TLS SERVER CERTIFICATE MANAGEMENT

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenges associated with Transport Layer Security (TLS) server certificate management by collaborating with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide Special Publication 1800-16, *Securing Web Transactions: Transport Layer Security (TLS) Server Certificate Management.* With this guide, we aim to encourage enterprises to establish and implement a formal TLS server certificate management program.

BACKGROUND

TLS is the most widely used protocol for securing web transactions and other communications on internal networks and the internet. TLS certificates are central to the operation and security of both internet-facing and private web services and play a key role in protecting clients by enabling them to confirm that they're talking to the right server. This can reduce the likelihood of users entering a password or other confidential information on an attacker's site that is posing as a legitimate server.

Some organizations have tens of thousands of TLS certificates and keys requiring ongoing maintenance and management. Organizations that improperly manage their TLS server certificates risk system outages and security breaches, which can result in revenue loss, harm to reputation, and exposure of confidential data to attackers. To address these security concerns, the NCCoE has undertaken this project to assist medium and large enterprises with managing their TLS server certificates.

CHALLENGE

Despite the mission-critical nature of TLS server certificates, many organizations don't have a formal TLS server certificate management program in place. This may be attributable to the complexity surrounding TLS server certificate management, starting with the broad distribution of certificates across enterprise environments and groups; the complex processes needed to manage them; and the multiple roles involved in their management and issuance. For example, TLS server certificates are typically issued by a central security team that has certificate expertise, but may lack access to the systems where the certificates are located. Conversely, system administrators lack an understanding about the risks and best practices associated with proper TLS server certificate management, but will typically install and oversee the certificates. This distributed management environment, compounded by the large and growing number of certificates, may pose significant risks to the enterprise, including:

- application outages caused by expired TLS server certificates
- security risks from encrypted threats or server impersonation
- disaster recovery risks in response to certificate authority (CA) compromise, algorithm deprecation, or cryptographic library bugs

BENEFITS

An effective TLS server certificate management program can produce the following benefits:

- reduced outages because certificates are managed and kept current
- improved security
- enhanced disaster recovery related to certificates
- increased efficiency as IT staff spend less time manually managing certificate inventory

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 demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
Visit https://www.nccoe.nist.gov

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

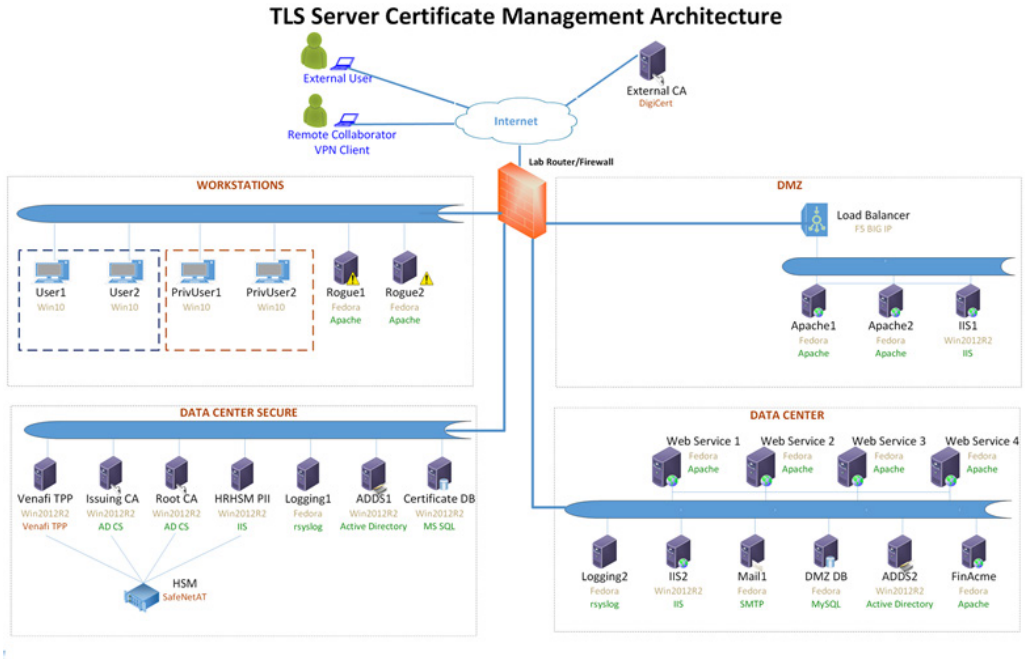
PROPOSED SOLUTION

The NCCoE, in collaboration with industry partners, is demonstrating a commercially supported, interoperable, secure, and tested example solution that efficiently and effectively provisions and manages TLS server certificates during normal operations and disaster recovery in a typical enterprise environment. The example solution supports the performance of the following actions:

- developing sets of policy attributes
- establishing and managing certificate inventories
- assigning and tracking certificate owners
- identifying TLS infrastructure issues and vulnerabilities
- automating enrollment and installation
- certificate status reporting
- continuous certificate monitoring

HIGH-LEVEL ARCHITECTURE

The diagram below illustrates the NCCoE laboratory architecture, which contains a certificate management system, hardware security module, and a variety of systems on which TLS server certificates are deployed (e.g., web servers, databases, application services, load balancers). These systems are distributed across multiple virtual local area networks to simulate the complexities of managing certificates across medium and large enterprises.



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors participating in this project submitted their capabilities in response to an open call in the *Federal Register*. Companies with relevant security capabilities 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:

Certain commercial entities, equipment, products, or materials may be identified to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or a recommendation or endorsement by NIST or NCCoE; neither it is intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE DRAFT PRACTICE GUIDE

For more information about this project, visit https://nccoe.nist.gov/tls-safe-web-transactions.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the TLS Server Certificate Management Community of Interest, please send an email to tls-cert-mgmt-nccoe@nist.gov.

September 2019