Create PKI Certificate Request

Process Asset Library
Office of Information and Technology
Create PKI Certificate Request Map
Process: Create PKI Certificate Request

Overview: The process map for Create PKI Certificate Request cycles through the following process and review activities:

CPCR-01 Product Build
CPCR-02 Initiate PKI Certificate Request
CPCR-03 Create Certificate Signing Request
CPCR-04 Submit Certificate Signing Request
CPCR-05 Process Certificate Request
CPCR-06 Need Information?
CPCR-07 Type of Certificate Needed?
CPCR-08 Create and Return Internal Certificate
CPCR-09 Create and Return with External Certificate
CPCR-10 Create Certificate File
CPCR-11 Change Management
CPCR-12 Install Certificate on Server
CPCR-13 Confirm Certificate Works Properly
CPCR-14 Functions Properly?
CPCR-15 Create Notification for Certificate Renewal
CPCR-16 Update Database with New Certificate
Create PKI Certificate Request Description and Goals

Description
The Create Public Key Infrastructure (PKI) Certificate Request process is used in enforcing the security required in the Office of Information and Security model that assures the confidentiality, integrity, and availability of VA information and information systems. Certificates are required to protect the data transferred between servers, networked devices and end users. PKI certificates are used to verify a server's identity. The request for a PKI certificate has the inherent responsibility to provide accurate information and to protect the keys/certificates issued for a configuration item such as a system, appliance, service, application, hardware, or network device.

Goals
The Goal of the Create PKI Certificate Request process is to:
- Standardize the process for New PKI Certificate Request
- Ensure Certificate Request information is reviewed for accuracy and completeness
- Ensure Change Management compliance
- Ensure PKI Certificate Management Database is maintained as the authoritative source for Certificate information
Create PKI Certificate Request RACI Information

The following describes the RACI information for this process:

**CPCR-01 Product Build**

Responsible Role: System Owner  
Accountable Role: Program Executive Officer  
Consulted Role: None Listed  
Informed Role: None Listed

**CPCR-02 Initiate PKI Certificate Request**

Responsible Role: System Owner  
Accountable Role: Program Executive Officer  
Consulted Role: None Listed  
Informed Role: None Listed

**CPCR-03 Create Certificate Signing Request**

Responsible Role: System Administrator  
Accountable Role: System Owner  
Consulted Role: None Listed  
Informed Role: None Listed

**CPCR-04 Submit Certificate Signing Request**

Responsible Role: System Administrator  
Accountable Role: System Owner  
Consulted Role: None Listed  
Informed Role: None Listed

**CPCR-05 Process Certificate Request**

Responsible Role: PKI Help Desk
CPCR-06 Need Information?

Responsible Role: PKI Help Desk
Accountable Role: Director, National Service Desk
Consulted Role: None Listed
Informed Role: None Listed

CPCR-07 Type of Certificate Needed?

Responsible Role: PKI Help Desk
Accountable Role: Director, National Service Desk
Consulted Role: None Listed
Informed Role: None Listed

CPCR-08 Create and Return Internal Certificate

Responsible Role: Enterprise Systems Engineering PKI Team
Accountable Role: Manager, Enterprise System Engineering PKI Team
Consulted Role: None Listed
Informed Role: None Listed

CPCR-09 Create and Return with External Certificate

Responsible Role: PKI Help Desk
Accountable Role: Director, National Service Desk
Consulted Role: None Listed
Informed Role: None Listed

CPCR-10 Create Certificate File
Responsible Role: System Administrator  
Accountable Role: System Owner  
Consulted Role: None Listed  
Informed Role: None Listed

**CPCR-11 Change Management**

Responsible Role: PKI Help Desk  
Accountable Role: Director, National Service Desk  
Consulted Role: None Listed  
Informed Role: None Listed

**CPCR-12 Install Certificate on Server**

Responsible Role: System Administrator  
Accountable Role: System Owner  
Consulted Role: None Listed  
Informed Role: None Listed

**CPCR-13 Confirm Certificate Works Properly**

Responsible Role: System Owner  
Accountable Role: Program Executive Officer  
Consulted Role: None Listed  
Informed Role: None Listed

**CPCR-14 Functions Properly?**

Responsible Role: System Owner  
Accountable Role: Program Executive Officer  
Consulted Role: None Listed  
Informed Role: None Listed
CPCR-15 Create Notification for Certificate Renewal

Responsible Role: System Owner
Accountable Role: Program Executive Officer
Consulted Role: None Listed
Informed Role: None Listed

