NIST SPECIAL PUBLICATION 1800-16B

Securing Web Transactions

TLS Server Certificate Management

Volume B:
Security Risks and Recommended Best Practices

William Haag
Murugiah Souppaya
NIST

Paul Turner
Venafi

William C. Barker
Dakota Consulting

Brett Pleasant
Susan Symington
The MITRE Corporation

July 2019

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-16B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-16B, 102 pages, (July 2019), CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to tls-cert-mgmt-nccoe@nist.gov.

Public comment period: July 17, 2019 through September 13, 2019.

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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 issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology (IT) security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Transport Layer Security (TLS) server certificates are critical to the security of both internet-facing and private web services. A large- or medium-scale enterprise may have thousands or even tens of thousands of such certificates, each identifying a specific server in its environment. Despite the critical importance of these certificates, many organizations lack a formal TLS certificate management program and do not have the ability to centrally monitor and manage their certificates. Instead, certificate management tends to be spread across each of the different groups responsible for the various servers and systems in an organization. Central security teams struggle to make sure that certificates are being properly managed by each of these disparate groups. Where there is no central certificate management

service, the organization is at risk because once certificates are deployed, it is necessary to maintain current inventories to support regular monitoring and certificate maintenance. Organizations that do not properly manage their certificates face significant risks to their core operations, including

- application outages caused by expired TLS server certificates
- hidden intrusion, exfiltration, disclosure of sensitive data, or other attacks resulting from encrypted threats or server impersonation
- disaster-recovery risk that requires rapid replacement of large numbers of certificates and private keys in response to either certificate authority compromise or discovery of vulnerabilities in cryptographic algorithms or libraries

Despite the mission-critical nature of TLS server certificates, many organizations have not defined the clear policies, processes, roles, and responsibilities needed for effective certificate management. Moreover, many organizations do not leverage available automation tools to support effective management of the ever growing numbers of certificates. The consequence is continuing susceptibility to security incidents.

This NIST Cybersecurity Practice Guide shows large and medium enterprises how to employ a formal TLS certificate management program to address certificate-based risks and challenges. It describes the TLS certificate management challenges faced by organizations; provides recommended best practices for large-scale TLS server certificate management; describes an automated proof-of-concept implementation that demonstrates how to prevent, detect, and recover from certificate-related incidents; and provides a mapping of the demonstrated capabilities to the recommended best practices and to NIST security guidelines and frameworks.

This NIST Cybersecurity Practice Guide consists of the following volumes:

- **Volume A:** Executive Summary
- **Volume B:** Security Risks and Recommended Best Practices **(you are here)**
- **Volume C:** Approach, Architecture, and Security Characteristics
- **Volume D:** How-To Guides – instructions for building the example solution

KEYWORDS

Authentication; certificate; cryptography; identity; key; key management; PKI; private key; public key; public key infrastructure; server; signature; TLS; Transport Layer Security

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Dean Coclin	DigiCert
Tim Hollebeek	DigiCert
Clint Wilson	DigiCert
Dung Lam	F5
Robert Smith	F5
Elaine Barker	NIST
Rob Clatterbuck	SafeNet Assured Technologies (SafeNet AT)
Jane Gilbert	SafeNet AT
Alexandros Kapasouris	Symantec
Mehwish Akram	The MITRE Corporation
Brian Johnson	The MITRE Corporation
Sarah Kinling	The MITRE Corporation
Bob Masucci	The MITRE Corporation
Susan Prince	The MITRE Corporation
Mary Raguso	The MITRE Corporation
Aaron Aubrecht	Venafi
Justin Hansen	Venafi

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly in order to conform to the publication and from which no deviation is permitted.

The terms “should” and “should not” indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.

The terms “may” and “need not” indicate a course of action permissible within the limits of the publication.

The terms “can” and “cannot” indicate a possibility and capability, whether material, physical or causal.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

i) under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

ii) without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee,

and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: tls-cert-mgmt-nccoe@nist.gov

Contents

List of Figures

List of Tables

1 Introduction

Organizations risk losing revenue, customers, and reputation, and exposing internal or customer data to attackers if they do not properly manage Transport Layer Security (TLS) server certificates. TLS is the most widely used security protocol to secure web transactions and other communications on the internet and internal networks. TLS server certificates are central to the security and operation of internet-facing and internal web services. Improper TLS server certificate management results in significant outages to web applications and services—such as government services, online banking, flight operations, and mission-critical services within an organization—and the risk of security breaches. Organizations should ensure that TLS server certificates are properly managed to avoid these issues.

The broad distribution of TLS server certificates across multiple groups and technologies within an enterprise requires that organizations establish formal management programs that include clear policies and responsibilities, a central Certificate Service, automation, and education. Successful implementation of a certificate management program relies on executive sponsorship, clear objectives, an action plan, and regular progress reviews.

1.1 Objective

The objective of this volume is to describe risks and challenges related to TLS server certificates and address those challenges by providing recommended best practices for large-scale TLS server certificate management. This document recommends that organizations establish a formal TLS certificate management program, and it enumerates elements that should be considered for inclusion in such a program. It is important to note that the best practices recommended in this guide are just that—recommendations.

1.2 Scope

The scope of this document is confined to recommendations regarding TLS server certificate management. TLS client certificate management is out of scope. This document is not intended to provide an extensive explanation of what TLS certificates and keys are or how they are used. Also, certificate management policies need to be considered within the context of an organization's overall enterprise security policies.

It is also beyond the scope of this document to discuss the broader aspects of organizational policies and procedures with which TLS server certificate management should be consistent. For example, general recommendations regarding security policy, vulnerability management, incident response, disaster recovery, security testing, etc. that are not specifically related to certificate management are out of scope. Discussion of general security protections for certificate management system components is also beyond the scope of this document. This document assumes the security of these components is

protected by recommended security best practices, e.g., patching, strong authentication, and access control that the organization has in place as part of its overall security policy.

An organization's business operations may be internally or externally supported. For those organizations that have third parties supporting key business operations, those third parties may use TLS certificates. If a function is outsourced, the organization should ensure that its requirements are met by the third party performing the function. The TLS certificate management recommendations provided in this document can be applied to these third parties as well as to the organization itself.

In accordance with their security policies, some organizations may choose to perform inspection of internal traffic that has been encrypted using TLS, by intercepting and decrypting TLS traffic at the network edge or by performing passive decryption at locations deeper within the network. The question of whether to perform such inspection is complex, and it involves important tradeoffs between traffic security and traffic visibility that organizations should weigh carefully. It is beyond the scope of this document to advocate for or against TLS traffic inspection. Some organizations have determined that the security risks posed by inspection of internal TLS traffic are not worth the potential benefits of having visibility into the encrypted traffic. Other organizations, however, have determined that it is in their best interests to perform TLS traffic inspection. For those organizations that have a policy of performing TLS traffic inspection, this document provides recommended best practices regarding how to securely manage the TLS private keys required for this purpose.

The security and integrity of TLS relies on secure implementation and configuration of TLS servers and effective TLS server certificate management. Guidance regarding the implementation and configuration of TLS servers is outside the scope of this document. The secure implementation and configuration of TLS servers is addressed in NIST *Special Publication 800-52*. Organizations should provide clear instruction to groups and individuals deploying TLS servers in their environments to read, understand, and follow the guidance provided in 800-52.

Lastly, the recommendations included in this document are generic. Each organization should determine for itself how to best apply these recommendations to its own enterprise. Volumes C and D of this Practice Guide describe a specific implementation used to demonstrate the application of these recommendations.

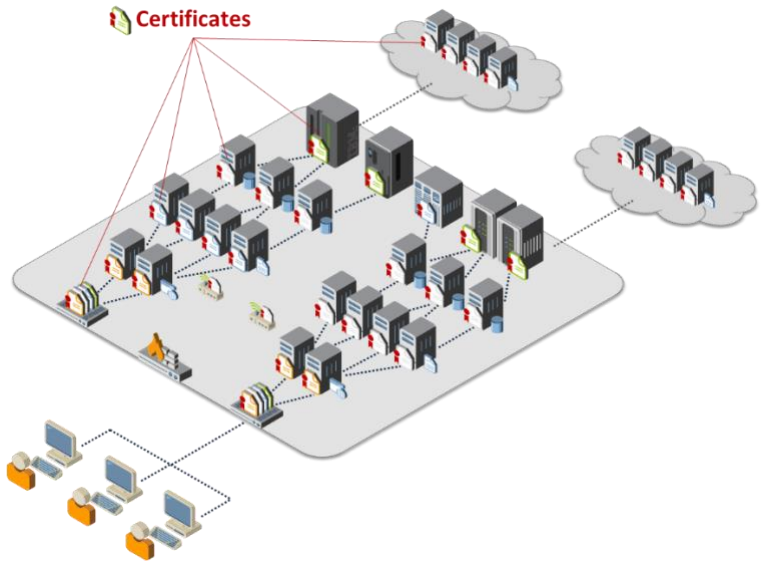
2 TLS Server Certificate Background

TLS is the security protocol used to authenticate and protect internet and internal network communications for a broad number of other protocols—including Hypertext Transfer Protocol (http) for web servers; Lightweight Directory Access Protocol (LDAP) for directory servers; and Simple Mail Transfer Protocol, Post Office Protocol, and Internet Message Access Protocol for email.

TLS server certificates serve as machine identities that enable clients to authenticate servers via cryptographic means. For example, when a bank customer connects across the internet to an online

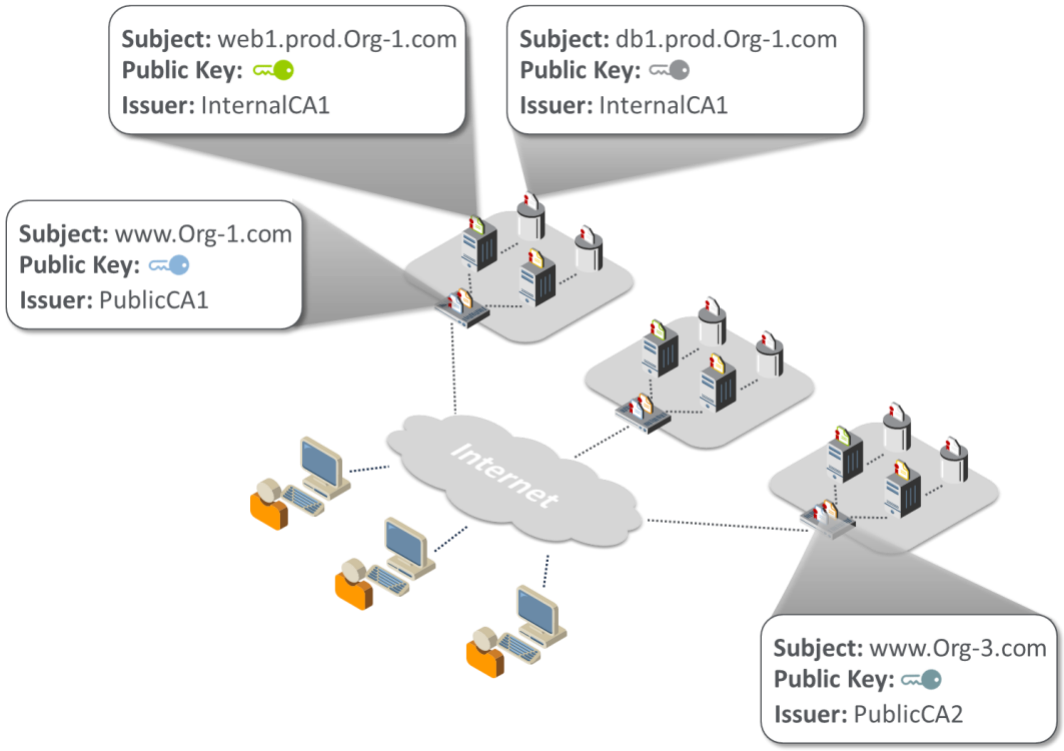
banking website, the customer's browser (i.e., the TLS client) will present an error message if the server does not provide a valid certificate that matches the address the user entered in the browser. Further, TLS server certificates are used extensively inside corporate and government networks to establish trust between machines — servers, applications, devices, micro-services, etc. Most enterprises have thousands of certificates, each identifying a specific server in their environment. (Note: Web browsers play the role of clients to web servers. As such, they contain functionality to automatically establish TLS connections on behalf of users, evaluate certificates received during the TLS handshake process, and present errors when unexpected certificate issues are encountered.) Figure 2-1 illustrates the pervasive use of certificates within organizations.

Figure 2-1 TLS Certificates Are Broadly Used for Communications in Organizations



Each TLS server certificate contains the address of the server that it identifies (e.g., *www.organization1.com*) and a cryptographic key, called a public key, which is unique to the server and used by clients to securely authenticate to the server (see Figure 2-2).

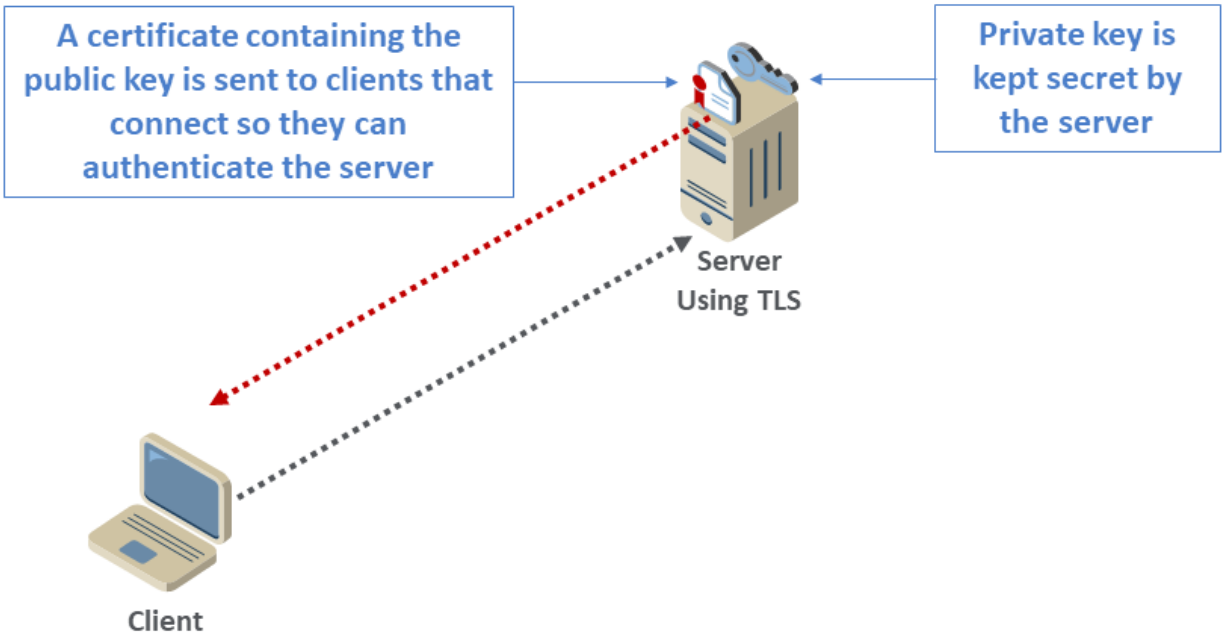
268 **Figure 2-2 Server Address, Public Key, and Issuer Information on Four of the Organization's TLS**
269 **Server Certificates**



270

271 As shown in Figure 2-3, each server holds a private key that corresponds to the public key in the
272 certificate so each server can prove it is the holder of the certificate. While the certificate is shared with
273 any client that connects to the server, the private key must be kept secure and secret so it cannot be
274 obtained by an attacker and used to impersonate the server. Many private keys used with TLS are stored
275 in plaintext files on TLS servers. Alternatively, private keys can be stored in files encrypted with a
276 password; however, the passwords are generally stored in plaintext configuration files so they are
277 accessible by the TLS server software when it is started. These common practices make it possible for
278 private keys to be viewed and copied by system administrators or malicious actors.

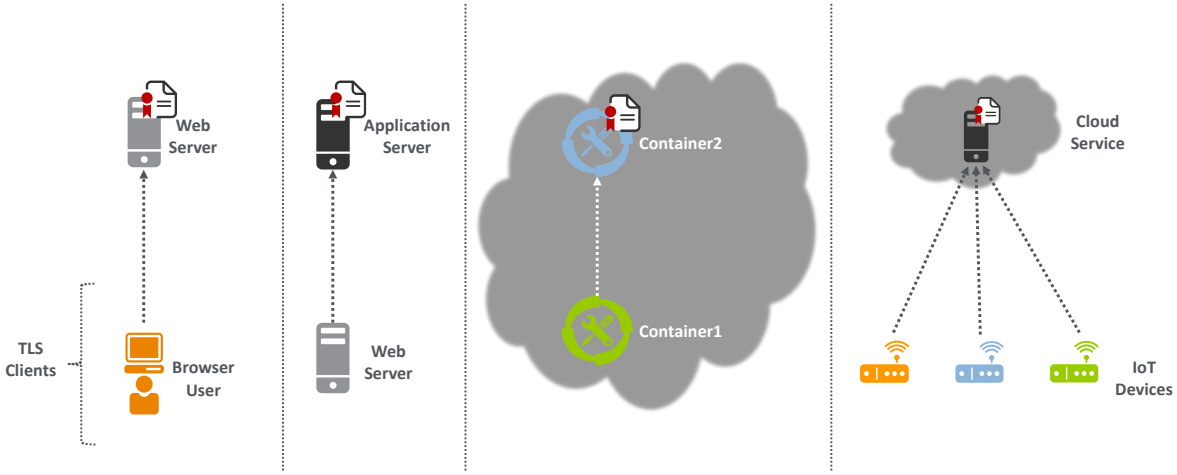
279 **Figure 2-3 Upon Connecting to the Server, the Client Receives the Server's TLS Certificate, Which**
280 **Includes the Server's Public Key**



281

282 In addition to users with browsers connecting to servers that have TLS server certificates, automated
283 processes also connect as clients to TLS servers and must trust TLS server certificates. Examples of
284 automated processes acting as TLS clients include a web server making requests to an application
285 server, one cloud container connecting to another, or an Internet of Things (IoT) device connecting to a
286 cloud service. (See Figure 2-4.)

