11 November 2025
Version 1.1

Pfizer Enterprise PKI Certification Practice Statement

Pfizer, Inc.
280 Shennecossett Rd
Groton, CT 06340

Contents

CHANGE LOG

The following table contains a revision history of the document.

Version	Author	Description	Date
1.0	Bill Stites	Initial Draft and review	6.3.2025
1.1	Bill Stites	Reviewed by GIS Security-Iason Itell and Legal-Ross Barker and signed off	11.1.2025

1 INTRODUCTION

The Pfizer Enterprise Public Key Infrastructure (PKI) issues trusted digital certificates to Pfizer users, devices and entities throughout the Pfizer network using distinct subordinate Certification Authorities (CA). As designed and deployed for specific uses, all in accordance with this certification practice statement (CPS). In its role as a CA, Pfizer performs functions associated with public key operations that include receiving requests, issuing, revoking, and renewing a digital certificate and the maintenance, issuance, and publication of Certificate Revocation Lists (CRLs) for users within the Pfizer Enterprise PKI.

1.1 OVERVIEW

The effective date for implementation of the practices disclosed in this document is the date of publication of the CPS and will apply to all certification authorities related activities within the Pfizer Enterprise PKI.

The PKI Enterprise Certificate Policy (CP) describes what the Pfizer Enterprise PKI does, and this CPS describes how it is done. Any discrepancies are deferred to the Pfizer Enterprise PKI CP.

Pfizer Enterprise PKI deploys a two-tier enterprise PKI architecture using Microsoft Active Directory Certificate Services. The root tier is comprised of an offline root certification authority. The subordinate tier is comprised of online issuing certification authorities that are integrated into a Pfizer Microsoft Active Directory Forest and fulfill the CA services, operations, and infrastructure for certificates operated in accordance with the requirements of this CPS, as well as applicable regulations and policies of Pfizer, Inc. This CPS applies to certificates issued to CAs, devices, and employees, contractors, and other affiliated personnel of a contracted/contracting organization. Hardware security modules (HSM) and other key components that are not certification authorities themselves but are critical to the PKI environment (e.g., CRL publication, key storage, hosting, etc.) are employed and are addressed within.

Also deployed and signed by Pfizer Root CA 2024 is an EJBCA CA server that performs various automated certificate enrollments to scale.

In accordance with RFC 3647 this CPS is divided into nine parts that cover the security controls, practices, and procedures for certificate services within the Pfizer Enterprise PKI. Where section headings do not apply the statement “Not applicable” or “No stipulation” will be used.

1.2 DOCUMENT NAME AND IDENTIFIERS

This document is the **Pfizer Enterprise PKI Certification Practice Statement** (CPS).

1.3 PFIZER ENTERPRISE PKI PARTICIPANTS

The Pfizer Enterprise PKI is intended to be a private hierarchy of certification authorities and Subscribers.

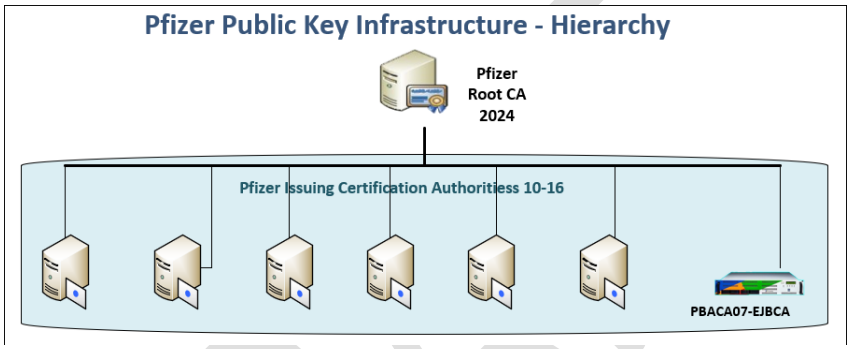
The participants in this PKI consist of the following:

1.3.1 Certification Authorities

In its role as a CA, Pfizer provides certificate services within the Pfizer Enterprise PKI. Pfizer will:

- Conform its operations to the CPS, as the same may from time to time be modified by amendments published in the Pfizer PKI Repository.
- Design and implement and maintain operational practices to achieve the requirements of this CPS.

- Issue, sign, and revoke X.509 certificates that bind a Subscriber's public key to the Subscriber's X.500 Distinguished Name and signature verification key. Upon receipt of a valid request to revoke the certificate from a person authorized to request revocation using the revocation methods detailed in this CPS, revoke a certificate issued for use within the Pfizer Enterprise PKI.
- Publish CRLs on a regular basis, in accordance with the applicable Certificate Policy and with provisions described in this CPS.
- Distribute issued certificates in accordance with the methods detailed in this CPS.
- Update CRLs in a timely manner as detailed in this CPS.
- Notify Subscribers via email of the imminent expiry of their Pfizer issued certificate (for a period specified in this CPS).



7.1.2.1 Pfizer Root CA

The Pfizer Root CA 2024 is the highest-level CA for the Pfizer Enterprise PKI. It establishes itself with a self-signed certificate and is recognized and accepted as the Trusted Root for all digital certificates. It is the top of the chain of trust, and it is managed and operated by the Pfizer Enterprise PKI team.

7.1.2.2 Pfizer Issuing CAs – 10-16

The Pfizer Issuing CAs are deployed subordinate CAs and signed by Pfizer Root CA 2024. These issue certificates to users, machines, devices, and PKI components in the Pfizer enterprise network.

7.1.2.3 Pfizer EJBCA – PBACA07

An EJBCA appliance acts as an RA for a specified Subordinate CA that deploys certificates to mobile devices and other use cases involving bulk and autoenrollment processes.

1.3.2 Registration Authorities

Registration Authorities (RAs) collect and verify subscriber's identities and information that is to be entered into the subscriber's public key certificate. Pfizer has established the necessary secure infrastructure to fully manage the lifecycle of digital certificates within the Pfizer Enterprise PKI. The RA performs its function in accordance with and are bound by the conditions of this CPS.

The RA is responsible for:

- Acceptance, evaluation, approval, and rejection of certificate applications.
- Control over the registration process.
- The identification and authentication process.
- All workflows in the management of certificate lifecycle management.

Registration Authorities (RAs) perform identification and authentication of subscribers for certificate issuance and revocation requests and pass along such requests to the Certification Authorities. RA activities are operated by the Pfizer Enterprise PKI team for all certificates issued under the Pfizer Enterprise PKI hierarchy. Keyfactor Command is used for the process of requesting, distributing and automation of certificate requests.

RA personnel involved in the issuance of digital certificates from this PKI must undergo the skills and training required in Section 5.3.

1.3.3 Subscribers (End Entities)

A subscriber is the entity that requests a certificate and holds the private key corresponding to the public key listed in the certificate. The subscribers by virtue of the enrollment process accept full responsibility for the storage and access to the private key of certificates issued to them by the Pfizer Enterprise PKI.

1.3.4 Policy Authorities

This is the entity that decides that a set of requirements for certificate issuance and use are sufficient for a given application. It is administered and governed by the Pfizer Enterprise PKI team.

