



This document is scheduled to be published in the Federal Register on 08/14/2015 and available online at <http://federalregister.gov/a/2015-20039>, and on FDsys.gov

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 150805680-5680-01]

National Cybersecurity Center of Excellence, Derived Personal Identity Verification
Credentials Building Block

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) invites organizations to provide products and technical expertise to support and demonstrate security platforms for the Derived Personal Identity Verification (PIV) Credentials Building Block. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address

cybersecurity challenges identified under the Derived PIV Credentials Building Block. Participation in the building block is open to all interested organizations.

DATES: Interested parties must contact NIST to request a letter of interest template to be completed and submitted to NIST that identifies the organization requesting participation in the NCCoE Derived PIV Credentials Building Block and the capabilities and components that are being offered to the collaborative effort. Letters of interest will be accepted on a first come, first served basis. Collaborative activities will commence as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities, but no earlier than September 14, 2015. When the building block has been completed, NIST will post a notice on the NCCoE Derived PIV Credentials Building Block website at <http://nccoe.nist.gov/derivedcredentials/> announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this Derived PIV Credentials building block.

ADDRESSES: The NCCoE is located at 9600 Gudelsky Drive, Rockville, MD 20850. Letters of interest may be submitted to piv-nccoe@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; Rockville, MD 20850. Organizations whose letters of interest are accepted in accordance with the process set forth in the SUPPLEMENTARY INFORMATION section of this notice will be asked to sign a Cooperative Research and Development Agreement (CRADA) with NIST. A CRADA template can be found at: <http://nccoe.nist.gov/node/138>.

FOR FURTHER INFORMATION CONTACT: Tim McBride via email to piv-nccoe@nist.gov; by telephone 240-314-6811; or by mail to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; Rockville, MD 20850. Additional details about the Derived PIV Credentials Building Block are available at <http://nccoe.nist.gov/derivedcredentials/>.

SUPPLEMENTARY INFORMATION:

Background

The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT assets, the NCCoE will enhance trust in U.S. IT communications, data, and storage systems; reduce risk for companies and individuals using IT systems; and encourage development of innovative, job-creating cybersecurity products and services.

Process

NIST is soliciting responses from all sources of relevant security capabilities (see below) to enter into a Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for the Derived PIV Credentials building block. The full Derived Personal Identity Verification

(PIV) Credentials building block can be viewed at:

<http://nccoe.nist.gov/derivedcredentials/>.

Interested parties must contact NIST to request a letter of interest template to be completed and submitted to NIST that identifies the organization requesting participation in the NCCoE Derived PIV Credentials Building Block and the capabilities and components that are being offered to the collaborative effort. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the Derived PIV Credentials building block objective or requirements identified below and to obtain additional information. NIST will select participants who have submitted responsive letters of interest on a first come, first served basis within each category of product components or capabilities listed below up to the number of participants in each category necessary to carry out this Derived PIV Credentials building block. However, there may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into a consortium CRADA with NIST (for reference, see ADDRESSES section above). NIST published a notice in the Federal Register on October 19, 2012 (77 FR 64314) inviting U.S. companies to enter into National Cybersecurity Excellence Partnerships (NCEPs) in furtherance of the NCCoE. For this demonstration project, NCEP partners will not be given priority for participation.

Derived PIV Credentials Building Block Objective

Organizations protect their information systems, in part, by limiting access to the minimum set of users required to perform a function. This principle of “least privilege” requires both authentication and authorization processes. Federal Information Processing Standards Publication 201-2, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” recommends using smart cards with user data in conjunction with passwords to provide two-factor authentication to federal information systems. While many desktop and laptop computers have built-in card readers, enterprises today rely heavily on the productivity of mobile devices (i.e., smartphones and tablets) that do not easily accommodate card readers. Organizations reliant on smart-card-and-password two-factor authentication need to authenticate users of mobile devices in a way that is more tamper-resistant than a password and as easy to use as a smart card. However, it is challenging to use smart card on the various mobile devices due to their form factor. Attaching or tethering a separate external smart card reader to the mobile phones or tablets creates usability and portability challenges and makes the card an impractical authentication token.