287 **Figure 2-4 Browsers and Various Automated Processes (Web Servers, Containers, and IoT Devices)**
288 **Connect as Clients to TLS Servers**



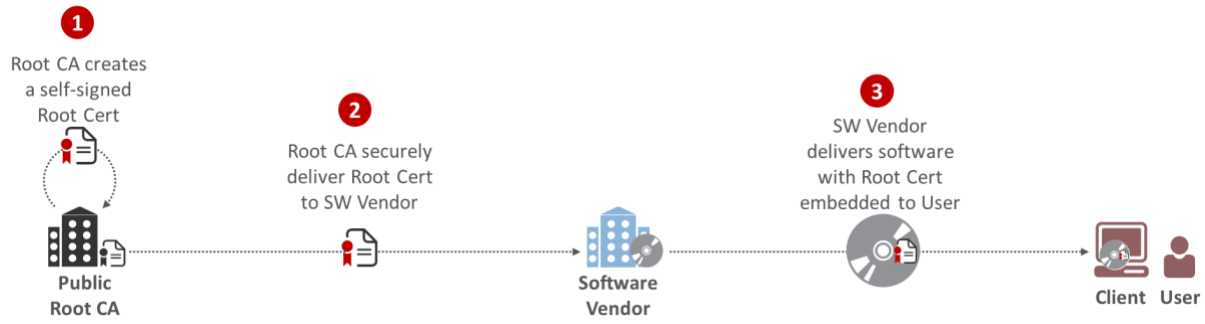
289

290 2.1 Certificate Authorities

291 TLS server certificates are issued by entities called certificate authorities (CAs). CAs digitally sign
292 certificates so that their authenticity can be validated — to prevent attackers from easily impersonating
293 servers. Clients (e.g., browsers, devices, applications, services) validate certificates by using a CA's
294 certificate to verify the signature. Clients, such as browsers, are configured to trust specific CAs (called
295 root CAs). This is done by installing a CA's certificate, commonly called a root certificate, on the client.

296 Some CAs arrange for their root certificate to get installed by software manufacturers in their software
297 (e.g., browser, application, or operating system) so the certificates issued by the CAs are trusted
298 broadly. These CAs are commonly called public root CAs. (See Figure 2-5.)

299 **Figure 2-5 A Public Root CA's Root Certificate Is Delivered to the User, Installed on a Software**
300 **Vendor's Software**



301

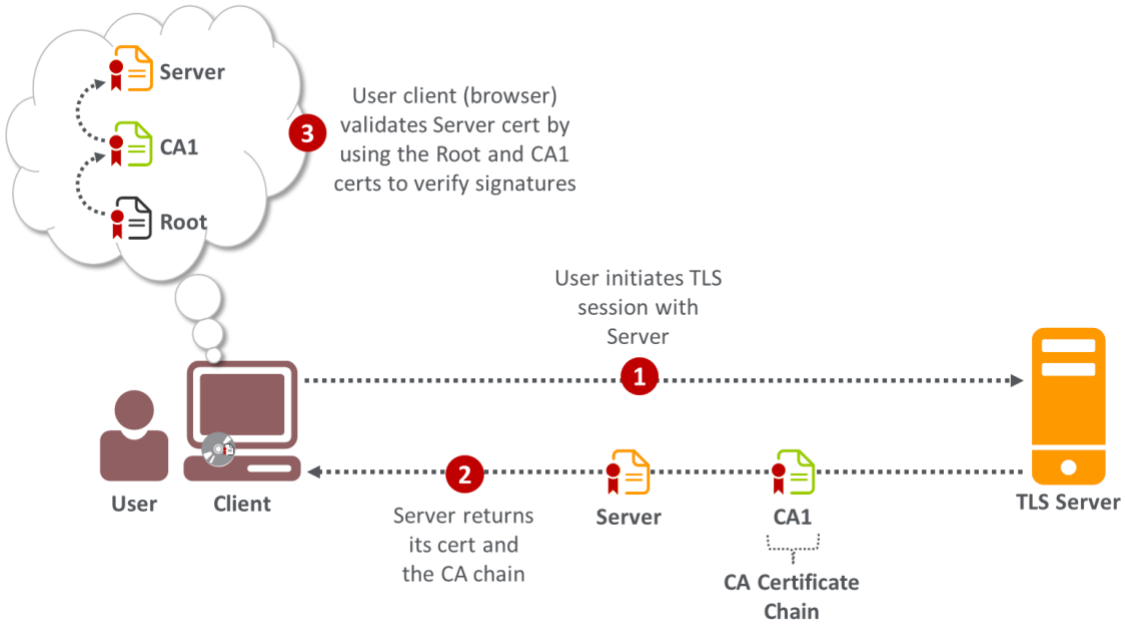
302 To protect them from attacks, root CAs are generally not connected to the internet and do not issue TLS
303 server certificates directly. Root CAs certify other CAs, generally called intermediate or issuing CAs,
304 which issue TLS server certificates. (See Figure 2-6.)

305 **Figure 2-6 A Root CA Issues a Certificate to an Intermediate/Issuing CA, Which Issues TLS**
306 **Server Certificates**

307

308 As shown in Figure 2-7, when a client, such as a browser, connects to a TLS server, the server will return
309 its certificate as well as the certificate for the CA that issued its certificate (called the CA certificate
310 chain).

311 **Figure 2-7 Upon Connecting to the Server, the Client Receives Both the Server's TLS Certificate and Its**
312 **CA Certificate Chain**



313

314 Public CAs are regularly audited to ensure they operate in compliance with the CA/Browser Forum
315 Baseline Requirements, which are standards intended to minimize the possibility of CA compromises
316 and fraudulent certificates. When CAs have been found to violate the requirements, their root
317 certificates have been removed from and distrusted by browsers, requiring customers of those CAs to
318 rapidly replace their TLS server certificates.

319 There are three different types of certificates issued by public CAs (as specified by the CA/Browser
320 Forum, which defines standards for public CAs), each with a different level of validation required by the
321 CA to confirm the identity of the requester and its authority to receive a certificate for the domain in
322 question:

323 - Domain Validated (DV): The CA validates that the requester is the owner of the domain, by
324 verifying that the requester can reply to an email address associated with the domain, has
325 operational control of the website at the domain address, or is able to make modifications to
326 the Domain Name System (DNS) record for the domain

327 - Organization Validated (OV): In addition to the checks for DV certificates, the CA conducts
328 additional vetting of the requester's organization

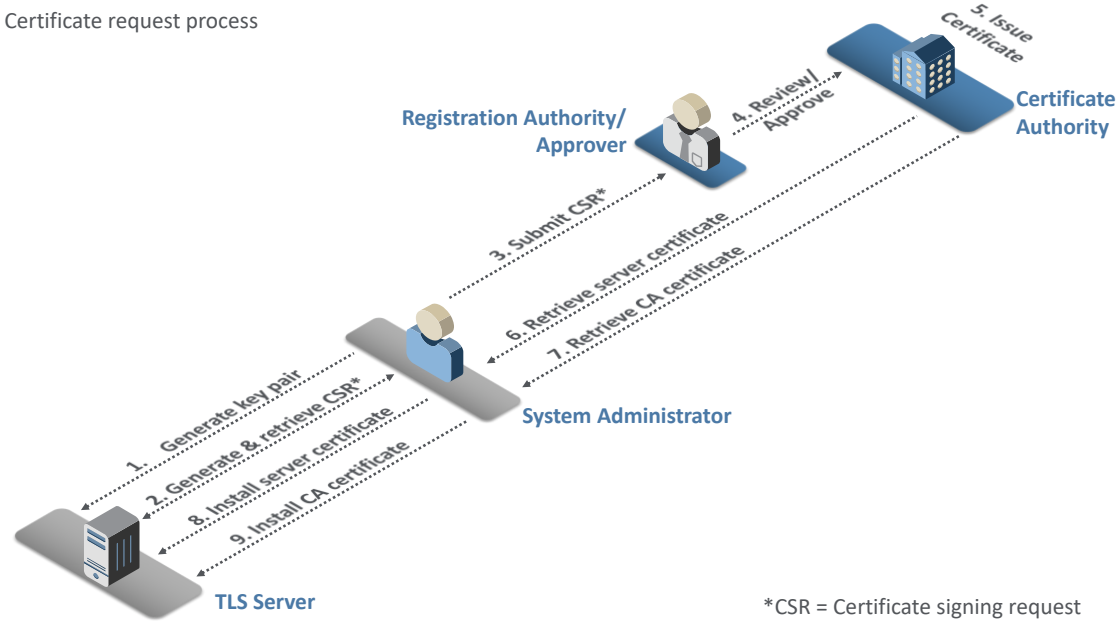
329 - Extended Validation (EV): EV certificates undergo the most rigorous checks, including verifying
330 the identity and the legal, physical, and operational existence of the entity requesting the
331 certificate, by using official records

Organizations that wish to issue certificates to their internal TLS servers can establish their own CAs, commonly called internal CAs. Organizations using internal CAs must ensure that all clients connecting to their servers trust the internal CAs by installing the internal CAs' root certificates on each system acting as a client (e.g., browsers, operating systems, applications, appliances).

2.2 Certificate Request and Installation Process

The following steps, shown in Figure 2-8 and detailed below, are typically followed by a system administrator to get a TLS certificate for a server that he or she manages.

Figure 2-8 Certificate Issuance Process



1. The system administrator for the TLS server uses utilities on the server to generate a cryptographic key pair (a public key and a private key).
2. The system administrator enters the address of the server (e.g., *www.organization1.com*). The utilities create a request for a certificate, called a certificate signing request (CSR), which contains the address of the server and the public key. The system administrator retrieves a copy of the CSR (which is contained in a file) from the server.

3. The system administrator submits the CSR to the registration authority (RA), who acts as a reviewer and approver of the certificate request.
4. The RA/approver reviews the CSR, performs necessary checks to confirm the validity of the request and the authority of the requester, and then sends an approval to the CA.
5. The CA issues the certificate.
6. The CA notifies the system administrator that the certificate is ready, either by emailing a copy of the certificate or providing a link from which it can be downloaded. The system administrator retrieves the server certificate.
7. The system administrator retrieves the CA certificate chain from the CA.
8. The system administrator installs the server certificate on the server.
9. The system administrator installs the CA certificate chain on the server.

The CA certificate chain is used by TLS clients to validate the signature on the server certificate. When a client connects to a TLS server, the server returns its certificate and the CA certificate chain, which can contain one or more CA certificates. The client starts with one of its locally trusted root CA certificates and successively validates the signatures on certificates in the CA certificate chain until it reaches the server certificate.

The system administrator must note the expiration date in the certificate to ensure that a new certificate is requested and installed before the existing certificate expires.

3 TLS Server Certificate Risks

When TLS server certificates are not properly managed, organizations risk negative impacts to their revenue, customers, and reputation. There are four primary types of negative incidents that result from certificate mismanagement: outages to important business applications, caused by expired certificates; security breaches resulting from server impersonation; outages or security breaches resulting from a lack of crypto-agility; and increased vulnerability to attack via encrypted threats.

3.1 Outages Caused by Expired Certificates

TLS server certificates contain an expiration date to ensure that the cryptographic keys are changed regularly; this reduces the possibility of a security breach caused by a compromised private key. If a server certificate is not changed before its expiration date, then clients should generate an error message and stop the connection process to the server. This causes the application supported by the server with the expired certificate to become unavailable.

Application outages can also be caused by the mismanagement of CA certificate chains that results in expired intermediate CA certificates. The TLS server is responsible for providing the client with the

intermediate CA certificates (CA certificate chain) necessary for the client to link the server's end-entity certificate with the root CA certificate trusted by the client. The absence or expiration of an intermediate certificate means the client will not trust the server, even though the server may have a perfectly trustworthy end-entity certificate. Intermediate CA certificates are typically renewed every few years, and it is possible for a TLS server to fail to use the most current version. As a result, although the server certificate has been updated, the installed intermediate CA certificate may expire, resulting in an outage due to expiration. Such outages are often difficult to diagnose because the focus of investigation is typically on the server certificate, which is still valid and not the cause of the outage.

Nearly every enterprise has experienced an application outage due to an expired certificate, including outages to major applications such as online banking, stock trading, health records access, and flight operations. Organizations' increased use of TLS server certificates to secure the organizations' applications increases the likelihood of outages, because there are more certificates to track and more certificates per business application that can impact operations.

Various scenarios result in a certificate expiring while still in use, causing an outage, including these:

- The system administrator forgets about the certificate
- The system administrator ignores notifications that the certificate will soon expire
- The system administrator does not properly install or update the CA certificate chain
- The system administrator is reassigned, and nobody else receives expiry notifications
- The system administrator enrolls for a new certificate but does not install it on the server(s) in time or installs it incorrectly
- The application relies on multiple load-balanced servers, and the certificate is not updated on all of them
- The certificate is installed on a backup system, but the certificate has expired before the backup system is brought online

Troubleshooting an incident where an application is unavailable due to an expired certificate can be complex and often requires hours to discover the source of the problem. If the server on which an expired certificate is deployed is being accessed by people using browsers, then each of those people will receive an error message, making it clear that the cause of the issue is an expired certificate. If, on the other hand, the server with the expired certificate is an application server receiving requests from a web server, then the web server stops its operations and may log a message, but that message may not be immediately discovered in the log file, increasing the amount of time required to identify the root cause of the outage and fix it. If certificates that are deployed on backup systems are not updated when they expire, an outage can occur if operations are shifted to the backup systems.

3.2 Server Impersonation

An attacker may be able to impersonate a legitimate TLS server (e.g., a banking website) if the attacker is able to get a fraudulent certificate containing the address of the server and the attacker's own public key by tricking a trusted CA into issuing the certificate to the attacker or by compromising the CA and issuing the certificate. A client connecting to the attacker's server will accept the certificate because the certificate contains the address to which the client intended to connect and because the certificate has been issued by a trusted CA. Because the certificate contains the attacker's public key (and the attacker also holds the private key corresponding to this public key), the attacker can decrypt the communications from the client (including passwords intended for login to the legitimate server). Alternatively, if the attacker can access a copy of the legitimate server's private key, then the attacker can also impersonate that server by using the legitimate server's certificate. To successfully perform these attacks, the attacker must redirect traffic destined for the legitimate server to a system that the attacker is operating (e.g., using Border Gateway Protocol [BGP] hijacking or DNS compromise). (Note: The BGP is used to communicate optimal routes between internet service providers on the internet. It is possible for an attacker to hijack traffic by falsely advertising that the fastest route to one or more internet protocol [IP] addresses is via systems that the attacker is operating, thereby causing traffic to be rerouted through the attacker's systems. The DNS provides translation between human-readable addresses [e.g., *www.company123.com*] and IP addresses. If an attacker can compromise an organization's DNS account, then the attacker can change the IP address to which traffic intended for that organization will be sent.)

Most private keys used on TLS servers are stored in files. The private keys are directly managed and handled by system administrators, who can make copies of the private keys. In addition, many TLS servers are clustered (for load balancing); in many cases, the same TLS server certificate and the private key will be copied to each server in the cluster. The manual handling and copying of private keys significantly increase the possibility of a key compromise.

3.3 Lack of Crypto-Agility

There are several types of incidents that have required organizations to replace large numbers of TLS certificates and private keys, including the following:

- **CA compromise**: If a CA is breached by an attacker, then the attacker can cause that CA to issue fraudulent certificates. After the CA breach is discovered and forensics are performed, it may be concluded that certificates issued by the CA cannot be trusted and that new certificates must be installed on all servers with certificates from the compromised CA.
- **Vulnerable algorithm**: Cryptographic algorithms are constantly evaluated for vulnerabilities, by parties with both positive and negative intent. When an algorithm is found to be vulnerable (e.g., Secure Hash Algorithm 1 [SHA-1] for signature generation), TLS server certificates that are dependent on the algorithm must be replaced. Ongoing advancements in quantum computing require that organizations establish the ability to rapidly replace all existing certificates and keys and be prepared for implementation of post-quantum algorithms.

- **Cryptographic library bug**: Because cryptographic operations are quite complex, a few groups have specialized in developing cryptographic libraries that are used by TLS servers and other systems. If a bug is found with the key-generation functions of a cryptographic library, then all keys generated since the bug was introduced must be replaced. (Note: In 2008, a key-generation bug in the cryptographic libraries in Debian Linux was discovered. That bug was introduced in 2006. In 2017, a key-generation bug was discovered in the Infineon cryptographic libraries used in smart cards and trusted platform module chips.)

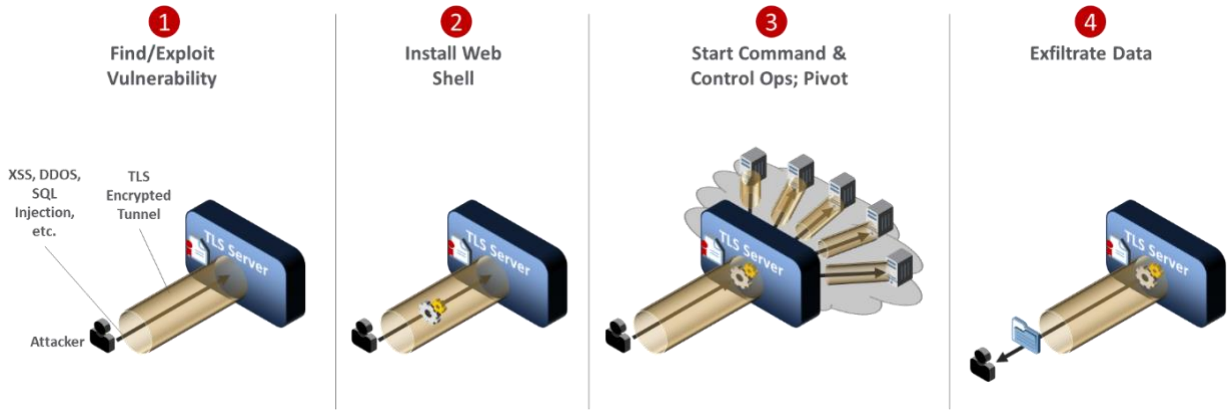
Most enterprises are not prepared to respond to the large-scale cryptographic failure that results from these types of incidents. Many organizations do not have comprehensive inventories of their TLS server certificates. In addition, they cannot contact the certificate owners, because they do not have up-to-date information about the certificate owners responsible for each certificate. Finally, many organizations rely on manual processes to manage certificates and do not have processes for tracking the progress in replacing large numbers of certificates — leaving the organizations to guess how many systems have been updated. All these factors can result in organizations requiring several weeks or months to replace all affected certificates, during which time business applications can be unavailable or vulnerable to security breaches.