The Policy Authority (PA):

- Establishes and maintains the CPS.
- Approves the establishment of trust relationships with external PKIs that offer appropriately comparable assurance.
- Ensures that all aspects of the CA services, operations, and infrastructure as described in the CPS are performed in accordance with the requirements, representations, and warranties of the CP.

1.3.5 Relying Parties

For each of the list items in §1.3 (End Entity, Subscriber, or Certificate Holder), the relying party relies upon the binding between the subscriber's name and the associated public key. For the purposes of this CP/CPS, a relying party is any entity who relies upon a certificate that is issued by Pfizer and that is used in a legal manner consistent with this CP/CPS and all related policies and agreements. A relying party is any entity that uses another's certificate for any, all, or a combination of the following reasons:

- To verify the integrity of a digitally signed message.
- To identify the creator of a message.
- To establish confidential communications with the certificate holder.

1.3.6 Other Participants

No stipulation.

1.3.7 Validation Authorities

Pfizer Enterprise PKI regularly publishes current and up-to-date revocation information available on sixteen highly available servers throughout the world. These provide any relying party with a way of obtaining certificate revocation status information.

Certificate Revocation Lists (CRLs) contain the serial numbers of revoked Pfizer Enterprise PKI certificates and date of revocation. Also included in specific information detailing the CRL itself, notably its validity period.

1.4 CERTIFICATE USAGE

The Pfizer Enterprise PKI provides digital certificates for uses including but *not limited* to secure server and client authentication, document signing, mutual client authentication, wireless and VPN authentication, and code signing.

1.4.1 Appropriate Certificate Uses

1.4.1.1 Low Assurance Level

No low assurance level policies are in effect for this PKI.

1.4.1.2 Basic Assurance Level

Basic Assurance Level is relevant to almost all certificates issued by the Pfizer Enterprise PKI.

1.4.1.3 High Assurance Level

High assurance is reserved for Code Signing and subCA certificates. These certificates are only issued from Constrained Certification Authorities designed specifically for these use cases. A subscriber agreement and higher security requirements are necessary for the issuance of certs with high assurance. See Section 3.2.3.

1.4.1.4 PKI Component

Certificates issued as part of the setup and role of PKI components, such as NDES and EJBCA are maintained, authenticated, and enrolled by The PKI Admin role, which serves as the identity validation of a subscriber.

1.4.1.5 Secure Server Certificates

Secure server certificates, also known as TLS certificates, facilitate the exchange of encryption keys in order to enable the encrypted communication between servers, or users to servers via a browser and other similar uses. These employ server authentication and\or client authentication extended key usages. Wildcard certificates cover sub-domains of any single domain and are rigorously vetted for complaince and feasability.

1.4.2 Prohibited Certificate Uses

Certificates are prohibited from being used to the extent that the use is inconsistent with applicable law or regulatory requirements, or any use not in accordance with the Pfizer CP and this CPS.

1.5 POLICY ADMINISTRATION

Information located in this section includes the contact information of the organization responsible for drafting, registering, maintaining, updating, and approving this CPS.

1.5.1 Organization Administering the Document

Pfizer Enterprise PKI team will be responsible for the ongoing maintenance and for asserting whether this certification practice statement conforms to the Pfizer Enterprise PKI Certificate Policy.

1.5.2 Contact Person

The following is the primary Pfizer, Inc. contact information:

PAM Operations
Pfizer, Inc.
445 Eastern Point Rd,
Groton, CT 06340
Email: DL-PKI-Support@pfizer.com

1.5.3 CPS Approval Procedures

The Pfizer Enterprise PKI team will determine the appropriate procedures for approving subsequent changes, amendments, or addenda to the Pfizer Enterprise PKI CPS.

7.1.2.4 1.5.3.1 Changes and notifications

The Pfizer Enterprise CA is not required to notify subscribers or change to the version number of this CP/CPS if the change, in the judgment of Pfizer Cyber Engineering PKI team, has minimal impact or none on the users of certificates and certificate revocation lists issued by the Pfizer Enterprise CA. For example, typographical corrections and changes to contact information require no notice.

The Pfizer Enterprise CA is required to notify subscribers or change the version number of this CP/CPS, if the change, in the judgment the Pfizer Enterprise CA, may have a significant impact on users of certificates and certificate revocation lists issued by the CA. The most recent copy of the Pfizer Enterprise PKI CP/CPS will supersede all previous versions and impose a legal obligation on subscribers, the Pfizer Enterprise CA, and all affected registration authorities.

Before making changes to this CPS, the CA will notify subscribers of upcoming changes via a web posting on the Pfizer Enterprise PKI Repository site.

1.6 Definitions and Acronyms

For convenience, a glossary has been provided at the Appendix A.

2 Publication and Repository Responsibilities

2.1 Repositories

This certification practice statement is accessible via the web at http://pki.pfizer.com/policies/pfizercps.pdf. The CRLs and all CA public-key certificates are available at Pfizer PKI Repository. The CRL Distribution Points contain all updated CRLS and are available through online resources 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.5% annually.

Additional information in the Pfizer PKI Repository contains:

- Current CRLs of all Pfizer CAs
- Current public key certificates for all Pfizer and specific and applicable public CAs
- Documentation that includes help, support, and Policy documents for the Pfizer Enterprise PKI

2.2 Publication of Certification Information

The Pfizer Enterprise PKI team team will make this document and other selected PKI documents available to PKI participants as described in Section 2.1 and Section 1.5.2.

This is also available upon email request: Priviledged Access Management, DL-PRIVILEGED-ACCESS-MGMT@pfizer.com.

2.3 Time or Frequency of Publication

Publication requirements for CRLs are provided in sections 4.9.7 and 4.9.12

2.4 Access Controls on Repositories

Documents published in the Pfizer PKI Repository are for public information and access is freely available. Pfizer has logical access control and version control measures in place to prevent unauthorized modification of the repository and its contents.

2.5 Confidentiality

2.5.1 Type of Information to Be Kept Confidential

Private keys held by the Pfizer Enterprise PKI that are used to sign certificates and certificate revocation lists (CRL), as well as private keys held by authorized registration authorities to sign certificate requests, are managed with highly restricted and distributed nCipher Hardware Security Modules.

2.5.2 Types of Information Not Considered Confidential

Information either appearing in the issued certificates or CRLs capable of being gathered from public sources is not considered confidential. In addition, any information received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure is not considered confidential. This CPS, certificates issued under this CPS, any associated revocation or certificate status information, and affiliated certificate policies are not considered confidential. A subscriber's distinguished name, which may include the subscriber's common name and electronic mail address, is not considered confidential.

2.5.3 Disclosure of Certificate Revocation and Suspension Information

A Pfizer Enterprise CA is the authorized source for revocation and suspension information for certificates within its purview. The Pfizer Enterprise PKI makes this information available to subscribers and relying parties through a published CRL. Revocation reason codes may be provided through the approved revocation mechanism (e.g., the reasonCode in an X.509 version 2 certificate revocation list) and are not considered confidential. Aside from the information contained in the certificate revocation list entry extension, no other information concerning the revocation is routinely disclosed.

2.5.4 Release to Law Enforcement Officials

The Pfizer Enterprise PKI will not disclose confidential information, unless such disclosure is due to either of the following:

- Disclosure is required under applicable law or regulation, applicable legal process or court order requiring the release of the information.
- The subscriber authorized the release of the information.