CPCR-16 Update Database with New Certificate

Responsible Role: Enterprise Systems Engineering PKI Team
Accountable Role: Manager, Enterprise System Engineering PKI Team
Consulted Role: None Listed
Informed Role: None Listed
Create PKI Certificate Request Associated Artifacts Information

Associated Artifacts information (including hyperlinks) for this process includes:
Request for Change
Version Description Document Template

Create PKI Certificate Request Tools and Web Sites Information

The Tools and Web Sites associated with this process (including hyperlinks) include:
CA Service Desk Manager
Certificate Management Database
VA PKI Information and Enrollment Portal
VA PKI SSL/TLS SharePoint Site

Create PKI Certificate Request Standards Information

Standards associated with this process (including hyperlinks) include:
Digital Signature Guide
Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1
OI&T Change Management Process Document
Release Requirements User Stories Decision Tree
Create PKI Certificate Request Process

Process Activity Name: CPCR-01 Product Build

Previous Activities
Process Begins

Next Activities
If "Return to BLD":
Product Build Process
Or
If "Continue with CPCR":
CPCR-02 Initiate PKI Certificate Request

Description
The Product Build (BLD) Process includes activities that create product and system builds, including system integration testing. Public-Key Infrastructure (PKI) Certificates are used to protect the data transferred by authenticating a configuration item such as a system, appliance, service, application, hardware or network device. The BLD process creates and updates a Version Description Document which identifies what is contained in the product build.

Input
Requirements Specification Document (or Use Stories)

Output
Version Description Document

Associated Artifacts
Version Description Document Template

Responsible Role
System Owner

Accountable Role
Program Executive Officer

Consulted Role
None Listed

Informed Role
None Listed

Tools and Websites
None Listed
Standards
Release Requirements User Stories Decision Tree

More Info
When creating or updating the Version Description Document, ensure that you copy the Compliance User Stories Template appropriate to your product/project as depicted in the Release Requirements Compliance User Stories Decision Tree for your type of project from the Rational Requirements Management Repository into your product/project instance in the repository and use the template.

Process Activity Name: CPCR-02 Initiate PKI Certificate Request

Previous Activities
CPCR-01 Product Build

Next Activities
CPCR-03 Create Certificate Signing Request

Description

Input
Version Description Document

Output
Certificate Request Information

Associated Artifacts
None Listed

Responsible Role
System Owner

Accountable Role
Program Executive Officer

Consulted Role
None Listed

Informed Role
None Listed

Tools and Websites
VA PKI Information and Enrollment Portal
VA PKI SSL/TLS SharePoint Site

Standards
None Listed

More Info
None Listed

Process Activity Name: CPCR-03 Create Certificate Signing Request

Previous Activities
CPCR-02 Initiate PKI Certificate Request
Or
CPCR-06 Need Information?

Next Activities
CPCR-04 Submit Certificate Signing Request

Description
The System Administrator provides a Fully Qualified Domain Name for the System to be implemented and creates the signing sheet for the VA Public-Key Infrastructure (PKI) Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Request.

Input
Certificate Request Information

Output
VA PKI SSL/TLS Request

Associated Artifacts
None Listed

Responsible Role
System Administrator

Accountable Role
System Owner

Consulted Role
None Listed

Informed Role
None Listed

Tools and Websites
VA PKI Information and Enrollment Portal
VA PKI SSL/TLS SharePoint Site
Standards
None Listed

More Info
None Listed

Process Activity Name: CPCR-04 Submit Certificate Signing Request

Previous Activities
CPCR-03 Create Certificate Signing Request

Next Activities
CPCR-05 Process Certificate Request

Description
The System Administrator submits the completed VA Public-Key Infrastructure (PKI) Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Request to the VA PKI Help mail group.

Input
VA PKI SSL/TLS Request

Output
Submitted VA PKI SSL/TLS Request

Associated Artifacts
None Listed

Responsible Role
System Administrator

Accountable Role
System Owner

Consulted Role
None Listed

Informed Role
None Listed

Tools and Websites
None Listed

Standards
Digital Signature Guide

More Info
Certificate Requests received before 2 pm Central Time will be completed and returned that same day. Certificates received after 2 pm Central Time will be completed the next business day.
Process Activity Name: CPCR-05 Process Certificate Request

Previous Activities
CPCR-04 Submit Certificate Signing Request
Or
CPCR-14 Functions Properly?

Next Activities
CPCR-06 Need Information?