This building block will demonstrate, using smart cards, initially PIV cards, how derived smart card credentials can be added to mobile devices so that they may be used for remote authentication to information technology systems in operational environments. An initial derived credentials proof of concept platform has been developed by NIST ITL’s Computer Security Division. Personal identification in mobile device environments is important in Federal (PIV), Federal Contractor (PIV-Interoperable or PIV-I), and general business (PIV-Compatible or CIV) environments. The goal of the building block effort is to demonstrate a feasible security platform based on Federal identity verification

standards and guidelines and the NIST-developed existing demonstration prototype proof of concept that can support operations in PIV, PIV-I, and CIV environments. This building block will use commercially available technologies to demonstrate a public key infrastructure (PKI) credentials derived from a PIV-compatible card that is consistent with the requirements in NIST Special Publication 800-157, “Guidelines for Derived Personal Identity Verification (PIV) Credentials.” The derived PIV X.509-based credentials will be used for logical access to remote resources hosted within an on-premises data center or in the public cloud. The corresponding derived private key will be stored in a cryptographic module with alternative form factor such as embedded hardware or software in a mobile device or a removable token such as a secure digital (SD) card, universal integrated circuit card (UICC, the new generation of SIM cards), or USB token. A detailed description of the Derived PIV Credentials Building Block is available at: <http://nccoe.nist.gov/derivedcredentials/>.

Requirements

Each responding organization’s letter of interest should identify which security platform component(s) or capability(ies) it is offering. Letters of interest should not include company proprietary information, and all components and capabilities must be commercially available. Components are listed in section 6 of the Derived Personal Identity Verification (PIV) Credentials Building Block description (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- Client systems
- Server systems

- Cloud computing services
- DNS/DNSSEC services
- Removable MicroSD tokens
- Removable USB security tokens
- Removable UICC tokens
- Embedded Mobile Device Software tokens
- Embedded Hardware
- Virtual private network service
- Domain name services
- Windows domain controllers
- Active Directory Federation Servers
- Identity management system
- Cards management system
- Certificate authorities for PIV and Derived PIV Credentials
- Application Proxy Servers
- PIV/PIV-I/ CIV Card Management Systems
- PIV/PIV-I/ CIV smart card writers and printer
- PIV/PIV-I/ CIV compliant smart card readers
- PIV/PIV-I/ CIV compliant Smart cards
- Mobile devices
- Operating Systems
- Laptop computer

Each responding organization's letter of interest should identify how their products address one or more of the desired solution characteristics in section 3 of the Derived Personal Identity Verification (PIV) Credentials Building Block description (for reference, please see the link in the PROCESS section above).

Additional details about the Derived PIV Credentials Building Block are available at: <http://nccoe.nist.gov/derivedcredentials/>.

NIST cannot guarantee that all of the products proposed by respondents will be used in the demonstration. Each prospective participant will be expected to work collaboratively with NIST staff and other project participants under the terms of the consortium CRADA in the development of the Derived PIV Credentials Building Block. Prospective participants' contribution to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities. Each participant will train NIST personnel, as necessary, to operate its product in capability demonstrations. Following successful demonstrations, NIST will publish a description of the security platform and its performance characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the Derived PIV Credentials Building Block. These descriptions will be public information.

Under the terms of the consortium CRADA, participants will commit to providing:

1. Access for all participants' project teams to component interfaces and the organization's experts necessary to make functional connections among security platform components
2. Support for development and demonstration of the Derived PIV Credentials Building Block in NCCoE facilities which will be conducted in a manner consistent with Federal requirements (e.g., FIPS 200, FIPS 201, SP 800-53, and SP 800-63)

In addition, NIST will support development of interfaces among participants' products by providing IT infrastructure, laboratory facilities, office facilities, collaboration facilities, and staff support to component composition, security platform documentation, and demonstration activities.

The dates of the demonstration of the Derived PIV Credentials Building Block capability will be announced on the NCCoE Web site at least two weeks in advance at <http://nccoe.nist.gov/>. The expected outcome of the demonstration is to improve Derived PIV Credentials within the enterprise. Participating organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE governance, business processes, and NCCoE operational structure, visit the NCCoE Web site <http://nccoe.nist.gov/>.

Richard Cavanagh,
Acting Associate Director for Laboratory Programs.

[FR Doc. 2015-20039 Filed: 8/13/2015 08:45 am; Publication Date: 8/14/2015]