2.5.5 Release as Part of Civil Discovery

The Pfizer Enterprise PKI will not disclose confidential certificate-related information unless the disclosure is required under applicable law or regulation, applicable legal process, or court order requiring the release of the information.

2.5.6 Disclosure upon Owner's Request

The Pfizer Enterprise PKI will release confidential certificate-related information with the prior written consent of the subscriber.

2.5.7 Other Information Release Circumstance

No stipulation

3 IDENTIFICATION AND AUTHENTICATION

This section describes the requirements associated with identifying and authenticating certificate subscribers within the operation of the PKI.

3.1 NAMING

3.1.1 Types of Names

The Pfizer Enterprise PKI CAs and subscribers are assigned X.500 Distinguished Names (DNs) for inclusion in the "Issuer Distinguished Name" and "Subject" fields of certificates. Alternate names are also asserted in the "Subject Alternative Name" field.

The Pfizer Enterprise PKI requires the following fields in the construction of the DN:

- For an individual: The First and Last name of the individual
- For Individuals, systems, devices, and services:
  - Organization
  - Locality
  - Country
- For systems, devices, and services:
  - Make, model, hostname tied to an IP address and/or serial number or other uniquely identifying information, where appropriate

Subject names may include String X.500 Attribute Types such as:

1. CN: commonName – *Required*
   L: localityName – *Required*
   ST: stateOrProvinceName – *Required*

O: organizationName – *Required*
OU: organizationalUnitName
C: countryName – *Required*

3.1.2 Need for Names to be Meaningful

No stipulation.

3.1.3 Anonymity or Pseudonymity of Names

Pfizer CAs will not issue anonymous certificates. CA certificates will not contain anonymous or pseudonymous identities.

3.1.4 Rules for Interpreting Names

No stipulation.

3.1.5 Uniqueness of Names

The Subject or DN shall be unique for all subscribers or certificate users of each CA. If applicable, for each subscriber where the naming components are similar, additional numbers or letters may be appended to provide uniqueness. It is possible for a subscriber to have two or more certificates with the same Subject Distinguished Name (DN).

3.1.6 Recognition, authentication, and trademarks

Each certificate applicant and, upon acceptance, each subscriber represents that:

- Their submission and use of a subject name and all other information connected or related to the certificate application does not infringe on the intellectual property rights or any other right of any third parties. See §2.6
- They are not intending to, and will not, use the subject name for any unlawful purpose. Each certificate applicant and subscriber will indemnify the Pfizer Enterprise CA in respect of all claims, demands, actions, costs, expenses, loss, and damage regarding any breach of this warranty. The Pfizer Enterprise certification authority is not obligated to seek evidence of trademarks, court orders, or any other right to use the subject name prior to issuance. The Pfizer Enterprise CA is not obligated to issue or to reissue a certificate with a subject name even if the certificate application contains a registered trademark owned by the certificate applicant or for which the applicant has submitted a trademark registration application.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to prove possession of private key

The method to prove possession of a private key shall be PKCS #10, or another cryptographically equivalent request (digitally signed request with private key). This requirement does not apply where a key pair is generated by a CA on behalf of a subscriber.

3.2.2 Authentication of Organization Identity

No Stipulation.

3.2.3 Authentication of Individual Identity

Verification of Pfizer email and active account in Pfizer Active Directory is sufficient authentication for the purposes of enrolling for a certificate signed and issued by a Pfizer CA.

An exception exists for code signing certificates and some other restricted use cases. Where requested, the RA shall require a written request that includes:

- The purpose and application use of the code signing certificate.
- A detailed explanation of how the private key will be protected and maintained.
  - A TPM, HashiCorp or HSM is required for storage of the private key.
- A sign-off from the subscriber's immediate manager

3.2.4 Non-verified Subscriber Information

Validation of authority is the responsibility of the CA or the RA. A CA will identify in its CPS the submitted subscriber information that is not verified as part of a Certificate request.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Every certificate request for re-key is treated as an initial registration and must satisfy the same requirements and the issuance of a new certificate.

3.3.2 Identification and Authentication for Re-key After Revocation

Any request for re-key will be treated as an initial registration and the issuance of a new certificate. Identification and authentication for Revocation Requests. Each CA must authenticate any requests for the Revocation of a certificate; requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether the associated private key has been compromised.

The Pfizer Enterprise PKI shall keep a record of the type and details of the revocation request including the identity and authentication of the requesting person.
A subscriber certificate revocation request is valid if it complies with one of the following requirements:

- The request is raised through the RA application or
- If a revocation request is not raised through the RA application, the Pfizer CA shall perform sufficient procedures to manually authenticate the subscriber's request.

Exceptions may be allowed in the following situations:

- An organizational change within Pfizer results in changes to the DNs of several employees
- A PKI user is temporarily unable to present him/herself in person (e.g., on extended travel) and the revocation was not due to a key compromise.

Revocation service requests for certificates issued by Pfizer Enterprise PKI CA certificates are required to be approved by the Pfizer CA prior to being processed.

4 Certificate Lifecycle Operational Requirements

All CA services will comply with the requirements set in:

- The Pfizer Enterprise PKI Certificate Policy (CP)

- The Pfizer Enterprise PKI Certification Practices Statement (CPS)
- Other applicable PKI documents such as Pfizer Enterprise PKI Security Hardening

The Pfizer Enterprise CA has established a process for requesting and delivering a certificate to ensure that certificates are issued only to properly authenticated individuals or entities. Once a certificate is delivered and accepted, Pfizer CA operations must manage the process of suspending, revoking, or renewing certificates as required. The Pfizer CA records and monitors security-related activities to ensure the integrity of the certificate process.

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit Certificate Application

Below is a list of people who may submit certificate requests to the CAs that are subject to this CPS.

- RA on behalf of Pfizer users.
- Any authorized representative of a Pfizer CA.
- Any authorized representative of a Pfizer RA.

An application for a certificate does not oblige a Pfizer Enterprise CA to issue a certificate.

4.1.2 Enrollment Process and Responsibilities

7.1.2.1 CA Certificate Management

All enrollment, renewal, and rekeying tasks will be performed by a quorum of the Certificate Management team on the Root CAs, Subordinate CAs and Hardware Security Modules (HSM).

7.1.2.2 Subscriber Certificate Application

The applicant and the Registration Authority must take the following steps when an applicant applies for a certificate:

- Establish and record the identity of Subscriber, according to the requirements of level of assurance required for the certificate as per §3.2 and the commensurate authentication requirements as per section §5.2.3;
- Obtain a public/private key pair for each certificate required.
- Establish that the public key forms a functioning key pair with the private key held by the Subscriber.

An application for all certificate requests shall include the following information:

- Common name and any additional SAN names
- IP or subnet for dynamic IPs, of the common name DNS record
- Requester's name and email and ServiceNow group
- Approver's AD group
- Requester's group cost center
- Description of intended use to include application or system name
- Attached and verified CSR or note to have CSR created by the RA

Any change to an existing certificate shall require a new certificate request.

These steps may be performed in any order that is convenient for the RA team and Subscribers, and that do not defeat security; but all steps must be completed prior to certificate issuance.

Public keys shall be delivered to the certificate issuer in a way that binds the applicant's verified identification to the public key being certified. This binding shall be accomplished using means that are as secure as the security offered by the keys being certified.