3.4 Encrypted Threats

Many organizations are working to encrypt all communications by using TLS server certificates to prevent interception of plaintext credentials and eavesdropping on communications. While TLS server certificates enable confidentiality for legitimate communications, they can also allow attackers to hide their malicious activities within encrypted TLS connections. When a TLS server certificate is installed and enabled on a server, all users who connect (including attackers) can establish an encrypted connection to the server. An attacker who establishes an encrypted connection can then begin to probe the server for vulnerabilities within that encrypted connection.

The following steps, shown in Figure 3- and detailed below, describe how an attacker can leverage encrypted connections in his or her attacks.

Figure 3-1 How an Attacker Leverages Encrypted Connections to Hide Attacks



1. The attacker begins by connecting to a server and establishing an encrypted TLS session. Within that encrypted session, the attacker can probe for vulnerabilities that exist on the server and its software

2. If the attacker discovers a vulnerability and sufficiently elevates his or her privileges, then the attacker can load malware, generally called a "web shell," onto the server

3. With this web shell loaded, the attacker can send commands over TLS connections (i.e., encrypted connections facilitated by the server's certificate). The attacker can then work to pivot to other systems by probing for vulnerabilities in servers accessible from the compromised system. The increased use of encryption enables an attacker who has compromised one system to pivot and attack other systems via encrypted connections, without being detected

4. Once the attacker has successfully reached data that he or she desires, the attacker is able to use the web shell to exfiltrate data. Because the attacker is establishing TLS connections by using the server's certificate to connect to the web shell, all the exfiltrated data is encrypted while in transit

As stated in Section 1.2, in accordance with their security policies, some organizations may choose to perform inspection of internal traffic that has been encrypted using TLS. The question of whether to perform such inspection is complex, and it involves important tradeoffs between traffic security and traffic visibility that each organization should weigh for itself.

Some organizations are concerned about the risk posed by attackers who leverage encrypted connections to hide their attacks, as illustrated in Figure 3-1 above. If these attackers gain access to trusted internal systems via malware or some other exploit, they may be able to move about the network without being detected by hiding their traffic within TLS connections. Organizations that are concerned about these risks want the option of decrypting internal TLS traffic so it can be inspected. Such inspection may be used not only for intrusion and malware detection, but also for troubleshooting,

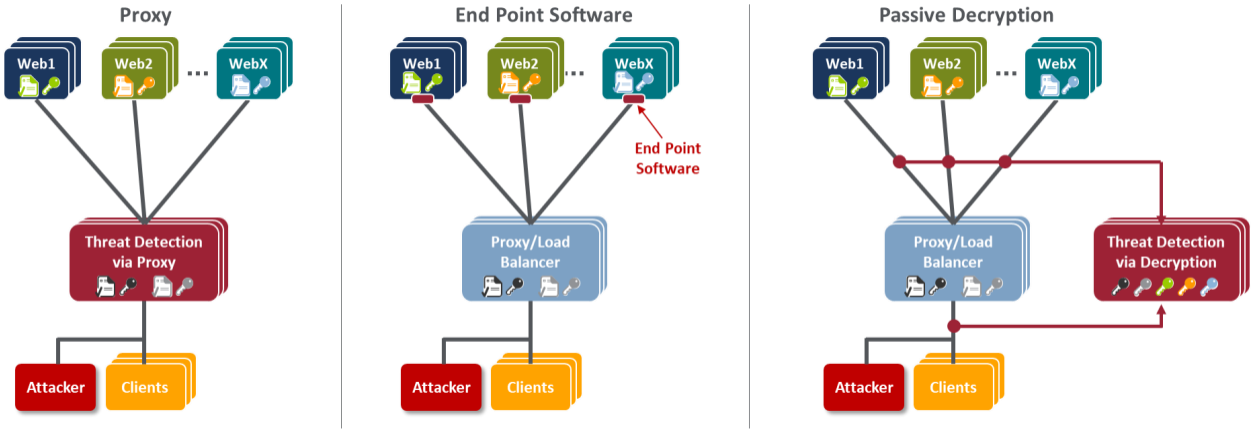
fraud detection, forensics, and performance monitoring. These organizations have concluded that the visibility into their internal traffic that can be provided by TLS inspection is worth the tradeoff of the weaker encryption and other risks that come with such inspection. For these organization, TLS inspection may be considered standard practice and may represent a critical component of their threat detection and service assurance strategies. Some of these organizations have complex networks that are several tiers deep, so it would not be realistic to expect them to be able to manage the movement of keys required to perform such inspection securely using purely manual processes. For those organizations that have a policy to perform inspection of TLS traffic, this document provides recommendations regarding how to securely move the TLS private keys needed for this inspection.

On the other hand, inspection creates a single location where traffic may be decrypted, creating an attractive target for hackers. It also may have compliance implications if sensitive data is being decrypted. An organization that performs decryption on border devices or that performs passive internal decryption runs the risk of such devices being taken over by a malicious attacker who would then have access to private keys and traffic. In addition, passive decryption requires the use of static key exchange, which results in weaker encryption than can be achieved when using ephemeral key exchange methods. If an attacker captures a server's private key and that key was negotiated using static key exchange, the attacker will also be able to decrypt traffic that had been captured in the past. If, instead, that key was negotiated using an ephemeral key exchange method, the key will provide forward secrecy, meaning the attacker will not be able to decrypt past traffic. For some organizations, the reduced security of performing inspection or using static keys is unacceptable. These organizations have determined that the security risks posed by inspection of internal TLS traffic are not worth the potential benefits of having visibility into the encrypted traffic. These organizations should have a policy against performing TLS inspection. As an alternative to inspection, they may choose to perform traffic analysis to try to detect illegitimate internal TLS traffic. None of the discussion or recommendations in this document are intended to mandate or encourage an organization to begin performing TLS inspection of its traffic if that organization has determined that the risks of TLS inspection are not worth the benefits.

An organization that has a policy to perform inspection of TLS traffic so it can monitor and detect malicious activity has several methods it can use to gain visibility into encrypted communications. Some examples are listed below and are illustrated in Figure 3-2:

- placing a threat detection system that acts as a reverse proxy in front of servers
- installing end point software on each server to monitor communications
- passively decrypting communications

536 **Figure 3-2 Methods for Gaining Visibility into Encrypted Communications**



537

538 The use of threat detection proxies is ideal at the perimeters of organizations for monitoring inbound
539 internet communications for attacks. The threat detection proxy is connected in-line, requiring all
540 inbound traffic to pass through it before moving on to the next device. The threat detection proxy
541 terminates the TLS connection. It decrypts and examines incoming traffic. If the traffic is determined to
542 be malicious, the proxy drops it. Because the threat detection proxy is terminating all TLS connections, it
543 must have a certificate for each server to which clients are attempting to connect. After the threat
544 detection proxy decrypts and examines the traffic, it can establish a TLS session with the appropriate
545 server behind it and send the traffic to that server in an encrypted TLS session.

546 While a threat detection proxy is ideal for use at the perimeter of an organization, many organizations
547 also want to inspect their internal TLS traffic. Many enterprise applications include multiple tiers of
548 servers and services (e.g., load balancers, web servers, application servers, databases, identity services)
549 that communicate with each other internally via encrypted TLS sessions, making it impractical to place
550 threat detection proxies between all systems on internal networks.

551 End point software can be installed on each server to monitor communications, alleviating the need to
552 install proxies, but may impose additional processing requirements on servers that are already under a
553 high load. In addition, because of the diversity of TLS server systems, it may be difficult to find an end
554 point solution that operates on all platforms and provides comprehensive and consistent visibility and
555 monitoring of all communications.

556 Passive, out-of-band decryption and threat analysis are performed by using devices that decrypt
557 TLS-encrypted communications but that do not terminate TLS connections. The TLS connection is
558 established between the client and the server. The passive decryption device listens to the TLS traffic
559 without affecting it and decrypts it. Threat analysis is performed either by the passive decryption device
560 or via other systems to which decrypted traffic is forwarded. Security-focused passive decryption
561 devices can detect malicious traffic that has been sent on TLS connections, but these devices do not

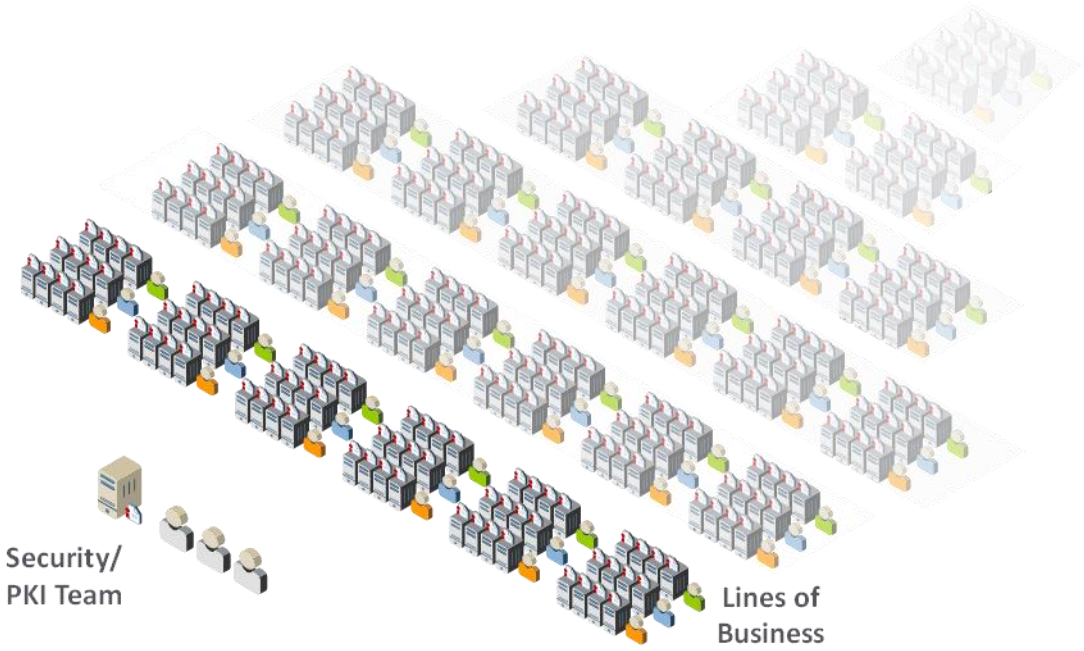
react in real time to block this traffic. Passive decryption does not require a change in network architecture or loading additional software on TLS servers. However, passive decryption poses a TLS server certificate management challenge, because private keys must be copied to decryption devices from each TLS server whose communications will be monitored. The transfer of private keys must be done securely to avoid a key compromise and rapidly to avoid blind spots in monitoring for attacks. Automation can significantly aid in securely transferring private keys from TLS servers to the decryption device and keeping keys up-to-date when certificates are replaced.

4 Organizational Challenges

Despite the mission-critical nature of TLS server certificates, many organizations do not have clear policies, processes, and roles and responsibilities defined to ensure effective certificate management. Moreover, many organizations do not leverage available technology and automation to effectively manage the large and growing number of TLS server certificates. As a result, many organizations continue to experience significant incidents related to TLS server certificates.

As illustrated by Figure 4-1, the management of TLS server certificates is challenging due to the broad distribution of certificates across enterprise environments and groups, the complex processes needed to manage certificates, the multiple roles involved in certificate management and issuance, and the speed at which new TLS servers are being deployed. TLS server certificates are typically issued by a Certificate Services team (often called the public key infrastructure team). However, the certificates are commonly installed and managed by the certificate owners — the groups and the system administrators responsible for individual web servers, application servers, network appliances, and other devices for which certificates are used.

583 **Figure 4-1 TLS Certificates Are Distributed Broadly Across Enterprise Environments and Groups**



584

585 4.1 Certificate Owners

586 The term "certificate owner" is used to denote a group responsible for systems where certificates are
587 deployed. Typically, there are several roles within a certificate owner group, including executives who
588 have ultimate accountability for ensuring that certificate-related responsibilities are addressed, system
589 administrators who are responsible for managing individual systems and the certificates on them, and
590 application owners who can review and approve certificate requests from system administrators to
591 ensure that only authorized certificates are issued. The certificate owners typically are not
592 knowledgeable about the risks associated with certificates or the best practices for effectively managing
593 certificates.

594 With the advent of virtualization, the development and operations (DevOps) teams provision systems
595 and software through programmatic means. This introduces a new type of certificate owner and new
596 TLS server certificate challenges for organizations. As organizations push for more rapid and efficient
597 deployment of business applications, many DevOps teams deploy certificates without coordination with
598 the Certificate Services team. This can result in certificates for mission-critical applications not being
599 tracked. This can be particularly problematic if bugs in DevOps programs/scripts cause certificates to be
600 improperly deployed or updated. In addition, as DevOps teams adopt newer frameworks and tools, it is
601 important to continue to monitor certificates and applications deployed and maintained by older
602 DevOps frameworks and tools.

4.2 Certificate Services Team

The Certificate Services team is typically the group that has been given responsibility for managing relationships with public CAs and for the internal CAs. The Certificate Services team typically comprises one to three people. Though the team members have good knowledge and expertise about TLS server certificates, they do not have the resources or access required to directly manage certificates on the extensive number of systems where certificates are deployed. However, the Certificate Services team is often blamed when TLS certificate incidents, such as outages, occur.

5 Recommended Best Practices

To effectively address the risks and organizational challenges related to TLS server certificates and to ensure that they are a security asset instead of a liability, organizations should establish a formal TLS certificate management program with executive leadership, guidance, and support. The formal TLS certificate management program should include clearly defined policies, processes, and roles and responsibilities for the certificate owners and the Certificate Services team, as well as a central Certificate Service. The program should be driven by the Certificate Services team but should include active participation by the certificate owners — whether the certificate owners are responsible for traditional servers, appliances, virtual machines, cloud-based applications, DevOps, or other systems acting as TLS servers.

5.1 Establishing TLS Server Certificate Policies

As previously mentioned, most certificate owners are typically not knowledgeable about the best practices for effectively managing TLS server certificates. Because certificate owners are responsible for the systems where certificates are deployed, it is imperative that they be provided with clear requirements and that those requirements be enforced as policies. This section provides recommended TLS server certificate policies. It also includes recommended responsibilities for the certificate owners and the Certificate Services team to successfully meet those requirements and policies.

These recommendations are intended to serve as guidance for organizations that do not already have their own TLS server certificate management policies and responsibilities defined, or that are looking to improve existing policies and procedures. They are not intended to override any organization's existing policies. Organizations should feel free to copy, delete, augment, or modify these recommended policies and responsibilities as needed to suit their own requirements. Appendix B contains a table that maps the recommended best practices for TLS server certificate management proposed in this document to the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework—CSF). Appendix C contains a table that explains how specific controls defined within NIST Special Publication 800-53 should be applied to these TLS server certificate management recommended best practices.

The recommended requirements in the remaining subsections use the word "should" throughout. Based on their own security policies, organizations may choose to make these recommendations mandatory, e.g., by changing "should" to "must."

5.1.1 Inventory

To address TLS server certificate risks, organizations should establish and maintain clear visibility across all TLS server certificates in their environment so they can perform the following actions:

- detect potential vulnerabilities (e.g., the use of weak algorithms, such as SHA-1)
- identify certificates that are nearing expiration and replace them
- respond to large-scale cryptographic incidents, such as a CA compromise, vulnerable algorithms, and cryptographic library bugs
- ensure compliance with regulatory guidelines and established organizational policy

This visibility is achieved by maintaining an inventory of all TLS server certificates. A single central inventory is recommended, as it minimizes the possibility of overlooking critical TLS server certificates.

Recommended Requirement:

An up-to-date inventory of all deployed certificates (end-entity certificates and CA certificate chain certificates) should be maintained, including certificates on backup systems that may not necessarily be online. For each certificate, the inventory should include the following components:

- Subject Distinguished Name (DN)
- Subject Alternative Names (SANs)
- issue date (i.e., notBefore date)
- expiration date (i.e., notAfter date)
- issuing Certificate Authority (CA)
- key length
- key algorithm (e.g., Rivest, Shamir, & Adleman [RSA]; Elliptic Curve Digital Signature Algorithm [ECDSA])
- signing algorithm
- validity period (i.e., from the notBefore date/time to the notAfter date/time)
- installed location(s) of certificate (e.g., IP or DNS address and file path)
- certificate owner (i.e., the group responsible for the certificate)

- group responsible for the DevOps technology used to deploy the certificate (if the certificate was deployed via DevOps technology)
- contacts (i.e., the group of individuals that should be notified of issues)
- approver(s) (i.e., the parties responsible for reviewing issuance and renewal requests)
- type of system (e.g., web, email, directory server, appliance, virtual machine, container)
- business application (i.e., the application using the certificate)
- applicable regulations (e.g., Payment Card Industry Data Security Standard [PCI-DSS], Health Insurance Portability and Accountability Act [HIPAA])
- key-usage flags
- extended key-usage flags

Recommended Responsibilities:

- Certificate Services team: provide a central system for certificate owners to establish and maintain their inventories
- Certificate owners: establish and maintain an inventory of all certificates and keys on their systems

5.1.2 Ownership

To rapidly respond to issues with TLS server certificates, it is necessary to know who is responsible for each certificate. This information should be kept up-to-date as people are reassigned or terminated. Because reassignments can happen frequently, and because there may be a lag in updating ownership information, it is recommended that ownership be assigned to functional groups (e.g., an Active Directory [AD] group) that contain multiple individuals, instead of assigning ownership to individuals. In cases where DevOps technologies are used to deploy TLS server certificates, the group responsible for the DevOps deployment technology should be tracked, in addition to the certificate owner, so they can both be contacted when incidents arise.

