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 background, challenge, goals, and benefits of *Derived Personal Identity Verification (PIV) Credentials* project description. The example solution proposed by this effort will not be 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 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.

GOALS

The Derived PIV Credentials project will build 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 how derived PIV credentials can be added to mobile devices so that they can be used for remote authentication to information technology systems in operational environments while meeting policy guidelines. 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 goal of this building block effort is a security architecture built from commercial and open source technology based on Federal PIV standards. The example solution will be published in an NCCoE Cybersecurity Practice Guide, NIST SP 1800-series document that can support operations in:

- Federal (PIV) infrastructure
- Non-federal critical infrastructure (PIV-Interoperable or PIV-I)
- General business (PIV-Compatible or CIV) environments

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.

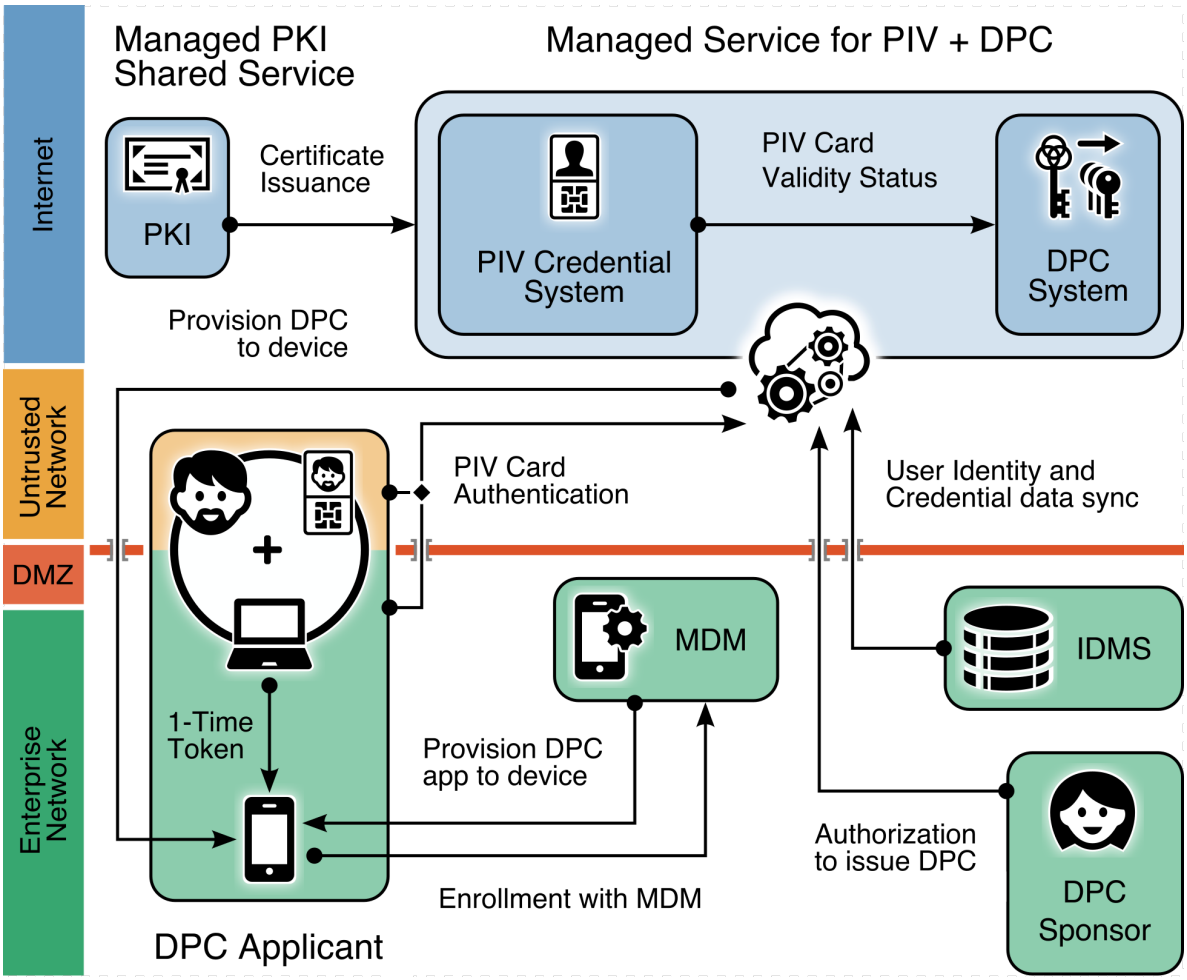
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges.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

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

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

HIGH-LEVEL ARCHITECTURE

We have developed several reference architectures to enable the issuance of a Derived PIV credential to a managed device. Below is one 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 and the others we have developed, please feel free to reach out to our development team at piv-nccoe@nist.gov.



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

Entrust Datacard™ | GO-Trust | intel | intercede | MobileIron | XTEC

Certain commercial entities, equipment, products, or materials may be identified 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, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PROJECT DESCRIPTION

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

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking collaborators, insights, and expertise from businesses, the public, and technology vendors. If you are interested in contributing or collaborating on this project, please contact us at piv-nccoe@nist.gov.

February 2017