



Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No.: [171108999-7999-01]

National Cybersecurity Center of Excellence (NCCoE) Transport Layer Security (TLS)  
Server Certificate Management 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 Transport Layer Security (TLS) Server Certificate Management 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 TLS Server Certificate Management 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. 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 [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. When the building block has been completed, NIST will post a notice on the NCCoE TLS Server Certificate Management Building Block website at:

<https://nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management> announcing the completion of the building block and informing the public that it will no longer accept letters of interest for this building block.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to [tls-cert-mgmt-nccoe@nist.gov](mailto:tls-cert-mgmt-nccoe@nist.gov) or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, 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 consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at: <http://nccoe.nist.gov/node/138>.

FOR FURTHER INFORMATION CONTACT: Tim Polk, William Haag, Jr. and Murugiah Souppaya via email to [tls-cert-mgmt-nccoe@nist.gov](mailto:tls-cert-mgmt-nccoe@nist.gov); by telephone 301-975-

0239; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the TLS Server Certificate Management Building Block are available at:

<https://nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management>

#### 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 TLS Server Certificate Management Building Block. The full building block can be viewed at:

<https://nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management>.

Interested parties should contact NIST using the information provided in the FOR FURTHER INFORMATION CONTACT section of this notice. NIST will then provide each interested party with a letter of interest template, which the party must complete, certify that it is accurate, and submit to NIST. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the building block objective or requirements identified below. NIST will select participants who have submitted complete 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 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 a National Cybersecurity Excellence Partnerships (NCEPs) in furtherance of the NCCoE. For this demonstration project, NCEP partners will not be given priority for participation.

**Building Block Objective:** The building block objective is to improve the overall security of TLS certificates and private keys. A detailed description of the TLS Server Certificate Management Building Block is available at:

<https://nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management>.

**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 3 of the TLS Server Certificate Management Building Block (for reference, please see the link in the PROCESS section above) and include, but are not limited to:

- TLS servers in the Cloud
- Public Certification Authority (CA)
- TLS Servers including webservers, application servers, or other services
- TLS Load Balancers
- DevOps Frameworks including application containers
- Internal CAs
- Certificate Management systems
- Certificate Network Scanning Tools including vulnerability scanning

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in Section 3 of the TLS Server Certificate Management Building Block (for reference, please see the link in the PROCESS section above):

1. External Systems – The architecture will include the following components that typically reside outside the organizational firewall:
  - TLS Servers in the Cloud Environment: The cloud environment will include multiple cloud instances acting as TLS servers. Certificates will be deployed and managed on these systems.

- Public CA: A publicly trusted CA will be used to issue one or more of the certificates used on TLS servers on the internal or external systems.
2. Internal Systems – The architecture will include several systems that are typically deployed within organizational network environments.
- TLS Servers: Multiple systems will be configured as TLS servers (e.g., webserver, application server, or other service). Certificates will be deployed and managed on these systems.
  - Load Balancer: A load balancer will act as a TLS server with a certificate and will facilitate the load balancing of traffic to the other TLS servers.
  - DevOps Framework(s): One or more DevOps frameworks (e.g., Docker) will be used to automate the management of cloud instances and the deployment of certificates on those instances.
  - Internal CA: An internal CA will be used to issue certificates to some of the TLS servers.
  - Certificate Manager: A certificate management system will be used to inventory and manage TLS server certificates deployed in the environment.
  - Certificate Network Scanning Tool: A tool, such as a vulnerability scanning or other tool, will be used to facilitate the discovery of TLS server certificates via network scanning.

3. Stakeholders/Roles – Humans play an important part in the management of TLS server certificates in enterprises; therefore, the following roles will be represented:

- Line of Business / Application Owner: People in leadership positions who are responsible for the line of business or application and who will drive the need for certificates to be deployed.
- System Administrators: Responsible for managing TLS servers and ensuring that the load balancer will be represented.
- DevOps Developer: Responsible for programming/configuring and managing the DevOps framework.
- Approver: One or more stakeholders who will review and approve/reject certificate management operations.
- PKI Team: One or more individuals who will manage the certificate management system and public/internal CAs.

Responding organizations need to understand and, in their letters of interest, commit to provide:

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 TLS Server Certificate Management Building Block in NCCoE facilities which will be conducted in a manner consistent with the following standards and guidance: OMB Circular A-

130; FIPS 200; FIPS 140-2; NIST Special Publications 800-52, 800-57, 800-63-3, 800-77, 800-177; NIST Framework for Improving Critical Infrastructure Cybersecurity; and Internet Engineering Task Force (IETF) Requests for Comments (RFCs) 2246, 4346, 5280 and 5246. The project will also be informed by two in-progress IETF standards draft-ietf-tls-tls13-21 The Transport Layer Security (TLS) Protocol Version 1.3 and draft-ietf-acme-acme-07 Automatic Certificate Management Environment (ACME).

Additional details about the TLS Server Certificate Management Building Block are available at:

<https://nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management>.

NIST cannot guarantee that all 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 TLS Server Certificate Management 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 TLS Server Certificate Management Building Block. These descriptions will be public information.

Under the terms of the consortium CRADA, 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 TLS Server Certificate Management 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 security of TLS certificates and private keys 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/>.

Kevin Kimball

NIST Chief of Staff

[FR Doc. 2017-27893 Filed: 12/26/2017 8:45 am; Publication Date: 12/27/2017]