Description
The Public-Key Infrastructure (PKI) Help Desk specialty support, National Service Desk, logs the VA Public-Key Infrastructure (PKI) Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Request. The PKI Help Desk reviews the information in the request to ensure the information is accurate and complete. If additional information is needed, the PKI Help Desk requests it. If the System communicates with an external service, the PKI Help Desk issues the PKI Certificate. If the System communicates with an internal service, the request is forwarded to the Enterprise System Engineering PKI Team.

Input
VA PKI SSL/TLS Request
VA PKI Help Desk Ticket, if needed

Output
Certificate Management Database Entry
Public-Key Infrastructure Certificate
Request for Certificate Information

Associated Artifacts
None Listed

Responsible Role
PKI Help Desk

Accountable Role
Director, National Service Desk

Consulted Role
None Listed

Informed Role
None Listed

Tools and Websites
Certificate Management Database
Process Activity Name: CPCR-06 Need Information?

Previous Activities
CPCR-05 Process Certificate Request

Next Activities
If "Yes":
CPCR-03 Create Certificate Signing Request
Or
If "No":
CPCR-07 Type of Certificate Needed?

Description
Public-Key Infrastructure Help Desk determines if more information is needed (Yes) or not (No).

Responsible Role
PKI Help Desk

Accountable Role
Director, National Service Desk

Consulted Role
None Listed

Informed Role
None Listed

Process Activity Name: CPCR-07 Type of Certificate Needed?

Previous Activities
CPCR-06 Need Information?

Next Activities
If "Internal":
CPCR-08 Create and Return Internal Certificate
Or
If "External":
CPCR-09 Create and Return with External Certificate

**Description**
The Public-Key Infrastructure Help Desk determines if an Internal certificate is needed (Internal) or if an external certificate is needed (External).

**Responsible Role**
PKI Help Desk

**Accountable Role**
Director, National Service Desk

**Consulted Role**
None Listed

**Informed Role**
None Listed

**Process Activity Name: CPCR-08 Create and Return Internal Certificate**

**Previous Activities**
CPCR-07 Type of Certificate Needed?

**Next Activities**
CPCR-10 Create Certificate File

**Description**
The Enterprise System Engineering (ESE) Public-Key Infrastructure (PKI) Team creates the PKI Certificate and updates the Certificate Management Database Entry with the System Owner, Domain Name and Certificate Expiration date and sends the PKI Certificate to the System Owner.

**Input**
VA PKI SSL/TLS Request

**Output**
Issued Public-Key Infrastructure Certificate
Updated Certificate Management Database Entry

**Associated Artifacts**
None Listed

**Responsible Role**
Enterprise Systems Engineering PKI Team

**Accountable Role**
Manager, Enterprise System Engineering PKI Team
Consulted Role
None Listed

Informed Role
None Listed

Tools and Websites
Certificate Management Database
VA PKI SSL/TLS SharePoint Site

Standards
None Listed

More Info
None Listed

Process Activity Name: CPCR-09 Create and Return with External Certificate

Previous Activities
CPCR-07 Type of Certificate Needed?

Next Activities
CPCR-10 Create Certificate File

Description
The Public-Key Infrastructure (PKI) Help Desk specialty support, National Service Desk, creates the Public-Key Infrastructure Certificate and updates the Certificate Management Database Entry with the System Owner, Domain Name and Certificate Expiration date and sends the PKI Certificate to the System Owner's email address.

Input
Public-Key Infrastructure Certificate

Output
Issued Public-Key Infrastructure Certificate
Updated Certificate Management Database Entry

Associated Artifacts
None Listed

Responsible Role
PKI Help Desk

Accountable Role
Director, National Service Desk
Consulted Role
None Listed

Informed Role
None Listed

Tools and Websites
Certificate Management Database

Standards
None Listed

More Info
None Listed

Process Activity Name: CPCR-10 Create Certificate File

Previous Activities
CPCR-08 Create and Return Internal Certificate
Or
CPCR-09 Create and Return with External Certificate

Next Activities
CPCR-11 Change Management

Description
The System Administrator creates the Public-Key Infrastructure (PKI) Certificate File to be installed and initiates a Request For Change.