4.2 CERTIFICATE APPLICATION PROCESSING

See Section 4.1.2

4.2.1 Performing Identification and Authentication Functions

See Section 4.1.2

4.2.2 Approval or Rejection of Certificate Applications

See Section 4.1.2. An RA will reject a certificate application if:

- Identification and authentication of all required Subscriber information in terms of this agreement are not performed or not consented to.
- The Pfizer CA deems the certificate issuance may negatively impact the CA's business or reputation.

4.2.3 Time to Process Certificate Applications

Pfizer makes reasonable efforts to confirm certificate application information and issue a certificate within a reasonable time frame. The time frame is greatly dependent on the type of certificate and the verification requirements as stated in the CPS. From time to time, events outside of the control of Pfizer may delay the issuance process, however Pfizer will make every reasonable effort to meet issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

An RA verifies the source of a certificate request before issuance. Certificates are checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, the CA stores contact and enrollment information with the RA and posts the certificate.

4.3.2 Notification to Subscriber of Certificate Issuance

RAs operating under this CPS may inform the subscriber (or other certificate subject) of the creation of a certificate and will make the certificate available to the subscriber through the RA.

4.3.3 Contents of Notification to Subscriber of Certificate Issuance

The RA will include the common name and requestor information and certificate as **.pem**, **.pb7**, or another suitable format.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

By accepting a Certificate, the Subscriber:

- Agrees to be bound by the continuing responsibilities, obligations and duties imposed by this CPS.
- Represents and warrants that to its knowledge no unauthorized person has had access to the private key associated with the certificate.
- Represents and warrants that the certificate information it has supplied during the registration process is truthful and accurate.

Upon receipt of a certificate, the subscriber is responsible for verifying that the information contained within the certificate is accurate and complete and that the certificate is not damaged or otherwise corrupted. In the event the certificate is inaccurate, damaged, or corrupted, the subscriber should contact the Pfizer PKI Team to have the certificate replaced as determined by the Pfizer CA.

Any of the following methods constitutes acceptance of a certificate:

1. A subscriber's receipt of a certificate and subsequent use of the key pair and certificate
2. Placement in a local store
3. Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

This CPS makes no stipulation regarding publication of subscriber certificates.

4.4.3 Notification of CA Certificate Issuance by the CA to Other Entities

Each Pfizer CA covered by this CPS publishes the following information to the PKI Repository that is available to subscribers and relying parties:

4. CA CRLs
5. Public-key CA certificates.
6. A copy or a link to the appropriate CPS

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

All subscribers will take reasonable steps to secure their private keys. The intended scope of usage for a private key is specified through certificate extensions, including the key usage and the key usage extensions, contained in the associated Certificate.

- Subscribers and CAs shall use their private keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates issued to them.
- Subscribers shall protect their private keys from unauthorized use and discontinue use of the private key following expiration or revocation of the certificate.
- Subscribers shall contact the RA if the private key is compromised.

Code Signing certificate subscribers shall always keep and maintain signing keys in an HSM, TPM or an approved key vault.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties are responsible for examining the CPS to understand all their rights and obligations under the CPS. The final decision concerning whether to rely on a verified digital signature is exclusively that of the relying party.

Reliance on a digital signature should only occur if:

- The digital signature was created during the operational period of a valid certificate, and it can be verified by referencing a validated Certificate.
- The relying party has checked the revocation status of the certificate by referring to the relevant CRLs and the certificate has not been revoked.
- The relying party understands that a digital certificate is issued to a subscriber for a specific purpose and that the digital certificate may only be used in accordance with the usages suggested in the CPS and named as object identifiers in the certificate profile.
- The certificate applied for is appropriate for the application it is used in.

4.6 CERTIFICATE RENEWAL

Certificate renewal in this policy means the replacement of a certificate using the same information—including public key information—as the previous certificate, except for the certificate validity period and serial number.

Because basic certificate renewal extends the lifetime of sensitive key material, which consequently results in increased vulnerability of key material to compromise, certificate renewal requires the issuance of a new key.

The validity period of certificates issued under this CPS shall be no more than one year and is detailed in the relevant field within the certificate.

4.6.1 Circumstance for Certificate Renewal

Pfizer makes reasonable efforts to notify subscribers via email of the imminent expiration of digital certificates. Notice shall ordinarily be provided within a 60-day period prior to the expiry of the certificate. A ServiceNow ticket will be created for the subscriber based on enrollment information for all certificates reaching the 60-day window to expiration date. When the expiration is addressed either by a renewal or a request to the RA to revoke, it remains the responsibility of the subscriber to manage the corresponding ticket in ServiceNow.

Issuing CAs may renew a certificate if:

- The associated public key has not reached the end of its validity period, and
- The associated private key has not been compromised, and
- The subscriber and attributes remain consistent, and
- Re-verification of subscriber identity is not required by the applicable CPS.

4.6.2 Who May Request Renewal

For all CAs operating under this CP, the Pfizer PKI team shall be the only requester for renewal of CA certificates. The subscriber or the RA may request the renewal of a subscriber certificate.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

Not stipulation.

4.6.7 Notification of Certificate issuance by the CA to other entities

As per Section 4.4.3.

4.7 CERTIFICATE RE-KEY

Pfizer Enterprise PKI does not support certificate re-key. However, certificates may be reissued in accordance with Section 4.3

4.7.1 Circumstance for Certificate Re-key

Certificate re-keying will not be supported by any assurance level or policy.

4.7.2 Who May Request Certification of a New Public Key

Requests for certification of a new private/public key pair are considered a new enrollment request per requirements set in Section 4.2.

4.7.3 Processing Certificate Re-keying Requests

No stipulation.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

Pfizer does not offer certificate modification. Instead, based on the case, Pfizer RA will revoke the old certificate and issue a new certificate as a replacement. See Section 4.3

4.9 CERTIFICATE REVOCATION AND SUSPENSION

CAs operating under this CPS issue Certificate Revocation Lists (CRLs). Pfizer does not utilize certificate suspension for CAs, however, the use of Certificate suspension for subscriber certificates is permitted in reviewed cases by the Pfizer PKI team. A Certificate shall be revoked when the binding between the subject and the subject's public key defined within the Certificate is no longer considered valid. When this occurs, the associated certificate shall be revoked and placed on the CRL of the issuing CA. Revoked certificates are included on all new publications of the CRL until the certificates expires.

4.9.1 Circumstances for Revocation

CAs operating under this CPS shall revoke a Certificate within 24 hours if one or more of the following occurs:

- The Subscriber requests in writing that the CA revoke the Certificate.
- The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization.
- The CA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise.

CAs operating under this Policy shall revoke a Certificate within 24 hours and must revoke a Certificate within 5 days if one or more of the following occurs:

- The certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
- The CA obtains evidence that the certificate was misused.
- The CA is made aware that a subscriber has violated one or more of its material obligations under the Subscriber agreement.
- The CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name.
- The CA is made aware of a material change in the information contained in the certificate.
- The CA is made aware that the certificate was not issued in accordance with these requirements of the CP or this CPS.
- The CA determines or is made aware that any of the information appearing in the certificate is inaccurate.
- The CA's right to issue certificates under these requirements expires or is revoked or terminated, unless the CA has decided to continue maintaining the CRL repository.
- Revocation is required by this CPS or the CP.
- The CA is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key.

