Venafi

COMPLIANCE BRIEF

Addressing TLS Certificate and Key Management for NIST 800-171 Compliance

The objective of NIST 800-171 is to protect Controlled Unclassified Information (CUI)—whether at rest or in transit—in nonfederal organizations. To effectively protect CUI, nonfederal organizations must ensure secure authentication, access control and confidentiality of communications.

Just as effective security requires management of human identities (usernames/passwords/certificates), it also requires effective management of machine identities—whether those machines are servers, applications, appliances, IoT devices or other systems. Transport Layer Security (TLS) certificates and their associated private keys are the primary machine identities used within organizations and on the internet to authenticate machines and ensure confidential communications. Consequently, the secure management of TLS certificates and private keys (machine identities) is essential to complying with NIST 800-171.

Several requirements of NIST 800-171 apply directly to the use of TLS, the management of TLS certificates/keys and the assurance of the authenticity of communications. Several other requirements do not explicitly call out authentication or key management but are affected by the secure use and management of TLS certificates and private keys. This document covers only the NIST 800-171 requirements that apply directly to TLS certificates and private keys.

The Role of TLS

The most broadly used security protocol on the internet and within corporate and government networks, TLS provides authentication and encrypted tunnels for HTTP, SMTP, IMAP and many other protocols. It relies on the use of certificates and private keys, with certificates providing a means for authenticating a system (or person) by associating an encryption key with an identifier for that system (e.g., a DNS address).

- Certificates are issued by a certificate authority (CA), which may be run internally or by a third party.
- The CA is responsible for confirming the identity of the system and the authority of the requester prior to issuing a certificate.
- Once a certificate is issued, any system that trusts the CA will trust that certificate.

Whenever TLS is used, the system acting as the TLS server must have a certificate. Optionally, a certificate may also be used by the system acting as a TLS client to authenticate itself (instead of using a password to authenticate, for example). Each of these certificates is accompanied by a unique private key. While certificates are public information—freely provided by a TLS server when a client connects—private keys must be kept secret and secured.

The broad use of TLS in nonfederal organizations and the severity of risks associated with TLS certificates require that nonfederal organizations demonstrate secure control and management of TLS certificates to be compliant with NIST 800-171.

Protecting TLS Certificates and Private Keys

Venafi is the cybersecurity market leader in machine identity protection, securing TLS certificates and keys on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi certificate and key security to protect communications, commerce, critical systems and data, and mobile and user access.

Venafi has achieved Common Criteria Certification and is already a trusted solution for several government agencies. Venafi customers include three of the top civilian agencies and the DoD.

NIST SP 800-171 Requirement	Venafi Platform Capabilities
3.13.8 – Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission, unless otherwise protected by alternative physical safeguards.	Organizations must demonstrate they are securely and effectively implementing TLS for the protection of CUI during transmission by showing they securely manage certificates and private keys. Venafi enables TLS to be implemented to protect CUI through the secure management of certificates and private keys and provides a full audit trail of all certificate and private key management operations.
3.13.10 – Establish and manage cryptographic keys for cryptography employed in the information system.	Organizations must be able to demonstrate the following: • An automated inventory of all certificates and private keys is established and maintained to ensure accuracy. • Ownership information for all certificates is maintained so that the correct individual/group can be contacted in case of an emergency. • All certificate and private key management operations are recorded on a central log to enable review. • Certificate enrollment operations are reviewed and approved by business/ application owners with knowledge of both applicable domain addresses and whether the individuals requesting the certificates are authorized to make the request. • Direct access to private keys used with certificates by system administrators is minimized. • Certificates are replaced when administrators who have had direct access to their private keys are reassigned or terminated. Venafi enables automated discovery, inventory, approvals and secure provisioning.

NIST SP 800-171 Requirement	Venafi Platform Capabilities
3.13.15 – Protect the authenticity of communications sessions.	To protect the authenticity of communications sessions, organizations must demonstrate that all TLS certificates and private keys are being securely managed by showing they perform automated scans (networks and files), maintain a complete inventory, have up-to-date ownership information, minimize administrator access to private keys and maintain an audit trail of all certificate and private key management operations. Venafi provides automated discovery, centralized inventory with metadata, automated hands-free management and comprehensive logging.
3.14.6 – Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	TLS traffic cannot be monitored and controlled unless the TLS inspection system (e.g., Symantec or Palo Alto Networks) has access to a server's private keys. Organizations must demonstrate that all TLS private keys are made available to TLS inspection systems and that those private keys are securely transferred and managed. Venafi makes it possible to automatically transfer server private keys to TLS inspection systems. This allows remote access systems to be monitored and controlled. This also ensures that private keys are securely managed through the process of installing inspection/ monitoring systems.

Security Risks for TLS Certificates and Keys

Because of the broad use of TLS, many organizations have thousands of TLS certificates deployed across their environment. If these certificates and corresponding private keys are not properly managed, organizations open themselves to security and operational risks:

- **Private Key Theft:** If not properly secured, private keys can be compromised and used by an attacker, a malicious insider or a former employee who previously had access. A compromised private key enables an attacker to masquerade as the system where that private key was originally held.
- **Issuance of Rogue Certificates:** If an organization does not use a secure process for requesting certificates, an attacker can circumvent the request process and get a rogue certificate containing a DNS address associated with the organization.
- **Service Disruptions and Outages:** Certificates contain an expiration date, after which they should not be accepted or used. If organizations do not track their deployed certificates and replace them before they expire, they can experience significant service outages and disruptions.

- **Bugs in Cryptographic Libraries:** The security and integrity of certificates and keys is highly dependent on the cryptographic libraries that are used to generate key pairs, validate certificates and perform cryptographic operations. Bugs in cryptographic libraries can require rapid changing of large numbers of keys and certificates. For example, the Heartbleed bug in OpenSSL made it possible for attackers to get a copy of a server's private key, and a bug in Debian resulted in the ability to guess 2048-bit keys more easily for 2 years (or longer if keys weren't replaced after the vulnerability was publicly reported). Both bugs required organizations to rapidly replace keys and certificates once the libraries were patched.
- **Large Scale Security Incidents:** If a CA is compromised or an algorithm used with certificates (e.g., SHA-1) is considered weak, organizations must change large numbers of certificates and keys. If organizations do not have sound management processes, they are not able to rapidly replace certificates when an unexpected event occurs.

When organizations abide by NIST 800-171 and protect CUI, they minimize the risk of these threats. Learn more about how Venafi can help your agency address TLS certificate and key management for NIST 800-171.

The Venafi Platform has achieved Common Criteria Certification, validated by the U.S. Federal Government approved Common Criteria Test Laboratories and the National Information Assurance Partnership (NIAP).

To learn more, visit **venafi.com**.

Trusted by

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. **To learn more, visit venafi.com**