Recommended Requirement:

- Contact information for certificate owners should be assigned to functional groups (e.g., AD groups), and the content of a group should be updated within <30> business days of a role reassignment or termination of an individual member of that group. (Note: Here and elsewhere in this practice guide, when specific time frames, such as "<30> business days" are recommended, these values are often placed within brackets ("<>") to indicate they are provided only as suggestions. Each organization should determine the time frames to be instituted within its own enterprise, based on its needs. If it is possible for organizations to require compliance within shorter time frames, then that would be preferable.)

- If the certificate was deployed via DevOps technology, contact information should be provided for the group that is responsible for this technology, and the content of this group should be updated within <30> business days of a role reassignment or termination of an individual member of that group

Recommended Responsibilities:

- Certificate Services team: provide a system to track ownership as part of the inventory
- Certificate Owners: keep ownership information up-to-date (i.e., membership information for certificate owner group up-to-date)
- DevOps team: Where DevOps technology is used to deploy the certificate, the DevOps team should keep membership information for DevOps deployment technology group up-to-date

5.1.3 Approved CAs

CAs are trusted issuers of certificates. If organizations do not control the CAs that are used to issue certificates in their environments, then they will face several potential risks:

- **Increased costs**: If multiple groups are individually purchasing certificates from CAs, then the cost per certificate can be significantly higher because organizations are not taking advantage of volume discounts
- **Trust issues**: Each CA used to issue TLS certificates to servers in an organization must be trusted by the clients connecting to those servers via a root certificate. If a large number of CAs (internal and external) is used, then the organization is required to take on the extra burden of maintaining multiple trusted CA certificates on clients to avoid cases in which the necessary CA is not trusted, which can result in outages
- **Security risk**: A certificate owner may decide to set up his or her own CA on a system that does not have the necessary security controls and to configure the system to trust that CA. This increases the possibility of an attacker impersonating a server if the attacker compromises that CA and issues fraudulent certificates
- **Unexpected CA incidents**: If one of the untracked CAs used in the organization's environment encounters an issue, such as a CA compromise or suddenly being untrusted by browser vendors, then the organization may have to scramble to avoid security or operational issues for core applications

To ensure they can rapidly respond to a CA compromise or another incident when using public CAs, organizations should maintain contractual relationships with more than one public CA. By doing this, organizations will not have to scramble to negotiate a contract (which may take days or weeks) while attempting to respond to an urgent situation. Organizations should also maintain at least one backup internal CA so they can respond to an internal CA compromise or incident.

Recommended Requirements:

Certificates should be issued only by the following CAs:

- <External CA1>
- <External CA2>
- <Internal CA1>
- <Internal CA2>
- <…>
- Contractual relationships with at least two public CAs that conform to the CA/Browser Forum Baseline Requirements should be maintained at all times
- Internal CAs should be securely operated. Backup internal CAs should be maintained to support a rapid response to incidents, such as CA compromise

Recommended Responsibilities:

- Certificate Services team: manage business relationships with approved external CAs, and operate or outsource the operation of approved internal CAs
- Certificate owners: ensure that only certificates from approved CAs are used

5.1.4 Validity Periods

The validity period for a certificate defines the time that it is valid, from the first date/time (notBefore) to the last date/time (notAfter) that it can be used. It is important to note that the validity period of a certificate is different than the cryptoperiod of the public key contained in the certificate and the corresponding private key. It is possible to renew a certificate with the same public and private keys (i.e., not rekeying during the renewal process). However, this is only recommended when the private key is contained with a hardware security module (HSM) validated to Federal Information Processing Standards (FIPS) Publication 140-2 Level 2 or above.

One of the greatest risks of private-key compromise is from administrators who have direct access to plaintext private keys (including the ability to make a copy) and who are then reassigned or terminated. Although certificates would ideally be changed (rekeyed) each time an administrator with access to private keys is reassigned, this is often not practical. Therefore, ensuring certificates and their corresponding private keys are changed regularly is important, as shorter validity periods reduce the amount of time that a compromised private key can be used for malicious purposes. However, validity periods that are too short may increase the risk of outages. Organizations should determine the ideal validity period that balances security and operational risks for their organization. In general, due to the

regular reassignment of administrative staff, it is recommended that validity periods be one year or less. The automated management of certificates can enable a more frequent renewal of certificates.

Recommended Requirement:

- The maximum validity period (i.e., from the notBefore date to the notAfter date for certificates should be <one year or less>

Recommended Responsibilities:

- Certificate Services team: ensure CAs are available to certificate owners to issue certificates with approved validity periods
- Certificate owners: ensure certificates are renewed and replaced before their expiration

5.1.5 Key Length

Each certificate contains a public key that is mathematically matched to a private key (which should be kept secret). To prevent an attacker from guessing the value of the private key, it is necessary to randomly pick the value of the private key from a large set of possible values. For example, it is more difficult for someone to guess a number selected between zero and 1,000,000 than a number selected between zero and 100. The key length effectively defines the size of the range of numbers from which private and public key values are selected. A longer key length is considered more secure. However, longer key lengths require more processing power and time, as well as more storage. Consequently, a balance must be struck between security risk and resource requirements. NIST monitors the industry to continually assess the potential crypto-analytical capabilities of possible attackers and their ability to guess the values of private keys. Based on this information, it sets recommended minimum key lengths. It is recommended that organizations require the use of keys with key lengths equal to or greater than the NIST recommendations.

Recommended Requirement:

All certificates should use key lengths that comply with NIST Special Publication (SP) 800-131A, which are currently equal to or greater than the following key lengths:

- RSA: <2,048>
- ECDSA: <224>

Recommended Responsibilities:

- Certificate Services team: provide dashboards, reports, and alerts that enable the rapid detection of unauthorized key lengths, and provide automation technologies that enable rapid remediation

- Certificate owners: use only TLS certificate public and private keys whose key lengths meet or exceed the organization's key-length policy, monitor their inventory, and replace certificates that do not comply with the policy

5.1.6 Signing Algorithms

Certificates are digitally signed by CAs so their authenticity can be verified. Signatures are generated by using digital signature algorithms (e.g., RSA, ECDSA) and hash algorithms (e.g., Secure Hash Algorithm 256 [SHA-256]). If certificates are signed by using a signing algorithm with an insufficient key length or by using vulnerable hash algorithms (e.g., SHA-1), then attackers can forge certificates and impersonate TLS servers. Consequently, organizations should ensure that all certificates are signed by using cryptographic algorithms that conform to approved standards.

Recommended Requirement:

- All certificates should be signed with an approved signature algorithm and key length and with an approved hash algorithm (e.g., SHA-256), as defined in NIST SP 800-131A and FIPS Publication 180-4

Recommended Responsibilities:

- Certificate Services team: ensure the availability of CAs that use approved signing algorithms, and provide reporting and alerting tools to enable the rapid identification of noncompliant certificates
- Certificate Owners: use only certificates signed with an approved signature algorithm and key length and with an approved hash algorithm, and identify and replace certificates signed with unapproved algorithms or key lengths

5.1.7 Subject DN and SAN Contents

The combination of Subject DN and SAN are used to identify the TLS server to which the certificate is issued. The Subject DN is in the form of an X.500 DN, which can include information such as the country, state, city/locality, organization, organizational unit (e.g., department), and a common name (CN). The CN, when present, and the SAN field contain the fully-qualified domain name or IP address of the TLS server. For publicly trusted certificates, the contents of the Subject DN are governed by the public CA that issues them. The CA/Browser Forum requires the SAN field to be present, however, the CN is now deprecated and the other fields in the DN are now optional, though in practice they are still present. For internal certificates, the contents of the Subject DN fields, such as the organizational unit, can help identify the group responsible for certificates.

Public CAs will often perform checks to validate that an organization owns a top-level domain (e.g., *www.company123.com*), and will then allow the organization to request a certificate with Subject DNs and with SANs containing domains subordinate to that domain (e.g., *www.company123.com*,

www.server1.company123.com). Consequently, it is critical that organizations implement approval processes that ensure the Subject DNs and SANs in all certificate requests are thoroughly reviewed and vetted before they are sent to the CA.

Recommended Requirements:

Names used in Subject DNs should conform to the following requirements:

- The Organization (O) attribute in the Subject DN should be one of the following values:
  - <e.g., Company, Inc.>
  - The Organizational Unit attribute in the Subject DN should conform to the following categorization:
    - <specify whether department, location, or another categorization should be used>
  - The Locale (City), State (Province), and Country codes should be set to the following location:
    - <City, State, Country of organization identified in O = headquarters offices>
  - The CNs and SANs should not include wildcards (e.g., *.company123.com).
- The fully-qualified domain names or IP addresses in all Subject DNs and SANs should be reviewed and approved by an individual who is knowledgeable about the application or system for which the certificate is being requested and who can confirm that the requester is authorized to make the request.

Recommended Responsibilities:

- Certificate Services team: provide technology solutions to automatically detect and prevent Subject DN and SAN policy violations
- Certificate owners: ensure the Subject DNs and SANs in all certificates comply with policy

5.1.8 Automation

The broadening use of and reliance on TLS server certificates to secure important applications is rendering manual certificate management impractical. Risks such as certificate-related outages are often the result of errors made while manually managing certificates. Organizations are unable to manually replace large numbers of certificates in response to large-scale cryptographic incidents, such as CA compromises, in a timely manner. Consequently, organizations should work to automate certificate management on as many systems and applications as possible to decrease security and operational risks. Historically, many organizations can find it difficult to induce certificate owners to move from manual to automated methods—though the move to automation can significantly reduce their work and risk. New automation tools (e.g., DevOps) and protocols have increased the methods and

options by which automated certificate management can be successfully performed. Consequently, organizations should define clear guidelines and policies for automation and for when continued manual management is justified due to operational or organizational constraints.

Recommended Requirement:

- Automation should be used wherever possible for the enrollment, installation, monitoring, and replacement of certificates, or justification should be provided for continuing to use manual methods that may cause operational security risks.

Recommended Responsibilities:

- Certificate Services team: provide a central system that supports certificate owners in automating the management of their certificates
- Certificate owners: automate the management of their certificates

5.1.9 Certificate Request Reviews – Registration Authority (RA)

To prevent the issuance of rogue certificates that can be used maliciously to impersonate legitimate servers, all certificate requests should be vetted to ensure they are issued only for valid systems and requested only by authorized parties. For certificates requested by individuals, it is important that the reviewer/approver has sufficient knowledge about the need for the certificate and about the personnel authorized to request certificates for the specific DNS address of the servers. It is generally impossible for a central team to be aware of all new applications and the people authorized to request certificates for those applications. Consequently, it is necessary to have certificate requests reviewed by local application owners who have this knowledge. For certificates requested by automated processes, such as DevOps frameworks, the necessary automated controls should be put in place to ensure that requesting applications are authenticated and that the DNS addresses for which they request certificates match specific patterns.

Recommended Requirements:

- All manual certificate requests for first issuance or renewal should be reviewed and approved by the business or application owner, who will confirm the following statements are true:
  - A certificate is required for the application/system. The certificate CN (when included) and SANs of the certificate match the addresses of the application/system in question.
  - The requester is authorized to make the request.
- When certificates are being issued by automated processes, the automated process should be reviewed by the business or application owner prior to implementation, who will confirm the following statements are true:
  - The automated process is capable of requesting certificates for specific CNs and SANs.

- There is consideration for the automation of the entire certificate life cycle, including renewal and revocation, built into the automated processes.
- A system for auditing and reviewing all certificates issued by the automated processes is in place.

Recommended Responsibilities:

- Certificate Services team: provide a central system for assigning approvers, alerting approvers when certificate requests need approval, and enabling approvers to review and approve/reject requests
- Certificate owners: assign review/approval responsibility to individuals who have knowledge of the systems (addresses) required for applications and of the individuals authorized to request certificates for those systems, and approve certificate requests in a timely manner

5.1.10 Private Key Security

Each TLS server certificate has a corresponding private key that must be kept secret to prevent compromise. Often, the private keys used with TLS server certificates are stored in plaintext files, which may be accessible by administrators if not properly secured. Even when the files where private keys are stored are encrypted with passwords, the passwords are stored in plaintext configuration files so that TLS servers can gain access to the private keys when they are started. It is possible to protect TLS private keys in HSMs; however, due to the large number of TLS servers where private keys would be required, many organizations have not used HSMs to protect private keys. Organizations should assess the criticality and risk of each TLS server and determine the appropriate level of protection required for private keys. Further, organizations should ensure that only authorized personnel have access to private keys and that the authorized personnel are trained in the processes necessary to keep the private keys secure.

Recommended Requirements:

- Access to TLS server private keys stored in plaintext files should be limited to authorized personnel. For mission-critical systems, TLS private keys should be stored in an HSM.
- Individuals granted access to private keys should complete training on procedures and practices for keeping private keys secure.

Recommended Responsibilities:

- Certificate Services team: provide training on the proper procedures for keeping private keys secure, and provide automation to simplify the management of TLS private keys stored in HSMs
- Certificate owners: ensure only authorized personnel are granted access to private keys, regularly review who is granted access to private keys, and ensure the authorized personnel receive training on the proper procedures for keeping private keys secure

5.1.11 Rekey/Rotation upon Reassignment/Terminations

Most private keys associated with TLS server certificates are stored in plaintext files. System administrators who manually manage TLS server certificates and associated private keys on their systems can make copies of the private-key files. Consequently, if a system administrator is reassigned or terminated, then the private key and certificate should be replaced (renewed) with a new key pair and certificate, and the previous certificate should be revoked, to prevent any malicious activities with the original private key and certificate. If automation is used for the management of certificates and private keys and if direct access by system administrators is limited (via limited-access controls and audit logging on any access), then certificate owners can avoid replacing certificates when a system administrator is reassigned or terminated.

Recommended Requirement:

- Private keys and the associated certificates that have the capability of being directly accessed by an administrator should be replaced within <30> days of reassignment or <5> days of termination of that administrator.

Recommended Responsibilities:

- Certificate Services team: provide automated certificate and key management services that remove the need for administrators to manually access private keys, alleviating the need to replace certificates and private keys when a system administrator is reassigned or terminated
- Certificate owners: ensure manually managed certificates and private keys are replaced when a system administrator with access is reassigned or terminated

5.1.12 Proactive Certificate Renewal

When a certificate is nearing expiration, it should be replaced. The replacement of certificates involves multiple steps, including reviewing and approving requests and testing the newly installed certificate(s) to ensure the application they secure is operating properly after replacement. If an unexpected issue is encountered with the new certificate and the associated private key, the previous certificate and private key can be restored and used if the certificate has not yet expired. If certificate owners are not proactive and instead wait until the last minute before requesting, obtaining, and installing a new certificate, this procrastination can cause unplanned, urgent work by multiple teams (including the Certificate Services team) and risk unplanned downtime for the application. Certificate owners should plan, initiate, and complete the certificate renewal, installation, and testing process several weeks ahead of certificate expiration to ensure unexpected issues and circumstances can be addressed and to avoid unnecessary "fire drills" for supporting teams (e.g., the Certificate Services team).

Recommended Requirement:

- Certificates should be renewed, installed, and tested at least <30> days prior to expiration of the currently installed certificate.
- If the validity period (total lifetime) of a certificate is shorter than <60> days (e.g., 20-day certificates used in short-lived/automated applications), then the certificate should be renewed before <80 percent> of the total validity period has elapsed.

Recommended Responsibilities:

- Certificate Services team: provide automated services for monitoring certificate expiration dates, send reports to certificate owners showing certificates expiring in the next <60–90> days, send alerts and escalations to certificate owners for certificates expiring in <30> days or fewer, and send alerts to executives for certificates expiring in <30> days or fewer
- Certificate owners: track upcoming expiration dates for their certificates, schedule replacement (in change windows where necessary), and ensure completion of certificate renewal, installation (of the new certificate), and verification of proper operation prior to the minimum renewal windows

5.1.13 Crypto-Agility

There are several incidents that can require organizations to rapidly replace large numbers of certificates and private keys, including CA compromise or distrust, vulnerable algorithms, or bugs in cryptographic libraries. There have been multiple examples of these incidents in recent years, including the CA compromise of DigiNotar, the distrust of Symantec certificates by browser vendors, the deprecation of SHA-1 for signature generation, and cryptographic library bugs in Debian and Infineon. In 2006, NIST first recommended that organizations stop using SHA-1 for signatures. However, many organizations were still struggling to eradicate the use of certificates signed with SHA-1 in 2017, when their use was forcibly stopped by browser vendors.

An unexpected cryptographic incident can require an organization to rapidly respond to ensure that its operations and services to customers are not interrupted for an extended period. In addition, the industry is preparing for a transition to quantum-resistant algorithms, which will require organizations to replace large numbers of certificates and private keys.

Recommended Requirements:

- System owners should maintain the ability to replace all certificates on their systems within <2> days to respond to security incidents such as CA compromise, vulnerable algorithms, or cryptographic library bugs.
- System owners should maintain the ability to track the replacement of certificates so it is clear which systems are updated and which are not.

- Select and establish contracts with backup CAs for public and internal certificates to enable rapid transition in response to a CA compromise.