Pfizer may also revoke a Certificate if any of the following occur:

- Either the Subscriber's or Pfizer's obligations under this CPS or the relevant subscriber agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised.
- There has been a modification of the information pertaining to the Subscriber that is contained within the certificate.
- A personal identification number, private key or password has or is likely to become known to someone not authorized to use it or is being or is likely to be used in an unauthorized way.

- A Subscriber's digital Certificate has not been issued in accordance with the policies set out in this CPS.
- The subscriber has used the enrollment service contrary to law, rule or regulation, or Pfizer reasonably believes that the subscriber is using the certificate, directly or indirectly, to engage in illegal or fraudulent activity.
- The certificate, if not revoked, will compromise the trust status of Pfizer. Pfizer shall revoke a subordinate CA certificate within seven (7) days if one or more of the following occurs:
    - Pfizer obtains evidence that the subordinate CA's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the baseline requirements;
    - Pfizer obtains evidence that the subordinate CA certificate was misused.
    - Pfizer is made aware that the subordinate CA certificate was not issued in accordance with, or that subordinate CA has not complied with, the baseline requirements or this CPS.
    - Pfizer determines that any of the information appearing in the subordinate CA certificate is inaccurate or misleading.
    - Pfizer or subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate.
    - Pfizer's, or subordinate CA's, right to issue certificates under the baseline requirements expires or is revoked or terminated, unless Pfizer has made arrangements to continue maintaining the CRL repository.
    - Revocation is required by the CP or this CPS.
    - The subordinate CA Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities.
    - The subordinate CA Certificate, if not revoked, will compromise the trust status of Pfizer.

Whenever any of the above circumstances occur, the associated Certificate is revoked and placed on the CRL.

4.9.2 Who Can Request Revocation

Within the Pfizer Enterprise PKI, a CA may summarily revoke certificates within its domain. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in this CPS. A subscriber may request that its own certificate be revoked. Revocation can also be initiated at the discretion of the Pfizer PKI team.

4.9.3 Procedure for Revocation Request

The request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally, or manually signed by the requester). A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally, or manually signed by the requester).
All requests for revocation shall be submitted to DL-PRIVILEGED-ACCESS-MGMT@pfizer.com via an approved online process or in writing. The authenticated revocation request and any resulting actions taken by the Pfizer PKI team shall be recorded and retained as required. In the case where a certificate is revoked, justification for the revocation shall also be documented. When a subscriber certificate is revoked, the revocation shall be published in the appropriate CRL of the issuing CA.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CPS. Subscribers are required to immediately request revocation of any certificate thought to be compromised to the RA/CA.

4.9.5 Time within Which CA Will Process the Revocation Request

CAs will revoke certificates as quickly as practical upon receipt, authentication and verification of a proper revocation request. Revocation requests are processed up to two hours before the next full CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

Prior to relying on information listed in a certificate, a relying party shall confirm the validity of each certificate in the certificate path in accordance with IETF PKIX standards, including checking for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each certificate in the chain.

The matter of how often new revocation data should be obtained is a determination to be made by the relying party. If it is temporarily infeasible to obtain Revocation information, then the relying party shall either reject the use of the certificate or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this CPS. Such use may occasionally be necessary to meet urgent operational requirements. Relying parties shall verify a certificate's validity and revocation status prior to relying on the certificate.

4.9.7 CRL Issuance Frequency

Certificate Revocation lists (CRLs) are issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. Certificate status information is published no later than the next scheduled update and Certificate overlap is permitted. This will facilitate the local caching of Certificate status information for off-line or remote operation.

- Pfizer Root CAs will issue a full CRL at least once every 12 months with an overlap of up to 30 days.
- The "nextUpdate" time in the Root CA CRL will be no later than 12 months and 30 days after issuance time.
- Pfizer CAs that issue Certificates to Subscribers and/or operate on-line will issue a full CRL at least once every 10 days with an overlap of up to three days.
- The "nextUpdate" time in the Issuing CA CRL will be no later than 13 days after issuance time.
- Delta CRLs are published every 8 hours for CA 3, CA4, CA5 and CA6, All other CAs do not publish Delta CRLs
- Circumstances related to emergency CRL issuance are specified in section 4.9.12.

4.9.8 Maximum Latency for CRLs

The on-line Issuing CA CRLs are published within 10 minutes of generation and no later than the time specified in the next Update field of the previously issued CRL.

The Off-line Root CA CRLs are published within 8 hours of generation and no later than the time specified in the next Update field of the previously issued CRL.

4.9.9 On-Line Revocation/Status Checking Availability

No stipulation

4.9.10 On-Line Revocation Checking Requirements

No stipulation

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related to Key Compromise

When a CA certificate is revoked, a CRL must be generated and published within 24 hours of notifying subscribers and relying parties. No additional stipulation for subscriber certificates.

In the event of a SubCA or Issuing CA certificate revocation, the Pfizer Root CA shall generate and publish a new CRL immediately.

4.9.13 Circumstances for Suspension

For all certificates suspension is not permitted. This includes subscriber certificates.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 CERTIFICATE STATUS SERVICES

See Section 4.9.

4.10.1 Operational Characteristics

All CAs shall make certificate status information available via CRLs. CRLs are made available by using standards-based protocols. These protocols include:

- HTTP to retrieve CRL data.
- HTTP to retrieve CA certificates for chain building.
- LDAP following HTTP check for Active Directory user certificates.

4.10.2 Service Availability

CRL publication servers (CDPs) are available on a 24x7 basis, with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.5% annually. Load balancing architecture is designed for maximum High Availability of CRLs. The CDP servers publish CRL updates immediately to sixteen servers around the world.

Relying parties are bound to their obligations and the stipulations of this CPS irrespective of the availability of the certificate status service.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Certificates that have expired prior to or upon end of subscription are not required to be revoked.

4.12 Key Escrow and Recovery

This CPS requires keys associated with certificates used for non-repudiation will never be archived or escrowed.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No Stipulation

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

Commented [SB1]: I have reached out to Erick Cerrada for any report or statements of security controls regarding our presence in their AWS cloud environment. I would add this to an Appendix in this CPS and the CP

The following physical security controls will be in place prior to initial operation of the Pfizer Enterprise PKI.

5.1.1 Site Location and Construction

The location and construction of the facility housing Pfizer Enterprise PKI equipment is consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

The facility housing the PKI equipment provides a physically protected environment with controls to deter, detect and prevent unauthorized use of and disclosure of sensitive information. Pfizer Enterprise PKI equipment operating in a datacenter, strong safes, and cloud environment to support business continuity and disaster recovery should have equivalent physical security controls as the primary locations. Disaster recovery facilities are located at geographically disparate locations so operations can be resumed if the primary location is disabled.

5.1.2 Physical Access

The site locations of the CAs compliant with this CPS have been designed and implemented to meet the requirements specified in the CP and are both manually and electronically monitored for unauthorized intrusion.

Cryptographic and operational functions are housed in a facility which is classified as a secure Pfizer or Pfizer designated third party data center, strong safe or cloud environment. The CA equipment is protected from unauthorized access while the cryptographic module is connected and activated. This includes Pfizer Enterprise PKI hardware security modules (HSM) which like the Root CAs, reside only in physical premises.

