



Certificate Management Enterprise Technology Guideline

1. Scope

This Enterprise Technology Guideline (ETG) represents the official technology architecture standard for certificate management in VA IT systems. For more details, please visit the Technology Architecture Guidelines Confluence site (log-in required):

[Enterprise Technology Guidelines](#)

[Venafi Certificate Renewal Automation Runbook](#)

2. Background

On March 3, 2023, Google submitted a proposal on the Certification Authorities (CA) Browser forum, titled [Moving Forward, Together](#), which will reduce the lifespan of SSL/TLS from one year to ninety (90) days. This upcoming shift will potentially require more SSL/TLS certificates than most IT teams can currently handle. The reason the lifespan of SSL/TLS certificates continues to reduce from five (5) years to three (3) years to our current one (1) year certificate to the proposed 90 days is due to adversaries gaining access to increasingly powerful computers and software that make it easier to break encryption for existing SSL/TLS certificates.

3. Solution

VA shall implement enterprise capabilities for automation of Public Key Infrastructure (PKI) certificate renewal and provisioning to adapt to future changes in SSL/TLS lifespan reduction. These capabilities must be implemented by December 31, 2026.

1. Establishing automation of PKI certificate renewal and provisioning will require error handling as well as validation testing to ensure systems are not adversely impacted once provisioning is completed. The process will also require monitoring to ensure human intervention should unforeseen problems arise. This will require developer resources that must be provided for by each system that utilizes PKI certificates.
2. Reducing the lifespan of PKI certificates makes it more difficult for them to do so because it reduces the amount of session data that exists.

4. Public Key Infrastructure (PKI) Guidelines



The enterprise PKI program plays a key role in managing secrets and protecting the confidentiality, integrity, and availability of enterprise systems in VA. OIT currently provides the [Venafi Trust Protection Platform \(TPP\)](#) as the Enterprise Key and Certificate Management (EKCM) solution that facilitates the control and management of cryptographic keys and digital certificates used to secure Information Technology (IT) assets. This software allows organizations to keep an inventory of encryption keys and certificates installed on desktops, mobile devices, and application servers across enterprise networks and in the cloud. In addition, it monitors the environment to detect any new keys and certificates and provides visibility into how or where the keys and certificates on an enterprise network are used. Using this utility, information security staff can apply policies, track changes like key deletion or permission changes, and investigate anomalous key or certificate usage.

Enterprise PKI SharePoint site: [Enterprise VA PKI \(sharepoint.com\)](#)

Software Factory Utility for Certificate Management: [Venafi | Docs | CODE VA](#)

5. Self-Service Requests

[SSL/TLS Certificate](#)

[Venafi User Portal Access](#)

[VA PKI Policy Documents](#)

[Individual Software Certificate](#)

[Shared Mailbox/Corporate Mailbox Certificate](#)

[VA Partner Software Certificate](#)

[VA PKI Supported Software](#)

[VA PKI Help](#)

6. VA PKI Support Teams



VA Enterprise Technology Guidelines
Technology Architecture and Strategies (TAS)
Office of Information and Technology (OIT)

Name	ServiceNow Assignment Group	Email Distribution List
PKI Operations	IO.SS.PKI.OPERATIONS	OIT IO SS PKI VPC ALL EMPLOYEES OITITOPSSOIOSSPKIVPCALLEMPLOYEES@va.gov
PKI Engineering	IO.AS.PKI.ENGINEERING	OITIOSSPKIENGALLSTAFF@va.gov
Identity Access Management (IAM)	IO.TPS.IAM.Data Quality Team	IAM Data Quality Team IAMDataQualityTeam@va.gov
DNS Adds, Deletes, and Modifications	IO.AS.AD.DNS Adds Deletes & Modifications	
Network Edge Operations Team	NETWORK.NOC.NEO	NOCNetworkEdgeOperations@va.gov

7. Technical References

Venafi Trust Protection documents: [VA Public Key Infrastructure \(PKI\) - Venafi Trust Protection Platform Documents - All Documents \(sharepoint.com\)](#)

Playbooks for Certificate Automation by Environment:

[VA Public Key Infrastructure \(PKI\) - Playbooks for Certificate Automation by Environment - All Documents \(sharepoint.com\)](#)

PKI Troubleshooting:

[VA Public Key Infrastructure \(PKI\) - PKI Troubleshooting - All Documents \(sharepoint.com\)](#)



Document Version Control

Date	Version	Change Details	By
Nov 2024	1.0	Initial version that references CODE VA usage guidelines for Venafi and recent strategic architecture decision record for using enterprise automated certificate renewal and certificate management capabilities.	OCTO/AES
Dec 2025	2.0	Annual refresh and validation for currency.	DSD/TAS

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.