Recommended Responsibilities:

- Certificate Services team: document effective processes for replacing large numbers of certificates and private keys; train all certificate owners on certificate replacement processes; provide services, such as automation, that enable the rapid replacement of large numbers of certificates and private keys; actively track the occurrence of cryptographic incidents that require replacement of certificates and private keys, and communicate clearly to certificate owners when such an event occurs; and ensure contracts with backup CAs for both public certificates and internal certificates (if applicable) are in place
- Certificate owners: proactively support crypto-agility by maintaining an inventory of all certificates for which they are responsible and corresponding ownership information, making sure that certificate replacement processes are as efficient as possible and that personnel are trained; and appropriately prioritize replacement of certificates and private keys when cryptographic incidents occur

5.1.14 Revocation

If the private key associated with a TLS server certificate is compromised, then the certificate can be revoked by the CA so that potential relying parties are alerted and do not trust the certificate. Certificate owners should understand their responsibility in revoking certificates and should proactively revoke certificates when an incident occurs. Inadvertent or malicious revocation of a certificate can cause downtime for the application that it secures; therefore, organizations should ensure they have processes to prevent unauthorized revocation.

Recommended Requirements:

- TLS server certificates should be revoked if the associated private key has been or is suspected of being compromised.
- Revocation of a TLS server certificate outside the renewal/replacement process can be initiated only by a certificate owner or identified security personnel and should be approved by the Certificate Services team or a designated security approver.

Recommended Responsibilities:

- Certificate Services team: provide the infrastructure and services to ensure that certificates can be rapidly and securely revoked when necessary and that certificates cannot be revoked without proper approval
- Certificate owners: request revocation of old certificates that have been replaced but that are still valid, and request revocation of certificates when a private key is compromised or suspected to be compromised

5.1.15 Continuous Monitoring

Because of the broad use of TLS server certificates in all critical communications, operational or security failures related to TLS server certificates can significantly impact the business operations of organizations. TLS certificates should be continuously monitored to prevent outages and security vulnerabilities. The certificates should be monitored for impending expiration; for situations in which they are not operating, are not configured properly, or are vulnerable; and for situations in which they are not consistent with policy.

Recommended Requirements:

- The expiration dates of certificates should be continuously monitored. Notifications should be automatically sent to certificate contacts <90, 60, and 30> days prior to expiration. If a certificate is not successfully renewed and replaced <30> days prior to expiration, then escalation notifications should be sent to the certificate owner management and incident response teams.
- The operation and configuration of certificates should be periodically checked to identify any issues or vulnerabilities.
- Certificates should be periodically checked to ensure they are consistent with policy.

Recommended Responsibilities:

- Certificate Services team: provide systems and services for continuously monitoring TLS server certificates, and support certificate owners in implementing TLS server certificate continuous monitoring and in keeping it operational
- Certificate owners: ensure continuous monitoring processes are in place and operational for all their TLS server certificates

5.1.16 Logging TLS Server Certificate Management Operations

TLS server certificates serve as trusted credentials that authenticate servers for mission-critical applications. Just as logging data access is required for forensics and other purposes, logging all certificate and private-key management operations is critical. Organizations should ensure they have a complete chain of custody for private keys and certificates that includes a log of all operations, including key-pair generation, certificate requests, request approval, certificate and key installation, the copying of certificates and keys (e.g., for load-balanced applications), certificate and key replacement, and certificate revocation. Logs should be collected and stored in a central location so the complete chain of events for certificates and private keys can be reviewed when necessary.

Recommended Requirement:

- A complete automated log should be maintained of all TLS certificate and private-key management operations (from creation to installation to revocation) that includes a description of the operation performed, any relevant metadata about the event (e.g., the location of files), the identity of the person/application performing the operation, and the date/time it was performed.

Recommended Responsibilities:

- Certificate Services team: provide a system for collecting all logged events, and provide tools that automatically log certificate and private-key management operations
- Certificate owners: ensure all tools used for certificate and private-key management operations log events in a central log

5.1.17 TLS Traffic Monitoring

While providing authentication and confidentiality for legitimate communications and operations, TLS can also be used by attackers to hide their operations, such as scanning for vulnerabilities, leveraging vulnerabilities for privilege escalation, denial-of-service operations, and data exfiltration. Depending on organizational policy, in addition to monitoring the content of TLS communications for external-facing systems, organizations may monitor TLS communications between internal systems to retain the ability to detect attackers who are attempting to pivot between internal systems (to gain access to critical data) or are exfiltrating compromised data. This monitoring may be accomplished in a variety of ways, including via proxy, end point software, or passive decryption. As discussed in Section 3.4, each organization should decide for itself whether the security risks posed by monitoring internal TLS traffic are worth the potential benefits of having visibility into the encrypted traffic. If, on the other hand, the organization determines it is in its best interests to perform TLS traffic monitoring, then the recommended related requirements and responsibilities are as follows.

Recommended Requirement:

- Where TLS monitoring via passive decryption is supported, TLS server private keys should be securely and automatically transferred to TLS decryption devices and updated when TLS certificates are replaced.

Recommended Responsibilities:

- Certificate Services team: provide a secure method for transporting TLS private keys between TLS servers and passive decryption devices when passive decryption is used for TLS traffic monitoring
- Certificate owners: ensure all communications protected by TLS are monitored for unauthorized operations and data exfiltration

5.1.18 Certificate Authority Authorization

An attacker can impersonate a server if the attacker is able to get a certificate issued that includes the name of the server and his or her own public key. To mitigate this type of attack, organizations can populate Certificate Authority Authorization (CAA) records for the DNS domains of their servers with the names of one or more CAs authorized to issue certificates for that server. When a CA receives a certificate request for a domain, it should check the domain in the DNS to see if a CAA record is defined. If a CAA record is defined, then before issuing a certificate, the CA should ensure the CA's name is listed in a CAA record for the domain. CAA records can be specified for second-level domains (e.g., *www.organization1.com*), which will apply to all subordinate domains and to individual domains (e.g., *www.alpha.organization1.com*). Because an attacker can attempt to request a certificate for a domain from one of the CAs listed in the CAA record, the organization should ensure the listed CAs accept certificate requests only from parties authorized by the organization.

Recommended Requirement:

- CAA records should be populated with authorized CAs for all domains for which public certificates may be issued.

Recommended Responsibilities:

- Certificate Services team: ensure CAA records are defined with approved CAs for all second-level domains owned by an organization
- Certificate owners: ensure the Certificate Services team is aware of all second-level domains for which the certificate owner is requesting certificates

5.1.19 Certificate Transparency

Certificate Transparency (CT) provides a publicly searchable log of issued certificates. CT is primarily focused on certificates issued by public CAs. Some browsers require that certificates issued by public CAs be published to a publicly available CT log; otherwise, the browser will display a warning to the user. The availability of CT logs enables organizations to confirm that unauthorized certificates have not been issued for their domains.

Recommended Requirement:

- CT logs should be regularly monitored to ensure unauthorized certificates have not been issued for any domains owned by the organization.

Recommended Responsibility:

- Certificate Services team: establish an automated process for monitoring CT logs

5.1.20 CA Trust by Relying Parties

Clients that connect to TLS servers verify the validity of those servers' certificates by using CA certificates or root certificates that they store locally in their systems. Many operating systems and applications (e.g., browsers) are preloaded with certificates from public CAs that have met the requirements of standards organizations, such as the CA/Browser Forum. Some applications, such as browsers, may include more than 100 trusted CA certificates. To reduce their exposure to CA compromise incidents, organizations should minimize the CAs that their clients trust to only those they are likely to need to trust. For example, if certain systems acting as TLS clients are used only for internal operations, then they should trust only the certificate(s) from the internal CA(s). Furthermore, if certain TLS clients communicate with TLS servers from select partners, then certificates from only the CAs expected to be used by those partners should be trusted. Organizations should maintain an inventory of CA certificates trusted on all their systems, ensure only needed CAs are trusted, and maintain the ability to rapidly remove or replace CA certificates that should no longer be trusted.

Recommended Requirement:

- CA certificates trusted by TLS clients should be limited to only those required to validate TLS certificates of the servers with which the client communicates. All unneeded CA certificates should be removed. The following CAs should never be trusted:
  - <e.g., DigiNotar>
  - <…>

Recommended Responsibilities:

- Certificate Services team: provide the technology and services for discovering and creating inventories of existing CA certificates and for managing (e.g., adding, removing) CA certificates
- Certificate owners: limit CA trust to the minimum needed for each system and ensure all other CAs are removed

5.2 Establish a Certificate Service

Manually managing TLS server certificates is infeasible due to the large number of certificates in most enterprises. It is also not feasible for each certificate owner to create their own certificate management system. The most efficient and effective approach is for the Certificate Services team to provide a central Certificate Service that includes technology-based solutions that provide automation and that support certificate owners in effectively managing their certificates. This service should include the technology/services for CAs, certificate discovery, inventory management, reporting, monitoring, enrollment, installation, renewal, revocation, and other certificate management operations.

The central Certificate Service should also provide self-service access for certificate owners so they are able to configure and operate the services for their areas without requiring significant interaction with the Certificate Services team. Furthermore, the central Certificate Service should be able to integrate with other enterprise systems, including identity and access management systems, ticketing systems, configuration management databases, email, workflow, and logging and auditing.

5.2.1 CAs

Approved CAs should be designated and made available to certificate owners for requesting public and internal certificates. If, as is common, different CAs will be used for issuing public and internal certificates, then instructions should be provided to certificate owners to help them select the correct CA based on the purpose of the server where the certificate will be used. Establish backup CAs for both public and internal certificates, including completing contracts with backup public CAs so an immediate cutover is possible in case of a CA compromise, for business reasons, or because of some other motivation.

5.2.2 Inventory

An up-to-date inventory of deployed TLS server certificates is the foundation of an effective certificate management program. The functionality required by an inventory system generally makes it infeasible for certificate owners to operate and manage their own inventory systems. It is imperative that the Certificate Services team provides a central system that certificate owners can use to maintain an inventory of their certificates. Without a central, up-to-date inventory, the Certificate Services team has no way of proactively monitoring for certificate-related security and operational risks or supporting certificate owners in minimizing such risks.

The central inventory system should provide the following characteristics and functions:

- **Automatic parsing**: certificates contain multiple fields of information (e.g., subject, issuer, expiration date) that should be monitored. The inventory system should provide automatic parsing of the contents of certificates that are loaded into it so searches can be performed on individual fields
- **Additional metadata**: It should be possible to associate additional information/metadata with each certificate (e.g., identifiers of the owners and approvers; installed locations; application identifiers; cost center numbers)
- **Organization**: With hundreds or thousands of certificates spread across many certificate owners and geographic locations, the inventory system should support organizing certificates into distinct groups/folders
- **Access controls**: To prevent unauthorized actions, it should be possible to define and enforce access controls that are assigned to groups or individuals

- **Support certificate management**: As the foundation of a certificate management program, the inventory system should integrate with and support all other certificate management functions (e.g., discovery, enrollment portal, approvals, automation)

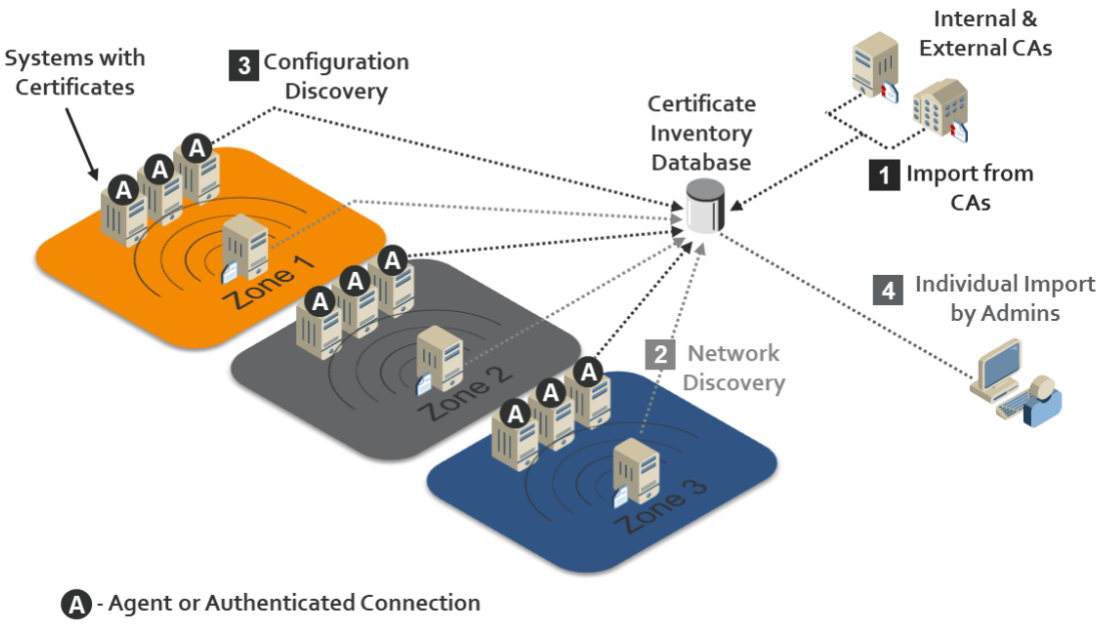
5.2.3 Discovery and Import

Manually establishing and maintaining an up-to-date and comprehensive inventory is difficult, if not impossible. Because of the complexity of most enterprise environments — which contain firewalls, different security/operations restrictions, etc. — it is often not sufficient to have a single method of automatically populating and maintaining an inventory. The central Certificate Service should provide multiple options for automated discovery and the import of certificates, including those listed below:

- **CA import**: automated import of certificates from CAs. This is often the fastest way to initially populate the certificate inventory. However, it will only provide an inventory of certificates from known CAs
- **Network discovery**: automated scanning of one or more configurable sets of IP addresses, IP address ranges, and ports for TLS server certificates. This helps provide a comprehensive view of all certificates and their locations. Organizations typically find certificates from unapproved CAs and self-signed certificates (which should likely be replaced with certificates from approved CAs). The network discovery service should support operation across multiple network zones separated by firewalls
- **Configuration discovery**: Network discovery can find certificates and determine their network location(s); however, it does not allow for collection of configuration information, such as the type of keystore (e.g., Privacy Enhanced Mail, Public Key Cryptography Standards [PKCS] #12, HSM), the storage location on the server, and other information that can be helpful in detecting issues and in setting up automated management for the certificate. The inventory system should provide a means of discovering certificate configuration information via an authenticated connection or agent
- **Bulk import**: In addition to network discovery and CA import, it is beneficial to have the option for administrators to import certificate data. This helps in cases where network discovery and CA import are not possible and in cases where there is additional information/metadata (e.g., contacts, approvers, cost centers) that can be associated with each certificate to help in tracking and management.

Figure 5-1 depicts options for automated discovery and import of certificates.

1220 **Figure 5-1 Various Options for Automated Discovery and the Import of Certificates**



1221

1222 ## 5.2.4 Management Interfaces

1223 Certificate owners and the Certificate Services team should provide user interfaces to view and manage
1224 certificates. The interfaces should be simple enough to support certificate owners who have small
1225 numbers of certificates and perform management operations infrequently. The interfaces should also
1226 offer more-sophisticated functionality to support the needs of certificate owners with large numbers of
1227 certificates and the needs of the Certificate Services team.

1228 The interfaces should provide the following characteristics and functions:

1229 1230 - **Inventory view**: Certificate owners should be able to view their certificates (to which they have been granted access). The Certificate Services team should be able to view the entire inventory
1231 1232 1233 - **Searching and filtering**: Certificate owners with large numbers of certificates, and the Certificate Services team, should be able to search and filter operations so they can quickly find specific certificates
1234 1235 1236 - **Enrollment and renewal**: The portal should provide a simple method to request new certificates and to renew existing certificates. Having a single interface for enrollment and renewal across all CAs reduces the retraining needed when moving CAs, resulting in better crypto-agility
1237 1238 1239 - **Approvals**: If an external system is not used for reviewing certificate requests, then the portal should provide a method for an approver to perform RA functions to review the relevant details of certificate requests and to approve/reject the requests with comments

5.2.5 Automated Enrollment and Installation

Manually requesting, installing, and managing large numbers of certificates is error-prone and resource-intensive; increases security risk; and does not allow for a rapid response to large-scale incidents, such as CA compromises. In cloud environments, the ability to quickly spin up new instances to support increased loads is critical. Because most enterprises have a range of systems from different vendors with diverse management methods, the central Certificate Service should offer multiple options for automation, including those listed below:

- **Programmatic automation**: The central Certificate Service should provide a set of application programming interfaces (APIs) (e.g., Representational State Transfer) that enable enrollment, revocation, reporting, etc. The central Certificate Service should support easy integration with and access from DevOps frameworks and other programming tools
- **Standard protocol support**: The central Certificate Service should support standard protocols for requesting certificates, including the Simple Certificate Enrollment Protocol (SCEP), Automated Certificate Management Environment, and Enrollment over Secure Transport
- **Proprietary automation**: Some systems may not support programmatic or standards-based enrollment and installation but may provide other methods (e.g., APIs, command-line utilities) that can be used to automate certificate enrollment and installation. This may be performed with an agent or via a remote authenticated connection
- **Secure key transport**: Within organizations that, by policy, permit TLS traffic monitoring and enable detection of encrypted threats by using passive decryption devices, the central Certificate Service should provide the ability to securely transport TLS private keys from TLS servers to the decryption devices that enable inspection of encryption communications

Automation should support integration with HSMs when HSMs are used for protection of private keys.

5.2.6 RA/Approvals

Certificate requests should be reviewed and vetted to ensure unauthorized certificates are not issued or used for malicious purposes. Large enterprises generally have hundreds of different departments, business applications, projects, and systems administrators, making it infeasible for a central group to have the relevant knowledge needed to vet requests. The central Certificate Service should provide the ability to assign individuals (e.g., application owners) to review certificate requests for their respective areas. Once approvers are assigned, the central Certificate Service should automatically route certificate requests to assigned reviewers for approval and enable them to review any relevant data needed to properly vet requests.

