New NCCoE building blocks for email security and PIV credentials

July 6 2015, by Leah Kauffman

Credit: AI-generated image (disclaimer)

NIST's National Cybersecurity Center of Excellence (NCCoE) has proposed two new building blocks, one to help organizations improve the security of email, the other to enable mobile devices to provide security services based on personal identity verification (PIV) credentials. PIV cards (as they are known in the federal government) and other so-called

smart card identity credentials contain computer chips that can receive, store, and transmit information securely. They are currently used in conjunction with a card reader to ensure authorized access to computer systems, certify emails, or provide an additional layer of security for physical access to facilities.

The NCCoE invites the public to comment on the draft documents. The comment period for each is open until August 14, 2015.

The NCCoE addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

Building blocks are example cybersecurity implementations that apply to multiple industry sectors and will be incorporated into many of the center's sector-specific use cases. The NCCoE's work to develop building blocks results in NIST Cybersecurity Practice Guides (Special Publication series 1800), publicly available descriptions of the practical steps needed to implement a cybersecurity reference design.

The draft building block "Domain Name System-Based Security for Electronic Mail" proposes using the Domain Name System (DNS) -Based Authentication of Named Entities (DANE) protocol to help prevent unauthorized parties from reading or modifying an organization's email, or using it as a vector for malware.

The draft secure email building block document can be viewed at nccoe.nist.gov/dnssecuredemail . Comments should be submitted to dns-email-nccoe@nist.gov by August 14, 2015.

The draft building block "Derived Personal Identity Verification (PIV)

Credentials" proposes a way to enable mobile devices, which lack card readers, to make use of two-factor authentication (information derived from a PIV card or other smart card, plus a password), a more secure method than relying on a password alone. Mobile device users, then, can benefit from the same level of security that users of desktop computers and card readers have. While PIV is a federal credential, the technology can be employed in the private sector as well.

More information: The draft derived PIV credentials building block document can be viewed at nccoe.nist.gov/derivedcredentials . Comments should be submitted to piv-nccoe@nist.gov by August 14, 2015.

Provided by National Institute of Standards and Technology