Physical access controls have been established to reduce the risk of equipment tampering when the cryptographic module is not installed and activated. Cryptographic smartcards are protected against theft, loss, and unauthorized use at all times. The PINs and passwords for operating HSMs are securely protected by the cardholders or operation staff or securely protected by approved methods defined by Pfizer's security policies.

5.1.3 Power and Air Conditioning

The CAs operating under this CPS have sufficient power to finish any pending actions and record the state of the equipment before lack of power or air conditioning causes a shutdown. The site also has redundant power and generator backup to assist with keeping the CA available as long as appropriate.

5.1.4 Water Exposures

The secure facility of CA equipment is constructed and equipped, and procedures is implemented, to prevent floods or other damaging exposure to water.

5.1.5 Fire Prevention & Protection

The secure facility of CA equipment constructed and equipped; and procedures implemented; to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures meet all local applicable safety regulations.

5.1.6 Media Storage

CA media is stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive, or backup information is duplicated and stored in safes in ta location separate from the CAs and is protected from unauthorized access.

5.1.7 Waste Disposal

Sensitive waste material (paper, media, or any other waste) is disposed of in a secure fashion to prevent the unauthorized use of, access to, or disclosure of waste containing confidential/private information. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 Off-Site backup

Backups of critical system data or any other sensitive information, including audit data is maintained in a secure off-site facility. Backups that consist of enough information to reconstitute PKI systems are sent on a periodic basis to an offsite backup location with physical security controls commensurate with the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The primary trusted roles defined in this Policy are:

- CA Administrator
- Registration Administrator
- System Administrator
- PKI Key Managers
- CA Event Monitor
- Security Auditor

Individual personnel are specifically designated to assume these four roles as defined below. These six roles are employed at the Root CA, CA, Issuing CA (identified in Certificates as an authoritative source for revocation

information) and RA in locations as appropriate. Additional role creation for the purpose of role separation is permitted (e.g., new role of Template Manager to configure certificate templates with Administrator limited to publishing the templates). Separation of these duties is required for critical CA functions to prevent one person from maliciously using a CA system without detection.

The most sensitive tasks, such as access to and management of the CA's cryptographic module and associated key material require multiple trusted persons. Every task that requires a multiple control requires 2 of 6 administrators.

CAs have a verification process that provides an oversight of all activities performed by privileged CA role holders. Those roles are those (but are not limited to) that can issue Certificates, generate keys, and administer the CA configuration settings.

A list of personnel appointed to trusted roles is maintained and reviewed annually.

5.2.1.1 CA Administrators

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. Administrators do not issue certificates to subscribers.

Only the CA Administrator also performs all System Administrator/System Engineer roles on any offline Root CA.

5.2.1.2 Activation Card Holders

Activation card holders maintain an ACS and/or OCS smart card for use in signing ceremonies where the CA private key is accessed on the accompanying HSM, These roles are further detailed in Section 6.2

5.2.1.3 Registration Administrators – CMS, RA, Validation and Vetting Personnel

The Registration Administrator role is responsible for issuing and revoking Certificates, including enrollment, identity verification, and compliance with required issuance and revocation steps such as managing the certificate request queue and completing certificate approval checklists as identity vetting tasks are successfully completed.

5.2.1.4 System Administrators/ System Engineers (Operator)

The System Administrator installs and configures system hardware. The system administrator also manages and monitors online CA, CMS (Certificate Management System) and RA system updates with software patches and other maintenance needed for system stability and recoverability.

5.2.1.5 Security Auditor

The auditor role is independent and does not act in any other trusted role. Internal auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if Root CA, Issuer CA, or RA is operating in accordance with this CPS.

5.2.1.6 PKI Key Managers

The PKI Key Managers are CA Event Principals vetted and provided strong safe access to access cards and the accompanying passwords for a quorum for the successful access to an HSM and Root CA in a CA ceremony event. Passwords are split and kept in secure locked safes in a secure room requiring two administrators for entry.

5.2.1.7 CA Event Monitor

The CA Event Monitor role is responsible for the recording and direction the agenda of a PKI Ceremony. This role is not combined with any other role. This role does not handle or manage any components, passwords, combinations, TEB bag or safe contents.

5.2.2 Number of Persons Required per Task

One person is not allowed to act alone to completely manage a CA component server. Mechanisms such as multiple keys are in place to prevent this from occurring. Along with multiple keys, where possible, roles are separated amongst individuals.

Two or more persons are required for the following tasks:

- CA key generation
- CA signing key activation.
- CA private key backup.

Where multiparty control is required, at least one of the participants shall be an PKI Administrator. All participants must serve in a trusted role as defined in section 5.2.1. The security auditor trust role does not serve in any other trusted role.

5.2.3 Identification and Authorization for Each Role

All CA personnel will identify and authenticate themselves before being permitted to perform any actions set forth in the section 5.2.1 for that role.

5.2.4 Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

- Those performing authorization functions such as the verification of information in Certificate applications and approvals of Certificate applications and Revocation requests,
- Those performing backups, recording, and record keeping functions.
- Those performing audit, review, oversight, or reconciliation functions; and
- Those performing duties related to CA and HSM key management or CA and HSM administration.

5.3 PERSONNEL CONTROLS

Personnel granted privileged CA and RA roles must meet Pfizer's personnel security requirements. All CA personnel receive appropriate training with respect to their duties.

5.3.1 Qualifications, Experience and Clearance Requirements

All persons filling trusted roles are selected based on loyalty, trustworthiness, and integrity.

5.3.2 Background Check Procedures

The Pfizer Enterprise PKI enforces appropriate personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of its personnel.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA or RA receive comprehensive training. Training shall be conducted in the following areas:

- PKI principles, concepts, application, and operations

- CA (or RA) security principles and mechanisms.
- All PKI software versions in use on the CA (or RA) system.
- All PKI duties they are expected to perform.
- Hardware security module operations.
- Standard and evolving cryptographic practices
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

All individuals responsible for PKI roles are made aware of changes in the CA operation. Any significant change to the operations will have a training (awareness) plan, and the execution of such plan is documented. Documentation is maintained identifying all personnel who received training, and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

For any deliberate violation of trust for persons in a trusted position as defined in this CPS, the person at a minimum must be removed from that position of trust.

5.3.7 Independent Contractor Requirements

Contractors assuming trusted roles as outlined in this CPS will pass the same background checks and training requirements as Pfizer employees and are subject to the duties and requirements described in this section. They are also subject to sanctions stated in section 5.3.6.

5.3.8 Documentation Supplied to Personnel

Pfizer Enterprise PKI personnel will be provided this CPS, the CP and other technical and operational documentation needed to maintain the integrity of Pfizer Enterprise PKI operations. They are also provided with Pfizer Enterprise PKI procedures and other documentation relevant to their job functions in accordance with this CPS.

5.4 AUDIT LOGGING PROCEDURES

Audit log files are generated for events related to the security of the Pfizer Enterprise PKI.

5.4.1 Types of events

All security events related to physical and logical access, configuration changes, key generation and usage, Certificates creation, movement of removeable media, and any other events that may be required for auditing purposes are recorded.