5.2.7 Reporting and Analytics

To address TLS server certificate-related risks, certificate owners and the Certificate Services team should have visibility across their inventory and be able to quickly identify TLS server certificate issues or vulnerabilities. The most efficient method of addressing risks is proactive notifications sent by the central Certificate Service, based on configured rules. However, reports and dashboards can help in planning (e.g., an unexpectedly large number of certificate expirations coming in the next few weeks) and identifying anomalies that would otherwise not be caught by the automated rules. The central Certificate Service should support the following reporting and analysis tools:

- **Custom reporting**: Users should be able to create customized reports, including the data to be presented, the filtering criteria for the results, the scheduling of execution, and the selection of report recipients
- **Dashboards**: To help in identifying anomalies or unexpected issues, dashboards should proactively highlight risks, such as certificates with weak keys, vulnerable algorithms, impending expirations, operational errors, and other issues
- **Interfaces to monitoring systems**: Many organizations rely upon automated security incident and event monitoring systems that collect, analyze, and correlate information that is subsequently displayed or used to notify humans of events and the actions required. Certificate-related anomalies and issues should be delivered to such systems

5.2.8 Passive Decryption Support

If passive decryption devices are used to monitor TLS-encrypted communications for attacks, then those devices must have copies of the private keys from all monitored TLS servers so the devices are able to decrypt TLS traffic to those servers. Manually transporting private keys from TLS servers to passive decryption devices creates risk of a compromise. Consequently, when passive decryption is used, the central Certificate Service should provide an automated and secure method for transporting private keys from TLS servers to passive decryption devices and for keeping the private keys up-to-date when new keys (and certificates) are deployed.

5.2.9 Continuous Monitoring

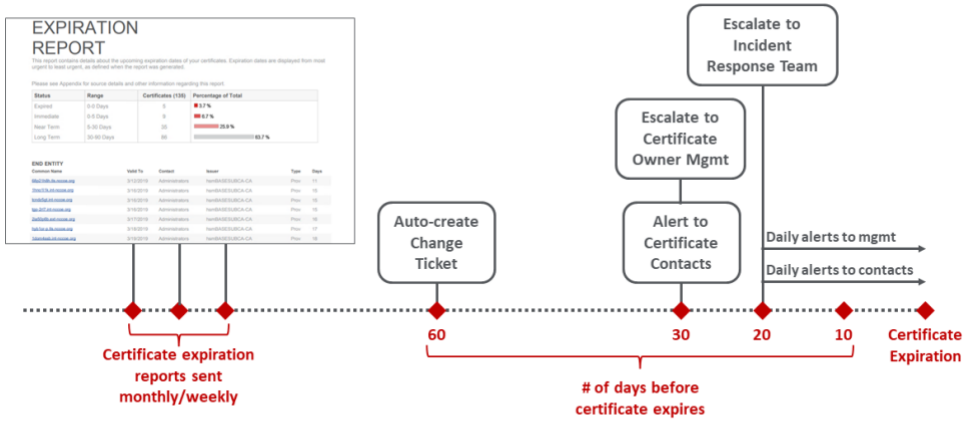
To prevent operational or security incidents, the certificates should be continuously monitored across the enterprise. Continuous monitoring should include the following types of monitoring:

- **Expiration monitoring**: To prevent outages due to expired certificates, the expiration dates for all certificates should be monitored. It should be possible to configure the time periods when notifications will be sent to certificate contacts prior to expiration (e.g., 90 days, 60 days, 30 days). If timely action is not taken, then it should be possible to escalate and send notifications to managers or a central incident response team

- **Operation/configuration monitoring**: Once a known good state is established (e.g., the location and configuration of certificates), the central Certificate Service should monitor and detect situations in which certificates are not operating, are not configured properly, or are vulnerable
- **Policy compliance**: The central Certificate Service should detect and send alerts when deployed certificates are not consistent with policy

Because certificate expirations are a regular occurrence, especially for certificate owners with large numbers of certificates, it is important to not inundate certificate owners with notifications, as they will likely start to ignore them. An effective strategy is to combine the use of reports, change tickets, and alerts. Sending regular (e.g., monthly) reports containing a list of certificates expiring within a certain number of days (e.g., 120 days) helps certificate owners plan for expirations. Automatically creating change tickets in the organization's central ticketing system can ensure certificate renewals and replacements are handled in the same way that other change operations are performed. Sending alerts within 30 days of expiration and escalating to management and incident response teams ensures certificates not replaced in a timely fashion are identified before they expire. Figure 5-2 provides an example schedule for reports, tickets, and alerts.

Figure 5-2 Example Timeline of Processes and Notifications Triggered by Impending Certificate Expiration



5.2.10 Education

Management of TLS server certificates in an enterprise environment is complex, time-consuming, error-prone, and security-sensitive. Most certificate owners are not knowledgeable about TLS server certificates, the processes for effectively managing certificates, or their own certificate-related

responsibilities. Consequently, the Certificate Services team should provide readily accessible educational materials, preferably online and available on demand. The TLS server certificate educational materials should include the following items:

- basic introduction to certificates and keys (e.g., when certificates are used, obtaining certificates, protecting keys, certificate changes, revocation)
- risks of improper TLS server certificate management
- explanation of TLS server certificate policies and certificate owner responsibilities
- step-by-step instructions for managing TLS server certificates, including any of the following steps offered via the central Certificate Service:
  - creating an inventory
  - reviewing the inventory and identifying risks/vulnerabilities (e.g., generating reports)
  - manually requesting and installing TLS server certificates on each relevant operating system/application (e.g., Apache)
  - DevOps/API-based request and installation
  - agentless automated installation
  - agent-based automated installation
  - renewing certificates
  - revoking certificates

There are many educational resources available on the internet that can alleviate the need to create new materials. An internal TLS server certificate education website can include links to helpful web pages and websites.

5.2.11 Help Desk

In addition to educational materials, certificate owners should have a central support service that they can contact about questions and that can assist in troubleshooting issues. Many certificate owners may be new to TLS server certificate management or responsible for only a small number of certificates (e.g., one to five certificates) and will likely need assistance in successfully performing necessary operations. Any certificate owner calling the help desk should be required to have completed the educational programs that apply to their use cases so that help-desk personnel do not need to explain basic concepts that can be learned prior to the request for help.

TLS server certificates are typically installed or renewed during scheduled maintenance windows, which are often scheduled on weekends and/or in the middle of the night. Issues related to TLS server

certificates can often arise during these scheduled maintenance operations; therefore, help-desk personnel should be made available during all times when certificate issues may arise (e.g., 24 hours a day, seven days a week). Help-desk personnel should be knowledgeable about and experienced in TLS server certificate management. It is possible to have general help-desk personnel answer and address Level One certificate calls and escalate to more-experienced personnel as needed for Level Two and Level Three calls.

5.3 Terms of Service

It is helpful to define the terms of service for the central Certificate Service to avoid confusion by certificate owners about the services they will receive and their responsibilities. The terms of service should include those listed below:

- description of the services provided (e.g., network discovery, monitoring enrollment, automation)
- responsibilities of the certificate owners and the Certificate Services team (e.g., the Certificate Services team will help with network discovery, but a certificate owner is responsible for working with the network team to allow the discovery on their systems)
- expected service levels — stated in service level agreements — with response times

5.4 Auditing

Due to the fundamental role that TLS server certificates play in securing data and systems, periodic reviews of TLS server certificate management practices are essential. Auditors should confirm that TLS server certificate policy requirements are addressed. For example, all certificate owners should be able to demonstrate they have a certificate inventory and to describe the steps they have taken to ensure all certificates are included in the inventory. The Certificate Services team should demonstrate it is providing the services needed for certificate owners to comply with policy.

TLS server certificate risks can lie latent for long periods of time and then can unexpectedly have significant impact to an organization's operations —due to either operational outages or security issues. Consequently, regular audits of certificate management practices performed by compliance auditors are critical to prevent unanticipated issues.

6 Implementing a Successful Program

The broad distribution of TLS server certificates across distinct groups, networks, and systems can present unique challenges in implementing an effective certificate management program across an enterprise environment. The following resources are helpful for successful implementation:

- **Executive owner**: It is essential to have an executive owner for the certificate management program. This executive owner should be prepared to educate the executives of each group of certificate owners on TLS server certificate risks and the executives' responsibilities
- **Prioritization of risks**: Each organization has different challenges and priorities related to TLS server certificates. Although the best practices detailed in this practice guide are intended to help address all the risks related to TLS server certificates, it is helpful to prioritize those risks based on historical certificate issues and business needs. This prioritization can help in communications with certificate owners and with setting objectives and prioritizing tasks
- **Objectives**: Establishing clear and achievable objectives provides targets, helps focus efforts, and improves the likelihood of successful implementation. For example, if an organization finds it does not have an inventory and recognizes there are two groups that may be difficult to inventory in the near term, then one objective may be to create an inventory of all other groups' TLS server certificates in the next 12 months
- **Action plan**: An action plan with specific tasks, responsibilities, and milestones, geared to achieve the objectives, should be created, communicated, and reviewed by all stakeholders (e.g., certificate owners, Certificate Services team, executive owner). The action plan should be prioritized to address the most important objectives first. For example, an action plan might include the following objectives:
  - 30 days from the start of the project:
    - complete certificate imports from CA1, CA2, and CA3
    - require certificate enrollment through the central Certificate Service portal and prevent enrollment directly to CAs
  - 90 days from the start of the project:
    - complete network discovery across all North American and European data centers
    - complete the assignment of certificate owners for all certificates in inventory
  - 180 days from the start of the project:
    - automate certificate enrollment and installation on all load balancers
    - automate certificate enrollment and installation for all e-commerce web servers
    - complete network discovery across all Asia-Pacific data centers
- **Regular executive reviews**: The objectives and action plan should be reviewed with the executive owner at commencement of the project, and regular reviews should be scheduled (e.g., every 90 days) to track progress. During these reviews, the executive owner should note areas where additional action by certificate owners is needed so the executive owner can proactively communicate with peer executives to ensure action is taken

- **Periodic audits**: Due to the critical role that TLS server certificates play in the security and operations of organizations, and the risks resulting from improper management, regular audits should confirm the Certificate Services team and certificate owners are fulfilling their responsibilities in TLS server certificate management.

Security testing should be defined as part of the organization's policies. Before going live with any recommendations in this document, authorization from the security team should be provided, as specified by security policy.

Appendix A List of Acronyms and Abbreviations

ACME	Automated Certificate Management Environment
AD	Active Directory
API	Application Programming Interface
BGP	Border Gateway Protocol
CA	Certificate Authority
CAA	Certificate Authority Authorization
CAS	Certification Authority System
CAPI	Cryptographic Application Programming Interface (also known variously as CryptoAPI, Microsoft Cryptography API, MS-CAPI or simply CAPI)
CIO	Chief information officer
CN	Common Name
CRL	Certificate Revocation List
CSF	Cybersecurity Framework
CSR	Certificate Signing Request
CT	Certificate Transparency
DevOps	Development Operations
DN	Distinguished Name
DNS	Domain Name System
ECDSA	Elliptic Curve Digital Signature Algorithm
EV	Extended Validation
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

IETF	Internet Engineering Task Force
IIS	Internet Information Server (Microsoft Windows)
IoT	Internet of Things
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
NCCoE	National Cybersecurity Center of Excellence
OS	Operating System
OV	Organization Validated
PCI-DSS	Payment Card Industry Data Security Standard
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RA	Registration Authority
REST	Representational State Transfer (API)
RMF	Risk Management Framework
RSA	Rivest, Shamir, & Adleman (public key encryption algorithm)
SAN	Subject Alternative Name
SCEP	Simple Certificate Enrollment Protocol
SHA-1	Secure Hash Algorithm 1
SHA-256	Secure Hash Algorithm 256
SP	Special Publication
SSL	Secure Socket Layer (protocol)
SSLV	SSL Visibility (Symantec Appliance)
TLS	Transport Layer Security (protocol)
TPP	Trust Protection Platform (Venafi)

UPN	User Principal Name
URL	Uniform Resource Locator

Appendix B Glossary

Active Directory	A Microsoft directory service for the management of identities in Windows domain networks.
Application	1. The system, functional area, or problem to which information technology is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and management information systems are examples of applications. (NIST SP 800-16) 2. A software program hosted by an information system. (NIST SP 800-137)
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources. (NIST SP 800-63-3)
Automated Certificate Management Environment	A protocol defined in IETF RFC 8555 that provides for the automated enrollment of certificates.
Certificate	A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its validity period. (NIST SP 800-57 Part 1 Rev. 4 under Public-key certificate) (Certificates in this practice guide are based on IETF RFC 5280.)
Certificate Authority	A trusted entity that issues and revokes public key certificates. (NISTIR 8149)
Certificate Authority Authorization	A record associated with a Domain Name Server (DNS) entry that specifies the CAs that are authorized to issue certificates for that domain.
Certificate Chain	An ordered list of certificates that starts with an end-entity certificate, includes one or more certificate authority (CA) certificates, and ends with the end-entity certificate's root CA certificate, where each certificate in the chain is the certificate of the CA that issued the previous certificate. By checking to see if

	each certificate in the chain was issued by a trusted CA, the receiver of an end-user certificate can determine whether or not it should trust the end-entity certificate by verifying the signatures in the chain of certificates.
Certificate Management	Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed. (CNSSI 4009-2015) (In the context of this practice guide, it also includes inventory, monitoring, enrolling, installing, and revoking.)
Certificate Revocation List	A list of digital certificates that have been revoked by an issuing CA before their scheduled expiration date and should no longer be trusted.
Certificate Signing Request	A request sent from a certificate requester to a certificate authority to apply for a digital identity certificate. The certificate signing request contains the public key as well as other information to be included in the certificate and is signed by the private key corresponding to the public key.
Certificate Transparency	A framework for publicly logging the existence of Transport Layer Security (TLS) certificates as they are issued or observed in a manner that allows anyone to audit CA activity and notice the issuance of suspect certificates as well as to audit the certificate logs themselves. (Experimental RFC 6962)
Chief information officer	Organization's official responsible for: (i) Providing advice and other assistance to the head of the organization and other senior management personnel of the organization to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, directives, policies, regulations, and priorities established by the head of the organization; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the [organization]; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the organization, including improvements to work processes of the organization. (NIST SP 800-53 Rev. 4 adapted) Note: A subordinate organization may assign a chief information officer to denote an individual filling a position with security

	responsibilities with respect to the subordinate organization that are similar to those that the chief information officers fills for the organization to which they are subordinate.
Client	1. A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a consumer. (NIST SP 800-146) 2. A function that uses the PKI to obtain certificates and validate certificates and signatures. Client functions are present in CAs and end entities. Client functions may also be present in entities that are not certificate holders. That is, a system or user that verifies signatures and validation paths is a client, even if it does not hold a certificate itself. (NIST SP 800-15)
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST SP 800-145)
Common Name	An attribute type that is commonly found within a Subject Distinguished Name in an X.500 directory information tree. When identifying machines, it is composed of a fully qualified domain name or IP address.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. (NIST SP 800-53 Rev. 4)
Container	A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container. (NIST SP 800-190)
Cryptographic Application Programming Interface	An application programming interface included with Microsoft Windows operating systems that provides services to enable developers to secure Windows-based applications using cryptography. While providing a consistent API for applications,

	CAPI allows for specialized cryptographic modules (cryptographic service providers) to be provided by third parties, such as hardware security module (HSM) manufacturers. This enables applications to leverage the additional security of HSMs while using the same APIs they use to access built-in Windows cryptographic service providers. (Also known variously as CryptoAPI, Microsoft Cryptography API, MS-CAPI or simply CAPI)
Cryptography API: Next Generation	The long-term replacement for the Cryptographic Application Programming Interface (CAPI).
Demilitarized Zone	A perimeter network or screened subnet separating an internal network that is more trusted from an external network that is less trusted.
Development Operations (DevOps)	A set of practices for automating the processes between software development and information technology operations teams so that they can build, test, and release software faster and more reliably. The goal is to shorten the systems development life cycle and improve reliability while delivering features, fixes, and updates frequently in close alignment with business objectives.
Digital Certificate	Certificate (as defined above).
Digital Signature	The result of a cryptographic transformation of data that, when properly implemented, provides origin authentication, assurance of data integrity, and signatory non-repudiation. (NIST SP 800-133)
Digital Signature Algorithm	A Federal Information Processing Standard for digital signatures, based on the mathematical concept of modular exponentiations and the discrete logarithm problem. (FIPS 186-4)
Directory Service	A distributed database service capable of storing information, such as certificates and CRLs, in various nodes or servers distributed across a network. (NIST SP 800-15) (In the context of this practice guide, a directory services stores identity information and enables the authentication and identification of people and machines.)
Distinguished Name	An identifier that uniquely represents an object in the X.500 directory information tree. (RFC 4949 Ver 2)
Domain	A distinct group of computers under a central administration or authority.

Domain Name	A label that identifies a network domain using the Domain Naming System.
Domain Name Server	The internet's equivalent of a phone book. It maintains a directory of domain names, as defined by the Domain Name System, and translates them to Internet Protocol addresses.
Domain Name System	The system by which Internet domain names and addresses are tracked and regulated as defined by IETF RFC 1034 and other related RFCs.
Elliptic Curve Digital Signature Algorithm	A digital signature algorithm that is an analog of DSA using elliptic curve mathematics and specified in ANSI draft standard X9.62. (NIST SP 800-15)
Enrollment	The process that a CA uses to create a certificate for a web server or email user. (NISTIR 7682) (In the context of this practice guide, enrollment applies to the process of a certificate requester requesting a certificate, the CA issuing the certificate, and the requester retrieving the issued certificate.)
Extended Validation Certificate	A certificate used for HTTPS websites and software that includes identity information that has been subjected to an identity verification process standardized by the CA Browser Forum in its Baseline Requirements that verifies that the identified owner of the website for which the certificate has been issued has exclusive rights to use the domain; exists legally, operationally, and physically; and has authorized the issuance of the certificate.
Federal Information Processing Standards (FIPS)	A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability. (NIST SP 800-161)
Hardware Security Module (HSM)	A physical computing device that provides tamper-evident and intrusion-resistant safeguarding and management of digital keys and other secrets, as well as crypto-processing. FIPS 140-2 specifies requirements for HSMs.