Input
Issued Public-Key Infrastructure Certificate

Output
Public-Key Infrastructure Certificate File
Request For Change

Associated Artifacts
None Listed

Responsible Role
System Administrator

Accountable Role
System Owner

Consulted Role
None Listed
**Informed Role**
None Listed

**Tools and Websites**
CA Service Desk Manager

**Standards**
OI&T Change Management Process Document

**More Info**
The Request For Change documents the requirements for the change in the Change Management process.

**Process Activity Name: CPCR-11 Change Management**

**Previous Activities**
CPCR-10 Create Certificate File

**Next Activities**
If "Remain in CPRC":
CPCR-12 Install Certificate on Server
Or
If "Go to CHG":
Change Management Process

**Description**
The Change Management (CHG) Process is initiated once the Public-Key Infrastructure (PKI) Certificate is created. In CHG a Request For Change (RFC) is reviewed for completeness, the Approving Official to grant approval for installing the PKI Certificate in the production environment, and the RFC is updated.

**Input**
Issued Public-Key Infrastructure Certificate
Version Description Document

**Output**
Request For Change

**Associated Artifacts**
Request for Change

**Responsible Role**
PKI Help Desk

**Accountable Role**
Director, National Service Desk
Process Activity Name: CPCR-12 Install Certificate on Server

Previous Activities
CPCR-11 Change Management

Next Activities
CPCR-13 Confirm Certificate Works Properly

Description
The System Administrator installs the Public-Key Infrastructure (PKI) Certificate after the Request For Change is approved for the PKI Certificate File to be installed into the system for production use. The Request for Change updates the Configuration Management tool with the addition of a new Configuration Item(s). The System Administrator informs the System Owner that the Public-Key Infrastructure Certificate is ready to test.

Input
Public-Key Infrastructure Certificate File
Request For Change

Output
Notification of Certificate Installation

Associated Artifacts
None Listed

Responsible Role
System Administrator

Accountable Role
System Owner

Consulted Role
None Listed
Informed Role
None Listed

Tools and Websites
CA Service Desk Manager

Standards
None Listed

More Info
None Listed

Process Activity Name: CPCR-13 Confirm Certificate Works Properly

Previous Activities
CPCR-12 Install Certificate on Server

Next Activities
CPCR-14 Functions Properly?

Description
The System Owner determines if the Public-Key Infrastructure (PKI) Certificate is working properly in conjunction with the System Administrator. If the PKI Certificate does not function properly, the PKI Help Desk is contacted and a Help Ticket is created.

Input
Notification of Certificate Installation

Output
VA PKI Help Desk Ticket, if needed

Associated Artifacts
None Listed

Responsible Role
System Owner

Accountable Role
Program Executive Officer

Consulted Role
None Listed

Informed Role
None Listed

Tools and Websites
CA Service Desk Manager
**Standards**
None Listed

**More Info**
None Listed

**Process Activity Name: CPCR-14 Functions Properly?**

**Previous Activities**
CPCR-13 Confirm Certificate Works Properly

**Next Activities**
If "Yes":
CPCR-15 Create Notification for Certificate Renewal
And
CPCR-16 Update Database with New Certificate
Or
If "No":
CPCR-05 Process Certificate Request

**Description**
The System Owner determines if the certificate functions properly (Yes) or not (No).

**Responsible Role**
System Owner

**Accountable Role**
Program Executive Officer

**Consulted Role**
None Listed

**Informed Role**
None Listed

**Process Activity Name: CPCR-15 Create Notification for Certificate Renewal**

**Concurrent Activities**
CPCR-16 Update Database with New Certificate

**Previous Activities**
CPCR-14 Functions Properly?
Next Activities
Process Ends

Description
The System Owner creates a Certificate Expiration Reminder for the system 60 days prior to the certificate expiration date.

Input
Closed Request for Change

Output
Certificate Expiration Reminder

Associated Artifacts
None Listed

Responsible Role
System Owner

Accountable Role
Program Executive Officer

Consulted Role
None Listed

Informed Role
None Listed

Tools and Websites
None Listed

Standards
None Listed

More Info
None Listed

Process Activity Name: CPCR-16 Update Database with New Certificate

Concurrent Activities
CPCR-15 Create Notification for Certificate Renewal

Previous Activities
CPCR-14 Functions Properly?

Next Activities
Process Ends
Description
The Enterprise System Engineering Public-Key Infrastructure (PKI) Team updates the Certificate Management Database Entry with the information from the VA PKI Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Request.

Input
Closed Request for Change
VA PKI SSL/TLS Request

Output
Updated Certificate Management Database Entry

Associated Artifacts
None Listed

Responsible Role
Enterprise Systems Engineering PKI Team

Accountable Role
Manager, Enterprise System Engineering PKI Team

Consulted Role
None Listed

Informed Role
None Listed

Tools and Websites
Certificate Management Database

Standards
None Listed

More Info
None Listed

END OF PROCESS