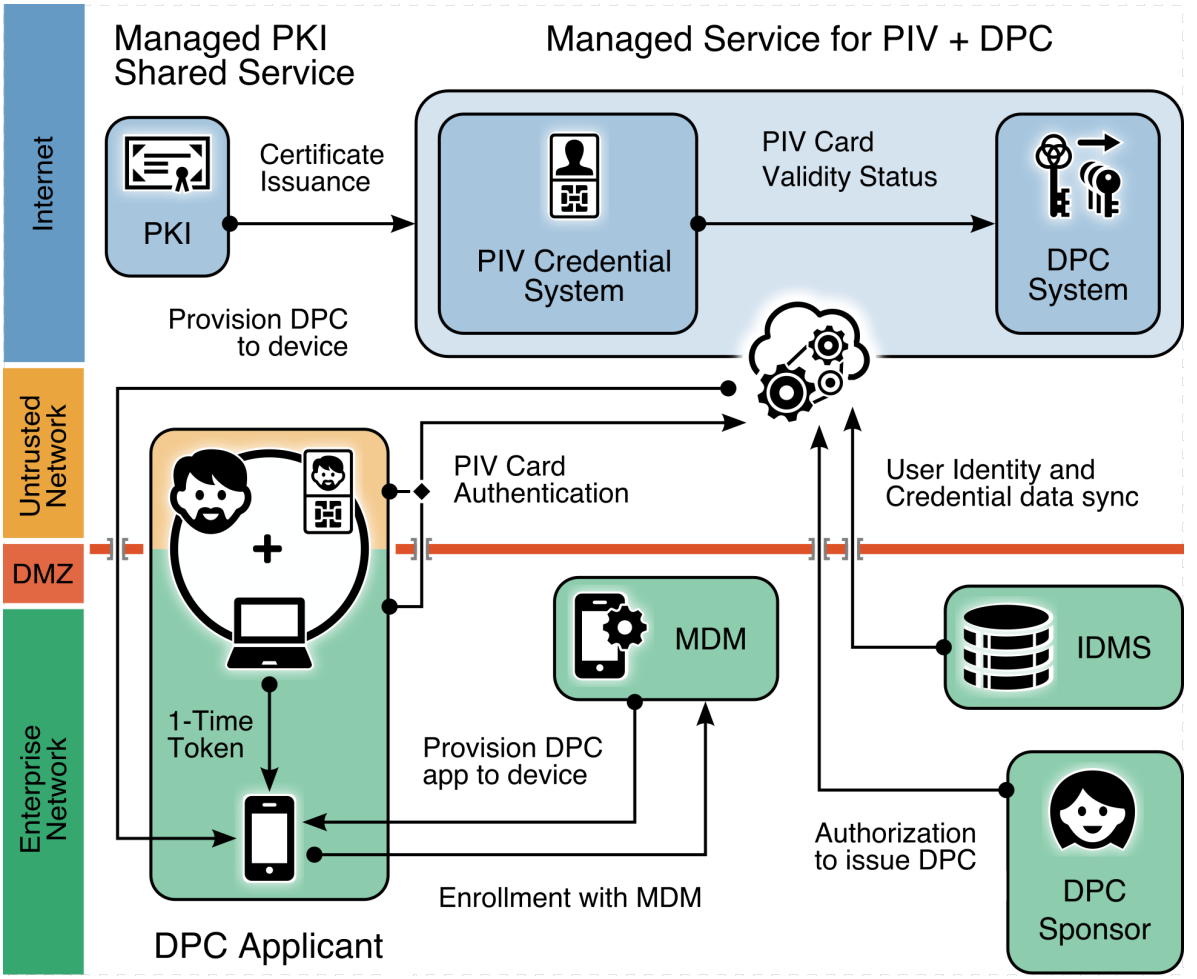
For users, this type of security platform allows strong authentication to access web sites and exchange secure email from mobile devices. For organizations, it offers cost savings by incorporating the user's previously established PIV identity into the new derived PIV credential, thereby eliminating the need for further identity proofing.

LEARN MORE ABOUT NCCOE
Visit http://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE

We developed a reference architecture to enable the issuance of a Derived PIV credential to a managed device. Below is an example scenario that includes using a cloud-based CMS (Credential Management System) solution to deliver a Derived PIV credential issuance app to the mobile device. For additional information about this scenario, please feel free to reach out to our development team 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.

DOWNLOAD THE PRACTICE GUIDE

For more information about this project, visit:
https://nccoe.nist.gov/projects/building_blocks/piv_credentials

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email at piv-nccoe@nist.gov.

September 2017