Hostname	Hostnames are most commonly defined and used in the context of DNS. The hostname of a system typically refers to the fully qualified DNS domain name of that system.
Hypertext Transfer Protocol	A standard method for communication between clients and Web servers. (NISTIR 7387)
Internet Engineering Task Force (IETF)	The internet standards organization made up of network designers, operators, vendors, and researchers that defines protocol standards (e.g., IP, TCP, DNS) through process of collaboration and consensus.
Internet Message Access Protocol	A method of communication used to read electronic mail stored in a remote server. (NISTIR 7387)
Internet of Things (IoT)	As used in this publication, user or industrial devices that are connected to the internet. IoT devices include sensors, controllers, and household appliances.
Internet Protocol	The Internet Protocol, as defined in IETF RFC 6864, which is the principal communications protocol in the IETF Internet protocol suite for specifying system address information when relaying datagrams across network boundaries.
Lightweight Directory Access Protocol (LDAP)	The Lightweight Directory Access Protocol, or LDAP, is a directory access protocol. In this document, LDAP refers to the protocol defined by RFC 1777, which is also known as LDAP V2. LDAP V2 describes unauthenticated retrieval mechanisms. (NIST SP 800-15)
Microservice	A set of containers that work together to compose an application. (NIST SP 800-190)
Organization	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements). (NIST SP 800-39) This publication is intended to provide recommendations for organizations that manage their own networks (e.g., that have a chief information officer).
Outage	A period when a service or an application is not available or when equipment is not operational.

Payment Card Industry Data Security Standard	An information security standard administered by the Payment Card Industry Security Standards Council that is for organizations that handle branded credit cards from the major card schemes.
Pivoting	A process where an attacker uses one compromised system to move to another system within an organization.
PIN Entry Device	An electronic device used in a debit, credit, or smart card-based transaction to accept and encrypt the cardholder's personal identification number.
Post Office Protocol (POP)	A mailbox access protocol defined by IETF RFC 1939. POP is one of the most commonly used mailbox access protocols. (NIST SP 800-45 Version 2).
Private Key	The secret part of an asymmetric key pair that is used to digitally sign or decrypt data. (NIST SP 800-63-3).
Public CA	A trusted third party that issues certificates as defined in IETF RFC 5280. A CA is considered public if its root certificate is included in browsers and other applications by the developers of those browsers and applications. The CA/Browser Forum defines the requirements public CAs must follow in their operations.
Public Key	The public part of an asymmetric key pair that is used to verify signatures or encrypt data. (NIST SP 800-63-3).
Public Key Cryptography	Cryptography that uses separate keys for encryption and decryption; also known as asymmetric cryptography. (NIST SP 800-77)
Public Key Infrastructure (PKI)	The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. (NIST SP 800-53 Rev. 4)
Registration Authority (RA)	An entity authorized by the certification authority system (CAS) to collect, verify, and submit information provided by potential subscribers, which is to be entered into public key certificates. The

	term RA refers to hardware, software, and individuals that collectively perform this function. (CNSSI 4009-2015)
Re-key	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key. NIST SP 800-32 under Re-key (a certificate)
Renew	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate. NIST SP 800-32 (The new certificate is typically used to replace the existing certificate, and both certificates typically contain the same Subject DN and SAN information. It is best practice to generate a new key pair and CSR, i.e., re-key, when renewing a certificate, but re-keying is not required by all certificate authorities. Renewal is typically driven by the expiration of the existing certificate but could also be triggered by a suspected private key compromise or other event requiring the existing certificate to be revoked.)
Replace	The process of installing a new certificate and removing an existing one so that the new certificate is used in place of the existing certificate on all systems where the existing certificate is being used.
Representational State Transfer	A software architectural style that defines a common method for defining APIs for Web services.
Risk Management Framework	The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.
Rivest, Shamir, & Adleman	An algorithm approved in [FIPS 186] for digital signatures and in [SP 800-56B] for key establishment. (NIST SP 800-57 Part 1 Rev. 4)
Root certificate	A self-signed certificate, as defined by IETF RFC 5280, issued by a root CA. A root certificate is typically securely installed on systems so they can verify end-entity certificates they receive.
Root certificate authority	In a hierarchical public key infrastructure (PKI), the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain. (NIST SP 800-32)

Rotate	The process of renewing a certificate in conjunction with a rekey, followed by the process of replacing the existing certificate with the new certificate.
Subject Alternative Name	A field in an X.509 certificate that identifies one or more fully qualified domain names, IP addresses, email addresses, URIs, or UPNs to be associated with the public key contained in a certificate.
Simple Certificate Enrollment Protocol	A protocol defined in an IETF internet draft specification that is used by numerous manufacturers of network equipment and software who are developing simplified means of handling certificates for large-scale implementation to everyday users, as well as referenced in other industry standards.
Secure Hash Algorithm 1	A hash function specified in FIPS 180-2, the Secure Hash Standard. (NIST SP 800-89)
Secure Hash Algorithm 256	A hash algorithm that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated. (FIPS 180-4 (March 2012))
Secure Transport	Transfer of information using a transport layer protocol that provides security between applications communicating over an IP network.
Server	A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries). (NIST SP 800-47)
Service Provider	A provider of basic services or value-added services for operation of a network; generally refers to public carriers and other commercial enterprises. (NISTIR 4734)
Simple Mail Transfer Protocol	The primary protocol used to transfer electronic mail messages on the internet. (NISTIR 7387)
Special Publication	A type of publication issued by NIST. Specifically, the Special Publication 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer

	security, and its collaborative activities with industry, government, and academic organizations. The 1800 series reports the results of NCCoE demonstration projects.
System Administrator	Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. (CNSSI 4009-2015)
Team	A number of persons associated together in work or activity. (Merriam Webster) As used in this publication, a team is a group of individuals that has been assigned by an organization's management the responsibility and capability to carry out a defined function or set of defined functions. Designations for teams as used in this publication are simply descriptive. Different organizations may have different designations for teams that carry out the functions described herein.
Transport Layer Security (TLS)	An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by RFC 5246 and RFC 8446.
Trust Protection Platform	The Venafi Machine Identity Protection platform used in the example implementation described in this practice guide.
User Principal Name	In Windows Active Directory, this is the name of a system user in email address format, i.e., a concatenation of username, the "@" symbol, and domain name.
Validation	The process of determining that an object or process is acceptable according to a pre-defined set of tests and the results of those tests. (NIST SP 800-152)
Web Browser	A software program that allows a user to locate, access, and display *web* pages.

Appendix C Mapping to the Cybersecurity Framework

The following table maps the recommended best practices for TLS server certificate management to the NIST Cybersecurity Framework.

Table 1 Mapping the Recommended Best Practices for TLS Server Certificate Management to the Cybersecurity Framework

CSF Function	CSF Subcategory	Applicability to TLS Server Certificates
Identify	**ID.AM-2**: Software platforms and applications within the organization are inventoried	An inventory of TLS server certificates is established and maintained—including certificate attributes and metadata, such as the certificate owner for each certificate.
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	The responsibilities for complying with TLS Server Certificate policies and maintaining operational integrity and security related to TLS server certificates are clearly defined for certificate owners, the Certificate Services Team, and other relevant stakeholders. (See NIST SP 1800-16b: Security Risks and Recommended Best Practices, Section 5.1)
	ID.GV-1: Organizational cybersecurity policy is established and communicated	TLS server certificate policies are established, communicated to all stakeholders, enforced, and audited. (See NIST SP 1800-16b: Security Risks and Recommended Best Practices, Section 5)
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with	certificate owners, the Certificate Services Team, and any other applicable stakeholders are educated on

	internal roles and external partners	and have agreed to their roles and responsibilities for ensuring TLS server certificate policy compliance and maintaining operational integrity and security related to TLS server certificates. (See NIST SP 1800-16b: Security Risks and Recommended Best Practices)
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	The impact of applicable legal and regulatory requirements on TLS server certificate policies and processes is reviewed. Necessary adjustments to policies and processes are completed and communicated. (See NIST SP 1800-16b: Security Risks and Recommended Best Practices)
	ID.GV-4: Governance and risk management processes address cybersecurity risks	The effectiveness of implementing and complying with TLS server certificate policies to address operational and security risks is regularly reviewed by management and auditors. Adjustments are made to policies and processes when deficiencies are identified. (See NIST SP 1800-16b: Security Risks and Recommended Best Practices)
Protect	**PR.AC-1**: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	The following are performed for TLS server certificates, which serve as machine identities: Certificates are issued by organizationally-approved certificate authorities Certificate requests are reviewed by knowledgeable persons or via approved automated processes

		An inventory of certificates is maintained Certificate owner information is kept up to date Certificate expiration dates are tracked and new certificates requested/installed prior to expiration Access to TLS private keys is limited to authorized personnel and keys are replaced when personnel with access are reassigned or terminated Certificate operation and configuration is continuously monitored All certificate/key management operations are logged Private keys are securely transferred to TLS inspection devices Certificates are revoked when a private key is suspected to have been compromised or another event occurs that may invalidate the trustworthiness of a certificate Certificate Authority Authorization (CAA) records are populated for public-facing TLS server certificates Certificate Transparency (CT) logs are monitored for fraudulent certificates
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Access to private keys associated with TLS server certificates is limited to authorized personnel. Certificates are replaced when personnel with direct access to corresponding private keys are reassigned or terminated. Controls

		are implemented to ensure that access to certificates is only granted to personnel or systems authorized for the corresponding domains.
	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	TLS server certificate requests are reviewed by knowledgeable personnel or via approved automated processes.
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	All servers have TLS server certificates so they can be securely authenticated by clients.
	PR.DS-1: Data-at-rest is protected	Least privileged access is enforced for TLS server private keys or, where possible, hardware security modules are used to generate, store, and protect TLS server private keys.
	PR.DS-2: Data-in-transit is protected	All servers enforce the use of TLS for communications and the corresponding TLS certificates and private keys are properly managed and secure.
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Private keys associated with TLS server certificates are replaced when people who have had direct access to those keys are reassigned or terminated. Certificates are revoked when a private key is suspected to have been compromised or another event occurs that may invalidate the trustworthiness of a certificate. New certificates are requested/installed prior to expiration.

	PR.IP-2: A System Development Life Cycle to manage systems is implemented	TLS server certificate management processes effectively manage the life cycle of TLS certificates (e.g., inventory, request, replacement, revocation, etc.).
	PR.IP-3: Configuration change control processes are in place	Change control processes are defined and enforced for TLS server certificates, e.g., certificates are replaced during off-hours and are tested before going operational.
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	The system supports the replacement of large numbers of TLS server certificates and private keys in response to CA compromises, vulnerable algorithms, or cryptographic library bugs.
	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	All TLS server certificate and private key management/administrative operations can be logged to a central location and reviewed in accordance with policy.
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Support is provided for managing the copying and transfer of TLS certificates needed to support resilience mechanisms such as load balancing and hot swap.
	DE.AE-5: Incident alert thresholds are established	Clear thresholds are defined for: Notifications and escalations related to certificates nearing expiration (e.g., 60, 30, 15 days prior to expiration) The implementation of large-scale certificate replacement processes (e.g., suspected CA compromise triggers replacement)

	DE.CM-1: The network is monitored to detect potential cybersecurity events	TLS inspection mechanisms are implemented to monitor encrypted traffic within TLS-secured connections to ensure that malicious activity and pivoting between internal systems is detected.
Respond	**RS.AN-5**: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	In response to disclosed vulnerabilities such as public certificate authority compromise, cryptographic algorithm vulnerabilities, and cryptographic library bugs and vulnerabilities, the system supports the replacement of large numbers of TLS server certificates and private keys.
	RS.MI-2: Incidents are mitigated	All certificates affected by a certificate authority compromise, algorithm vulnerability, or cryptographic library bug can be rapidly replaced.

1438

Appendix D Special Publication 800-53 Controls Applicable to Best Practices for TLS Server Certificate Management

The following table provides an explanation of how specific controls defined within 800-53 should be applied to TLS server certificate management recommended best practices.

Table 2 Application of Specific Controls to TLS Server Certificate Management Recommended Best Practices

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
AC-1	ACCESS CONTROL POLICY AND PROCEDURES Control: a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. An access control policy that: i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.	An access control policy is defined for TLS private keys. Private keys associated with TLS server certificates must be protected from compromise. Most TLS private keys are stored in files. Access to these files must be limited to authorized personnel. If a person with access to a private key is reassigned or terminated, the private key and certificate should be changed.
AC-5	SEPARATION OF DUTIES Control: a. Separate [Assignment: organization-defined duties of individuals]; b. Document separation of duties of individuals; and c. Define system access authorizations to support	When a certificate is requested, another party (with knowledge of the application and requester) or automated process should review and approve the request prior to certificate issuance.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	separation of duties. Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion.	
AC-6	LEAST PRIVILEGE Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Access to private keys should only be assigned to appropriate personnel with a need-to-know. Automation should be used where possible to minimize the need for direct private key access by people.
AC-16	SECURITY AND PRIVACY ATTRIBUTES Control: a. Provide the means to associate [Assignment: organization-defined types of security and privacy attributes] having [Assignment: organization-defined security and privacy attribute values] with information in storage, in process, and/or in transmission; b. Ensure that the security and privacy attribute associations are made and retained with the information; c. Establish the permitted [Assignment: organization-defined security attributes] for [Assignment: organization-defined systems]; and	The TLS server certificate inventory should include metadata fields for all relevant security and privacy attributes for each certificate, including issuer, key length, signing algorithm, validity period, and owner.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	d. Determine the permitted [Assignment: organization-defined values or ranges] for each of the established security and privacy attributes.	
AT-2	AWARENESS TRAINING Control: Provide basic security and privacy awareness training to system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by system changes; and c. [Assignment: organization-defined frequency] thereafter.	All certificate owners should have sufficient training to understand the best practices/policies for TLS server certificate and private key management as well as their role and responsibilities.
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES Control: a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. An audit and accountability policy that: i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the	Develop, document, and disseminate policies and procedures for auditing TLS server certificate management.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	implementation of the audit and accountability policy and the associated audit and accountability controls; b. Designate an [Assignment: organization-defined senior management official] to manage the audit and accountability policy and procedures; c. Review and update the current audit and accountability: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency]; d. Ensure that the audit and accountability procedures implement the audit and accountability policy and controls; and e. Develop, document, and implement remediation actions for violations of the audit and accountability policy.	
AU-2	AUDIT EVENTS Control: Verify that the system can audit the following event types: [Assignment: organization-defined auditable event types].	Ensure that all TLS certificate and private key management operations are logged, including key generation, certificate enrollment, copying of keys, and certificate issuance/renewal/replacement/revocation.
AU-3	CONTENT OF AUDIT RECORDS Control: The system generates audit records containing	Ensure that logged TLS server certificate management events contain all relevant data

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	needed for audits, including date/time, operation performed, identifiers for the person or system performing the operation, identifiers for the asset (e.g., certificate/key) affected, and any other relevant information.
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING Control: Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity].	Implement regular manual and/or automated reviews to detect unauthorized TLS server certificate and private key operations.
AU-12	AUDIT GENERATION Control: a. Provide audit record generation capability for the auditable event types in AU-2 a. at [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select which auditable event types are to be audited by specific components of the system; and c. Generate audit records for the event types defined in AU-2 d. with the content in AU-3.	Ensure that 1) all components involved in TLS server certificate and private key management generate audit records and that the appropriate information and audit records are collected to a central log.
AU-13	MONITORING FOR INFORMATION DISCLOSURE Control: Monitor [Assignment:	Monitor the internet for rogue installations of TLS certificates

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	organization-defined open source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information.	(which can indicate private key compromise).
CA-1	ASSESSMENT, AUTHORIZATION, AND MONITORING POLICY AND PROCEDURES Control: a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. A security and privacy assessment, authorization, and monitoring policy that: i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the security and privacy assessment, authorization, and monitoring policy and the associated security and privacy assessment, authorization, and monitoring controls; b. Designate an [Assignment: organization-defined senior	Establish clear policies and responsibilities for TLS server certificate management. Ensure that all certificate owners and the certificate services team are educated and understand their responsibilities.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	management official] to manage the security and privacy assessment, authorization, and monitoring policy and procedures; c. Review and update the current security and privacy assessment, authorization, and monitoring: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency]; d. Ensure that the security and privacy assessment, authorization, and monitoring procedures implement the security and privacy assessment, authorization, and monitoring policy and controls; and e. Develop, document, and implement remediation actions for violations of security and privacy assessment, authorization, and monitoring policy.	
CA-2	ASSESSMENTS Control: a. Develop a security and privacy assessment plan that describes the scope of the assessment including: 1. Security and privacy controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment,	Develop a security assessment plan to verify that TLS server certificate policies are followed. Ensure that an executive with sufficient authority is assigned to review and assess the current policy compliance status and posture of the TLS server certificate management program (e.g., do all groups have an up-to-date inventory, is ownership information kept up

