Compliance Brief

NIST 800-171: Certificate and Key Security for External Service Providers

An Anlysis of NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations[1]

As part of a federal agency, you are responsible for ensuring that protection for Controlled Unclassified Information (CUI) extends to all contractors, subcontractors and service providers who may handle that information. The National Institute of Standards and Technology (NIST) issued Special Publication 800-171 which includes a range of recommended requirements designed to protect the confidentiality of CUI when it is processed, stored or transmitted by nonfederal organizations. Many of these requirements involve protection for cryptographic keys and digital certificates.

It is important that your partners comply with these key and certificate protection requirements, but in many organizations, these standards are not well understood. To help you and your partners with effective implementation, we've assembled a list of NIST 800-171 requirements that involve implementing controls for certificates and keys.

Applying NIST 800-171 Requirements to Securing Certificates and Keys

3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

- Separate the duties of the administration of digital certificate and key management systems from those that request and issue digital certificates and keys.
- Separate ownership of the digital certificates and keys from ownership of the system where the digital certificates and keys reside.
- Ensure that access to digital certificates and keys requires formal approval from at least one person.
- Implement a change control policy to regulate digital certificates and keys.

3.1.11	Terminate (automatically) a user session after a defined condition.

- Rotate digital certificates and keys at regularly defined intervals.
- Rotate digital certificates and associated keys when a person leaves or changes roles within the organization.
- Remove associated SSH keys if a person leaves the organization.

3.1.12	Monitor and control remote access sessions.

- Monitor and control SSH keys, which are used for remote access.

3.1.22	Control information posted or processed on publicly accessible information systems.

- Validate that TLS and SSH are used and associated assets are implemented, secured, and managed appropriately.

3.2.1	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards,and procedures related to the security of organizational information systems.

- Educate leadership teams, system administrators, and end users about security risks, established policies, practice standards, and training procedures related to the management and securty of encryption assets.
- Define and enforce security policies for both TLS and SSH.

3.3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

- Audit records that "enable the monitoring, analysis, investigation and reporting" of key and certificate misuse, requiring a system that provides specific audit reporting functionality on the complete feature set.
- Implement auditable tasks such as inventory baseline, inventory status, changes to the inventory (additions and removals), user activity regarding keys and digital certificates, policy adherence and violations, approvals and workflows.

3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

- Create an inventory that accurately identifies key and certificate owners. Note that the requestor of a digital certificate or key cannot be relied upon as the lifetime owner because ownership can shift when the original owner changes positions or leaves the organization.

3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.

- Use a certificate and key management system with audit functionality that provides sufficient detail for audit review, analysis, and reporting.
- Cover auditable functions such as inventory baseline, inventory status, changes to the inventory (additions and removals), user activity in regards to the keys and digital certificates, policy adherence and violation, approvals and workflows.

3.4.1	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

- Inventory the entire lifecycle of all keys and certificates. Include an established baseline of how certificates are deployed and used. Deploy a certificate and key management system that is able to find and flag development and test certificates that have erroneously been placed into production environments.

3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.

- Define and enforce TLS and SSH policies as part of the required "security configuration setting." Monitor these policies for non-compliance and issue alerts when any non-compliance conditions are found. Get additional value from a system that provides remediation automation and guidance.

3.4.3	Track, review, approve/disapprove, and audit changes to information systems.

- Track, review, approve/disapprove key and certificate requests and installation/configuration.

3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

- Implement a systems that allows access restrictions to be defined by individuals or groups with supporting reports and approval mechanisms.

3.5.1	Identify information system users, processes acting on behalf of users, or devices.

- Identify and manage the secure lifecycle of all SSH and TLS trust instruments as SSH and TLS are often used by service accounts which can act on behalf of users or devices

3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

- Use keys and certificates for identification and authorization.

3.5.5	Prevent reuse of identifiers for a defined period.

- Define and enforce policies that prevent the duplication or reuse of keys and digital certificates.

3.5.6	Disable identifiers after a defined period of inactivity.

- Delete/revoke TLS and SSH keys that are no longer in use.

3.11.2	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.

- Conduct regular scans for vulnerabilities across all TLS and SSH assets.

3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.

- Establish remediation plans for TLS and SSH keys in the case of any event that warrants rotation, replacement or deletion. These plans should include a mass remediation scenario in case a vulnerability and/or risk that impacts a significant number of certificates and keys is identified.

3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

- Use TLS and SSH for sensitive or confidential internal and external communications.

3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.

- Get visibility into all keys and certificates and protect them against misuse to avoid unauthorized and unintended information transfer. As recent breaches have shown, cyber attackers are using encrypted traffic to hide their activities, using keys and certificates to enable "unintended information transfer" that lets malware in and sensitive data out without detection.

3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.

- Know where all keys and certificates are deployed and being used in order to ensure they are being used for their intended purpose and are not allowing cybercriminals unauthorized access and the ability to pivot this access to broaden their attack.

3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

- Validate TLS and SSH mechanisms for all CUI systems and ensure that the TLS keys and certificates and SSH keys are protected to avoid man-in-the-middle (MitM) attacks and unauthorized access to CUI.

3.13.10	Establish and manage cryptographic keys for cryptography employed in the information system.

- Define and enforce TLS and SSH policies to "establish and manage" cryptographic keys. Implement complete, secure management of the full lifecycle for digital certificates and keys, including inventory, audit, workflow and approval.

3.14.6	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

- Establish a baseline inventory of trusted digital certificates and keys.
- Schedule discovery scans across the entire network that look for anomalous use of digital certificates and keys based on the established trusted baseline.
- Setup notifications and reports to all stakeholders that provide immediate visibility into anomalous use of digital certificates and keys.

NIST 800-171 highlights the extent to which the federal government relies on external service providers to help carry out a wide range of federal missions and business functions using state-of-the-practice information systems. Consistent protections must be extended to these organizations to safeguard CUI. If your external service providers are struggling to comply with requirements for certificates and keys, Venafi can help. Privacy-minded leaders of Fortune 200 rely on the Venafi solution to meet certificate and key security requirements such as NIST 800-171. We can do the same for your external service providers.

RESOURCE

National Institute of Standards and Technology. NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. June 2015 (includes updates as of January 14, 2016).

TRUSTED BY THE TOP

5 OF 5 Top U.S. Health Insurers
5 OF 5 Top U.S. Airlines
4 OF 5 Top U.S. Retailers
4 OF 5 Top U.S. Banks
4 OF 5 Top U.K. Banks
4 OF 5 Top S. African Banks
3 OF 5 Top AU Banks

ABOUT VENAFI

Venafi is the cyber security market leader in protecting cryptographic keys and digital certificates which every business and government depends on to deliver safe encryption, authentication and authorization. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit www.venafi.com