CA, RA, and Certificate Lifecycle Management Events:

- CA Root signing key functions, including key generation, backup, recovery, and destruction.
- Subscriber certificate lifecycle management, including successful and unsuccessful certificate applications, Certificate issuances, Certificate re-issuances and Certificate renewals.
- Subscriber Certificate Revocation requests, including Revocation reason.
- Subscriber changes of affiliation that would invalidate the validity of an existing Certificate.
- CRL updates, generations, and issuances
- Custody of keys and of devices and media holding keys

- Compromise of a private key

Security Related Events:

- System downtime, software crashes and hardware failures
- CA system actions performed by Pfizer personnel, including software updates, hardware replacements and upgrades.
- Cryptographic HSM events, such as usage, de-installation, service or repair and retirement
- Successful and unsuccessful Pfizer Enterprise PKI access attempts
- Secure CA facility entry and exit.
- Adjustment to system clock

All logs include the following elements:

- Date and time of entry.
- Method of entry
- Source of entry
- Identity of entity making log entry

A message from any source requesting an action by the CA is an auditable event; the message must include the message date and time, source, destination, and contents. Procedures specifying integrity controls, event record lifetime and event record access shall be implemented and maintained.

5.4.2 Frequency of Processing Log

Logs are reviewed only when there is cause for review or for scheduled audits. Audits of the PKI logs shall occur minimally once a year.

5.4.3 Retention Period for Audit Log

Audit logs are kept for a period of three years or longer if required Pfizer's corporate retention policy or by law. Logs containing issuance and other certificate lifecycle events are kept as long as the certificate lifetime. At minimum, audit logs are retained until they are reviewed.

5.4.4 Protection of Audit Log

Audit logs are protected from unauthorized viewing, modification, deletion, or other tampering using a combination of physical and logical security access controls.

Procedures are implemented to protect archived data from deletion or destruction before the end of the security audit data retention period. Security audit data is moved to a safe, secure storage location separate from the location where the data was generated.

Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution, or destruction.

5.4.5 Audit Log Backup Procedures

Audit logs are backed up on a periodic basis in accordance with business practices.

5.4.6 Audit Collection System (Internal Vs. External)

The audit log collection system may or may not be external to the CA system. Automated audit processes are invoked at system or application startup and cease only at system or application shutdown. Audit collection systems are configured such that security audit data is protected against loss.

Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operation is suspended until the problem has been remedied.

5.4.7 Notification to Event-Causing Subject

No stipulation

5.4.8 Vulnerability Assessments

The CA will perform routine self-assessments of security controls. Occasional pen-testing and security testing of CA health and production will be performed and reported on.

5.5 *Records Archival*

5.5.1 Types of Records Archived

CA archive records are sufficiently detailed to determine the proper operation of the CA and the validity of any Certificate (including those revoked or expired) issued by the CA.

At a minimum, the following records are archived:

- Audit data, as specified in Section 5.4
- Data related to Certificate requests, verifications, issuances, and Revocations.
- CA policies, procedures, entity agreements, compliance records,
- Cryptographic device and key life cycle information
- Systems management and change control activities.

5.5.2 Retention Period for Archive

Archive records are kept for a minimum 10 years and 6 months: this corresponds with the maximum key validity of the online/issuing CAs plus 6 months.

5.5.3 Protection of Archive

Only authorized individuals by the Pfizer Engineering PKI team are permitted to add or delete from the archive. Archive media is stored in a safe, secure storage facility separate from the production CA location.

5.5.4 Archive Backup Procedures

Adequate backup procedures are in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a feasible period of time.

5.5.5 Requirements for Time-stamping of Records

All documents archived are marked with the date of their creation or execution.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain & Verify Archive Information

Only authorized CA personnel have access to primary and backup archives. The CA may, at its own discretion, release specific archived information, following a formal request from a Subscriber, a relying party, or an authorized agent thereof.

5.6 KEY CHANGEOVER

Toward the end of each private key's lifetime, a new CA signing key pair shall be generated. Once a new private signature key has been generated, only the new key will be used to sign CA and subscriber certificates. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in this CPS.

The CA's signing key has a validity period as described in section 6.3.2.

When the subCA or Root CA key pair is changed; from that time on, only the new key pair will be used for certificate signing purposes. The older, but still valid, public key will be available to verify old signatures until all the Certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that cover certificates signed with that private key, then the old private key will be retained and protected.

Automatic key changeover is not supported; therefore, a new certificate request shall be required. All such requests are processed in the same manner as the initial application.

5.7 COMPROMISE OR DISASTER RECOVERY

The operations of the Pfizer Enterprise PKI are included in and complies with Pfizer's Disaster Recovery planning. Any compromise of subscriber keys as a result of a disaster will result in the immediate revocation of the associated certificates.

5.7.1 Incident and Compromise Handling procedures

All incidents (including compromises), both suspected and actual, shall be reported to the Security Operations and Pfizer Enterprise PKI teams.

If the CA key is suspected to be compromised, the procedures outlined in section 5.7.3 are followed. Otherwise, alternate actions may be taken such as rebuilding systems and revoking end entity certificates. These procedures are in place to ensure that:

- A consistent response to incidents happening to Pfizer's assets.
- Incidents are detected, reported, and logged.
- Clear roles and responsibilities are defined.

The process also enables incidents to be analyzed in a way as to identify possible causes such that any weaknesses in Pfizer Enterprise PKI's processes may be addressed. Such plans are revised and updated as required at least once a year.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

If Pfizer determines that its computing resources, software, or data operations have been compromised, Pfizer will investigate the extent of the compromise and the risk presented to affected parties. Depending on the extent of the compromise, Pfizer Enterprise PKI may revoke affected certificates, to revoke entity keys, to provide new public keys to users, and to recertify subjects.

5.7.3 Entity Private Key Compromise Procedures

If Pfizer Enterprise PKI discovers or has reason to believe that a CA private key has been compromised, the following actions shall be taken:

- The Security Operations team is notified – Email: SecOps@Pfizer.com
- Immediately cease using the compromised certificate.
- Revoke the certificate and publish the serial number on the appropriate CRL and publish CRL to repositories.

- Revoke all certificates signed with the private key that corresponds to the public key listed in the certificate.
- Take reasonable steps to notify participants to cease using any certificates that are linked to the revoked certificate in question.

5.7.4 Business Continuity Capabilities After a Disaster

The CA has in place an appropriate contingency, continuity and disaster recovery plan that is capable of resuming services in accordance with this CPS. If CA equipment is damaged or rendered inoperative, but CA signature keys are not destroyed, CA operations will be reestablished, giving priority to the ability to generate certificate status information.

Pfizer Enterprise PKI systems are redundantly configured at its primary facility and are mirrored at a separate geographically diverse location for failover in the event of a disaster.

5.8 CA Termination

In the event of a CA or RA termination, Pfizer Enterprise PKI will provide as much advance notice as circumstance permits to relying parties prior to the termination. The CA will preserve relevant records for a period of time deemed fit for functional and legal purposes. See section 5.4.3

Before a CA terminates its services, the CA will:

- Make all reasonable efforts to inform subscribers and cross-certifying CAs.
- Make knowledge of its termination widely available
- Cease issuing certificates.
- CA operation will continue for 180 days, excluding issuance of new certificates.
- After the 180-day period:
    - All remaining issued certificates that are still valid are revoked after verification of issuance by another CA.
    - A CRL is published.
    - CA certificates are revoked, and a corresponding CRL will be published.
    - All copies of private keys will be destroyed.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is generated in a secure environment using FIPS 140-2 Level 3 validated cryptographic modules and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys.