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	assessment team, and assessment roles and responsibilities.	to date, are private keys secured, is automation used wherever possible, etc.).
CA-5	PLAN OF ACTION AND MILESTONES Control: a. Develop a plan of action and milestones for the system to document the planned remedial actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, impact analyses, and continuous monitoring activities.	Establish a remediation plan to address deficiencies. Ensure executive oversight. Regularly review progress on the achievement of milestones and provide executive support where needed to ensure sufficient resources to meet milestones.
CA-7	CONTINUOUS MONITORING Control: Develop a security and privacy continuous monitoring strategy and implement security and privacy continuous monitoring programs that include: a. Establishing the following security and privacy metrics to be monitored: [Assignment: organization-defined metrics]; b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for ongoing assessment of security	Implement continuous monitoring for all TLS server certificates, including: • Regular automated network discovery scans to detect newly deployed certificates • Monitoring certificate expiration dates • Automated checking that all known certificates are correctly installed and operational • Tracking of CT records for fraudulent certificates.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	and privacy control effectiveness; c. Ongoing security and privacy control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security and privacy status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security- and privacy-related information generated by security and privacy control assessments and monitoring; f. Response actions to address results of the analysis of security- and privacy-related information; and g. Reporting the security and privacy status of the organization and organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	Ensure that encrypted TLS sessions can be monitored for malicious activity via proxy, endpoint agent, or passive decryption.
CM-2	BASELINE CONFIGURATION Control: a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system.	Perform automated network discovery scans to establish a comprehensive baseline of the TLS server certificate inventory. Review and update baseline configuration.
CM-3	CONFIGURATION CHANGE CONTROL Control:	Ensure that certificate replacement operations are included in change control

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	a. Determine the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time-period]; f. Monitor and review activities associated with configuration-controlled changes to the system.	plans. Ensure all certificate management operations are scheduled and reviewed. Retain logs of all certificate management operations.
CM-6	CONFIGURATION SETTINGS Control: Establish and document configuration settings for components employed within the system using [Assignment: organization-defined common secure configurations] that reflect the most restrictive mode consistent with operational requirements.	Establish and document the following for TLS server certificates: - Key lengths - Signing algorithms - Certificate authorities - Validity periods - Private key access control and protection
CM-8	SYSTEM COMPONENT INVENTORY Control: a. Develop and document an inventory of system components	Ensure that a comprehensive TLS server certificate inventory

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	that: 1. Accurately reflects the current system; 2. Includes all components within the authorization boundary of the system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and b. Review and update the system component inventory [Assignment: organization-defined frequency].	is established and maintained, including: • Metadata • Installed locations • Owners
CM-12	INFORMATION LOCATION Control: a. Identify the location of [Assignment: organization-defined information] and the specific system components on which the information resides; b. Identify and document the users who have access to the system and system components where the information resides; and c. Document changes to the location (i.e., system or system components) where the information resides.	Identify the location of all TLS certificates and private keys . Identify and document and keep up to date information about all certificate owners and System Administrators. Identify and document and keep up-to-date-information about the location of private keys.
CP-2	CONTINGENCY PLAN Control: a. Develop a contingency plan for	Establish “crypto-agility” plans for the replacement of TLS server certificates in response

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	the system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the security and privacy controls originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, system, or	to a CA compromise, discovered algorithm vulnerability, discovered cryptographic bug, or compromised private keys.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification.	
CP-3	CONTINGENCY TRAINING Control: Provide contingency training to system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time-period] of assuming a contingency role or responsibility; b. When required by system changes; and c. [Assignment: organization-defined frequency] thereafter.	Ensure all certificate owners are trained and understand their responsibilities in TLS server certificate crypto-agility plans.
CP-4	CONTINGENCY PLAN TESTING Control: a. Test the contingency plan for the system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;	Ensure that TLS server certificate crypto-agility plans are regularly tested.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.	
CP-13	ALTERNATIVE SECURITY MECHANISMS Control: Employ [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.	Ensure that backup certificate authorities (CAs) are maintained, including maintaining contracts with backup public CAs.
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION Control: Uniquely identify and authenticate [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.	Ensure that all TLS servers have certificates for authentication. Ensure that all TLS clients properly validate TLS server certificates when establishing TLS connections
IA-4	IDENTIFIER MANAGEMENT Control: Manage system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device;	Ensure that all TLS server certificate requests are reviewed by a person with relevant knowledge of the application in question or via an approved automated process to verify that the common names (CNs) and subject alternative names (SANs) that serve as identifiers in TLS server

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	c. Assigning the identifier to the intended individual, group, role, or device; and d. Preventing reuse of identifiers for [Assignment: organization-defined time-period].	certificates are vetted before issuance.
IA-5	AUTHENTICATOR MANAGEMENT Control: Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; f. Changing/refreshing authenticators [Assignment: organization-defined time-period by authenticator type]; g. Protecting authenticator content from unauthorized	Ensure TLS server certificates, which serve as authenticators for servers, are properly managed, including: - An up to date inventory - Up to date ownership information - Secure private key handling and distribution - Sufficient key length and strong signing algorithms - Appropriate reviews for certificate requests - Replacement of certificates and keys on role changes and termination - Continuous monitoring -

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	disclosure and modification; h. Requiring individuals to take, and having devices implement, specific security controls to protect authenticators; and i. Changing authenticators for group/role accounts when membership to those accounts' changes.	
IA-9	SERVICE IDENTIFICATION AND AUTHENTICATION Control: Identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.	Use TLS server certificates for identification and authentication on all servers where TLS is the appropriate security protocol to secure communications (e.g., to secure HTTP, SMTP, LDAP, FTP, etc.).
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES Control: a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that: i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and	Document and disseminate TLS server certificate incident response plans for the following: - Certificate authority compromises - Cryptographic algorithms found to be vulnerable - Cryptographic library bugs that affect cryptographic keys and certificates - Compromise of one or more private keys that are associated with certificates - Compromise of the certificate management system itself

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b. Designate an [Assignment: organization-defined senior management official] to manage the incident response policy and procedures; c. Review and update the current incident response: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency]; d. Ensure that the incident response procedures implement the incident response policy and controls; and e. Develop, document, and implement remediation actions for violations of the incident response policy.	
IR-2	INCIDENT RESPONSE TRAINING Control: Provide incident response training to system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time-period] of assuming an incident response role or responsibility.	Ensure all certificate owners are trained and understand their responsibilities in TLS server certificate incident response plans.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
IR-3	INCIDENT RESPONSE TESTING Control: Test the incident response capability for the system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.	Ensure that TLS server certificate incident response plans are tested.
IR-4	INCIDENT HANDLING Control: a. Implement an incident handling capability for security and privacy incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinate incident handling activities with contingency planning activities; c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	• Document and disseminate TLS server certificate incident response plans for the following: Certificate authority compromises • Cryptographic algorithms found to be vulnerable • Cryptographic library bugs that affect cryptographic keys and certificates • Compromise of one or more private keys that are associated with certificates • Compromise of the certificate management system itself
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES Control: a. Develop, document, and disseminate to [Assignment:	Establish TLS server certificate maintenance policies and procedures, including purpose, scope, roles, responsibilities,

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	organization-defined personnel or roles]: 1. A system maintenance policy that: i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system maintenance policy and the associated system maintenance controls; b. Designate an [Assignment: organization-defined senior management official] to manage the system maintenance policy and procedures; c. Review and update the current system maintenance: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency]; d. Ensure that the system maintenance procedures implement the system maintenance policy and controls; and e. Develop, document, and implement remediation actions for	management commitment, coordination, and compliance.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	violations of the maintenance policy.	
MA-6	TIMELY MAINTENANCE Control: Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time-period] of failure.	Ensure that certificates are renewed and replaced a sufficient number of days prior to expiration to minimize downtime risk.
PL-2	SECURITY AND PRIVACY PLANS Control: a. Develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture; 2. Explicitly define the authorization boundary for the system; 3. Describe the operational context of the system in terms of missions and business processes; 4. Provide the security categorization of the system including supporting rationale; 5. Describe the operational environment for the system and relationships with or connections to other systems; 6. Provide an overview of the security and privacy requirements for the system; 7. Identify any relevant overlays, if applicable; 8. Describe the security and privacy controls in place or	Develop security plans for TLS private keys to ensure they are consistent with the security plans for other secrets such as passwords and keys for symmetric-key encryption.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distribute copies of the security and privacy plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles]; c. Review the security and privacy plans [Assignment: organization-defined frequency]; d. Update the security and privacy plans to address changes to the system and environment of operation or problems identified during plan implementation or security and privacy control assessments; and e. Protect the security and privacy plans from unauthorized disclosure and modification.	
PL-9	CENTRAL MANAGEMENT Control: Centrally manage [Assignment: organization-defined security and privacy controls and related processes].	Establish a central certificate service that enables central oversight and monitoring. Define clear TLS server certificate management responsibilities for the certificate services team and certificate owners.
PM-1	INFORMATION SECURITY PROGRAM PLAN	Develop and disseminate an information security program

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	Control: a. Develop and disseminate an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects the coordination among organizational entities responsible for information security; and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Review the organization-wide information security program plan [Assignment: organization-defined frequency]; c. Update the information security program plan to address organizational changes and	plan that includes the following for TLS server certificates: - Requirements for proper management - Roles and responsibilities - Coordination between the certificate services team and certificate owners

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	problems identified during plan implementation or control assessments; and d. Protect the information security program plan from unauthorized disclosure and modification.	
PM-2	INFORMATION SECURITY PROGRAM ROLES Control: a. Appoint a Senior Agency Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program; b. Appoint a Senior Accountable Official for Risk Management to align information security management processes with strategic, operational, and budgetary planning processes; and c. Appoint a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.	Appoint a senior executive with the mission of ensuring TLS server certificates are properly managed to minimize security and operational risks.
PM-4	PLAN OF ACTION AND MILESTONES PROCESS Control: a. Implement a process to ensure that plans of action and milestones for the security and privacy programs and associated organizational systems: 1. Are developed and maintained;	Establish actions and milestones for implementing and deploying the TLS server certificate information security program plan. Ensure regular reviews of progress and status are performed.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	2. Document the remedial information security and privacy actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with established reporting requirements. b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	
PM-5	SYSTEM INVENTORY Control: Develop and maintain an inventory of organizational systems.	Ensure that a comprehensive TLS server certificate inventory is established and maintained, including: • Metadata • Installed locations Owners
PM-7	ENTERPRISE ARCHITECTURE Control: Develop an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.	Establish an enterprise architecture that enables the monitoring of communications within TLS encrypted sessions for attacks (Inspect TLS traffic on sessions between external and internal devices as well as sessions between internal devices).
PM-9	RISK MANAGEMENT STRATEGY Control: a. Develops a comprehensive strategy to manage:	Ensure the following risks are addressed in the Risk

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; 2. Privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information; and 3. Supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services; b. Implement the risk management strategy consistently across the organization; and c. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.	Management Strategy for TLS server certificates: • Outages due to certificate expirations • Undetected pivoting between systems within TLS encrypted connections • Outages or disclosure of information that could result from an inability to rapidly change large numbers of certificates and keys in response to a large-scale cryptographic event • Discloser of private keys that could result from manual key transfer • Disclosure of information that could result from an adversary installing a rogue server certificate • Disclosure of information that could result from trusting a bogus certificate or unapproved certificate authority • Disclosure of information that could result from using an improperly configured certificate, a vulnerable cryptographic algorithm or an insufficiently long key
RA-3	RISK ASSESSMENT Control: a. Conduct a risk assessment, including the likelihood and magnitude of harm, from:	Ensure the following TLS server certificates risks are included in the Risk Assessment:

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	1. The unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 2. Privacy-related problems for individuals arising from the intentional processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization and missions/business process perspectives with system-level risk assessments; c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]]; d. Review risk assessment results [Assignment: organization-defined frequency]; e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact	• Outages due to certificate expirations • Undetected pivoting between systems within TLS encrypted connections • Outages or disclosure of information that could result from an inability to rapidly change large numbers of certificates and keys in response to a large-scale cryptographic events. • Discloser of private keys that could result from manual key transfer • Disclosure of information that could result from an adversary installing a rogue server certificate • Disclosure of information that could result from trusting a bogus certificate or unapproved certificate authority • Disclosure of information that could result from using an improperly configured certificate, vulnerable cryptographic algorithm or an insufficiently long key

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	the security or privacy state of the system.	
RA-5	VULNERABILITY SCANNING Control: a. Scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from control assessments; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability scanning process and control assessments	Scan for vulnerabilities in TLS server certificates, including: • Improperly configured certificates • Weak key lengths • Vulnerable cryptographic algorithms • Unapproved certificate authorities • Validity periods that exceed approved maximums

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability scanning tools that include the capability to readily update the vulnerabilities to be scanned.	
RA-7	RISK RESPONSE Control: Respond to findings from security and privacy assessments, monitoring, and audits.	Respond to findings from security and privacy assessments, monitoring, and audits for TLS server certificates and related system components.
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES Control: a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that: i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and the	Designate approved public and internal CAs from which TLS server certificates may be acquired and used. Designate approved TLS Server Certificate Management components that can be acquired and used, e.g. central certificate service software, HSMs, TLS inspection appliances.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	associated system and services acquisition controls; b. Designate an [Assignment: organization-defined senior management official] to manage the system and services acquisition policy and procedures; c. Review and update the current system and services acquisition: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency]; d. Ensure that the system and services acquisition procedures implement the system and services acquisition policy and controls; and e. Develop, document, and implement remediation actions for violations of the system and services acquisition policy. Designate approved public CAs from which TLS server certificates can be acquired.	
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE Control: a. Manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy	Define and document clear lifecycle management processes and responsibilities for TLS server certificates.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security and privacy roles and responsibilities; and d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	
SA-4	ACQUISITION PROCESS Control: Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Security and privacy documentation requirements; e. Requirements for protecting security and privacy documentation; f. Description of the system development environment and environment in which the system is intended to operate; g. Allocation of responsibility or identification of parties responsible for information	Enforce the criteria in requirements a. through g. in acquisition contracts with public certificate authorities.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	security, privacy, and supply chain risk management; and h. Acceptance criteria.	
SA-10	DEVELOPER CONFIGURATION MANAGEMENT Control: Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	Ensure that developers who leverage TLS server certificates in their developed systems (e.g., DevOps) follow TLS server certificate management policies and procedures. Ensure that system administrators that are responsible for installation and configuration of TLS management components such as the central certificate service software, HSMs, and TLS inspection appliances follow TLS server certificate management policies when initially configuring these components. Ensure that all configuration changes are approved an also conform to policies.
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES Control:	Ensure that secure management of TLS server certificates and private keys is incorporated into

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that: i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls; b. Designate an [Assignment: organization-defined senior management official] to manage the system and communications protection policy and procedures; c. Review and update the current system and communications protection: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency]; d. Ensure that the system and communications protection procedures implement the system	Communications Protection Policy and Procedures. Ensure that protection of TLS server certificate management components, e.g., central certificate management service software, HSMs, TLS inspection appliances, is incorporated into Systems Protection Policy and Procedures.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	and communications protection policy and controls; and e. Develop, document, and implement remediation actions for violations of the system and communications protection policy.	
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY Control: Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	Leverage TLS in the protecting the integrity and confidentiality of transmitted information. Implement secure management of TLS server certificates and private keys to ensure the secure operation of TLS.
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT Control: Establish and manage cryptographic keys for required cryptography employed within the system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	Establish and manage TLS private keys in compliance with requirements in NIST SP 800-57 and SP 1800-16B.
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES Control: Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider.	Document, publish, communicate, and enforce clear policies for TLS server certificate issuance and management.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
SC-23	SESSION AUTHENTICITY Control: Protect the authenticity of communications sessions.	Use TLS server certificates to authenticate servers.
SI-4	SYSTEM MONITORING Control: a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;	Monitor sessions and operations within TLS encrypted connections to detect attacks and indicators of potential attacks.

SP 800-53 Control #	SP 800-53 Requirement	Mapping to TLS Server Certificates
	f. Obtain legal opinion regarding system monitoring activities; and g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	

1446

Appendix E References

E. Barker, "Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms," NIST SP 800-175B, Gaithersburg, MD, Aug. 2016. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf.

E. Barker and A. Roginsky, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths," National Institute of Standards and Technology (NIST) Special Publication (SP) 800-131A Revision 1, Gaithersburg, MD, Nov. 2015. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf.

D. Cooper et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, May 2008. Available: https://tools.ietf.org/html/rfc5280.

M. Crispin, "Internet Message Access Protocol – Version 4rev1," RFC 3501, Mar. 2003. Available: https://tools.ietf.org/html/rfc3501.

T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) protocol version 1.2," RFC 5246, Aug. 2008. Available: https://tools.ietf.org/html/rfc5246.

Information Technology Laboratory, "Secure Hash Standard (SHS)," NIST, Federal Information Processing Standards PUB 180-4, Gaithersburg, MD, Aug. 2015. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

J. Klensin, "Simple Mail Transfer Protocol," RFC 5321, Oct. 2008. Available: https://tools.ietf.org/html/rfc5321.

P. Mockapetris, "Domain Names – Concepts and Facilities," RFC 1034, Nov. 1987. Available: https://tools.ietf.org/html/rfc1034.

K. Moriarty et al., "PKCS #12: Personal Information Exchange Syntax v1.1," RFC 7292, July 2014. Available: https://tools.ietf.org/html/rfc7292.

J. Myers and M. Rose, "Post Office Protocol – Version 3," RFC 1725, Nov. 1994. Available: https://tools.ietf.org/html/rfc1725.

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018. See https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST SP 800-53 Rev. 5 (Draft) Security and Privacy Controls for Information Systems and Organizations. See https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

T. Polk et al., “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,” NIST SP 800-52 Revision 1, Gaithersburg, MD, Apr. 2014. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf.

T. Pornin, “Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA),” RFC 6979, Aug. 2013. Available: https://tools.ietf.org/html/rfc6979.

M. Pritikin et al., “Simple Certificate Enrollment Protocol draft-nourse-scep-23,” Internet Draft, Sept. 7, 2011. Available: https://tools.ietf.org/html/draft-nourse-scep-23.

V. Rekhter et al., “A Border Gateway Protocol 4 (BGP-4),” RFC 4271, Jan. 2006. Available: https://tools.ietf.org/html/rfc4271.

E. Rescorla, “HTTP over TLS,” RFC 2818, May 2000. Available: https://tools.ietf.org/html/rfc2818.

J. Sermersheim, “Lightweight Directory Access Protocol (LDAP): The protocol,” RFC 4511, June 2006. Available: https://www.ietf.org/rfc/rfc4511.txt.