CA keys are generated in a key generation ceremony as specified in this CPS.

Auditable evidence is created during the key generation process proving that the CPS was followed, and role separation enforced during the process. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining signed and documented record

of the key generation. All key generation and CA operation ceremonies are followed and witnessed in accordance with this CPS.

6.1.1.1 CA Key Pair Generation

CA key pairs are generated in a secure environment, in Pfizer Enterprise PKI facilities, and comply with key generation and management practices described in this Certificate practices statement. Hardware security modules used in the generation and storage of private keys are at FIPS 140-2 Level 3.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key generation is normally generated and secured by the subscriber. Subscriber key-pair generation may be performed by the RA. If the CA or RA generates Subscriber key pairs, the requirements for key pair delivery specified in section 6.1.2 will also be met.

6.1.2 Private Key Delivery to Subscriber

If Subscribers have generated their own key pairs, there is no need to deliver private keys.

The distribution of key pairs generated by a CA or RA shall be delivered using KiteWorks for secure transmission of the key files to prevent the loss, disclosure, modification, or unauthorized use of the private keys on them. Delivery will be to no more than one person. The RA shall maintain a record of the subscriber acknowledgment of receipt of the token.

- The subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the activation data are provided to the correct subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the RA, the public key and private key must be delivered as a .pfx file or separately as a .cer and .ley file. These are delivered to the certificate issuer in such a way that the issuer can determine:

- The public key has not been modified in transit; and
- The sender possesses the private key corresponding to the transferred public key.

6.1.4 CA Public Key Delivery to Relying Parties

CA public keys are distributed in CA certificates and can also be obtained from the Pfizer PKI Repository in .pem and .crt formats.

6.1.5 Key Sizes

The following requirements pertaining to key sizes must be met:

- The root CA will have an RSA key with a minimum size of 4096 bits.
- All issuing CAs and other subordinate CAs must have an RSA key with a minimum size of 4096 bits.
- Subscriber certificates must have an RSA key with a minimum size of 2048 bits.
- Code signing key size shall be a minimum of 4096 bits.
- Minimum secure hashing algorithm will be SHA2 256 bit for all CAs and subscriber certificates.

Pfizer Enterprise PKI may require higher bit keys at its sole discretion.

6.1.6 Public Key Parameter Generation and Quality Checking

Pfizer CA keys are generated within a FIPS 140-2 Level 3 certified HSM.

6.1.7 Key Usage (X.509 v3 field)

The use of a specific key is constrained by the keyUsage extension in the X.509 certificate.

Public keys that are bound into CA certificates are used for signing certificates and status information (e.g., CRLs). The following table shows the specific keyUsage extension settings for CA certificates and specifies that all CA certificates shall:

- Include a keyUsage extension.
- Set the criticality of the keyUsage extension to TRUE.
- Assert the digitalSignature bit, keyCertSign bit and the cRLSign bit in the key usage extension.

Specific keyUsage extension settings for end entity Certificates are specified in this CPS. See section 7.1.1 for base certificates and section 7.1.2 for certificate extensions.

6.2 *Private Key Protection and Cryptographic Module Engineering Controls*

Pfizer Enterprise PKI has implemented a combination of physical, logical, and procedural controls to ensure the security of Pfizer CA private keys. Logical and procedural controls are described in the Section 6.5 and Section 6.6. Local access controls are described in the Section 5.1.2. Subscribers are required to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Modules and Standards

The Pfizer Enterprise PKI root and subordinate CAs use key pairs generated in nCipher Hardware Security Modules (HSM). These Cryptographic Modules are rated at FIPS 140-2 Level 3 or higher.

6.2.2 Private Key (k of n) Multi-Person Control

The Pfizer Enterprise PKI Root CA's private key is protected using a 'k of n' quorum with the minimum quorum of two for both the Administrator Control Set (ACS) and the Operator Control Set (OCS) smart cards to maintain multiple-person control of the root CA.

CA signature keys are backed up under multi-person control. Access to CA signing keys backed up for disaster recovery are under multi-person control. The names of the parties used for multi-person control are maintained on a list that is made available for inspection during compliance audits. See Section 5.2.

6.2.3 Private Key Escrow

CA private keys are never escrowed.

6.2.4 Private Key Backup

Pfizer Enterprise PKI does not store backups of end-entity or RA private keys.

The CA private signature keys are backed up under the same multi-person control as the original signature key. At least one copy of the private signature key is stored off-site. All copies of the CA private signature key are accounted for and protected in the same manner as the original.

6.2.5 Private Key Archival

Pfizer Enterprise PKI does not archive private keys.

6.2.6 Private Key Transfer To or From a Cryptographic Module

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in section 6.2.4. At no time does the CA private key exist in plaintext outside the cryptographic module. All other keys are generated by and in a cryptographic module.

If a private key is to be transported from one cryptographic module to another, the private key is encrypted during transport; private keys never exist in plaintext outside the cryptographic module boundary and will always have two-person access.

6.2.7 Private Key Storage on Cryptographic Module

Online CA private keys are stored in cryptographic modules at FIPS 140-2 Level 3. Root CA and Issuing CA keys are generated, stored in encrypted form, and backed up on offline cryptographic modules as described in sections 6.2.2, 6.2.4 and 6.2.6 above.

6.2.8 Private Key Activation

Private keys are activated according to the specifications of the cryptographic manufacturer. Activation data entry is protected from disclosure. All access is authenticated and logged. All access is authenticated to the cryptographic module before the activation of the private key.

6.2.9 Private Key Deactivation

Pfizer Enterprise PKI CA keys are deactivated upon system shutdown or stoppage of the CA services. Cryptographic modules that have been activated are not available to unauthorized access. After use, the cryptographic module is deactivated. CA cryptographic modules are removed and stored in a secure container when not in use.

6.2.10 Private Key Destruction

CA keys will be destroyed when they are no longer required. Individuals in trusted roles will destroy CA and RA private signature keys when they are no longer needed. Subscribers will destroy their private signature keys when they are no longer needed or when the certificates to which they correspond expire or are revoked.

Physical destruction of HSM hardware is not required.

6.2.11 Cryptographic Module Rating

See section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CAs public keys are archived as part of the certificate archive process. See Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The usage periods for public and private keys are:

- Pfizer Enterprise PKI Root CA keys, as 4096-bit RSA keys, are valid for no longer than twenty (20) years or equivalent key size approved by NIST or by Pfizer's Security Policies.

- Pfizer Enterprise PKI Issuing CA keys, as 4096-bit RSA keys, are valid for no longer than ten (10) years or equivalent key size approved by NIST or by Pfizer's Security Policies.
- Pfizer Enterprise PKI Subscriber keys, as 2048-bit RSA keys, are valid for no longer than one (1) years or equivalent key size approved by NIST or by Pfizer's Security Policies.
- All Certificates signed by a specific CA key pair will expire before the end of the that CA's key pair usage period.

Pfizer Enterprise PKI may voluntarily retire its CA private keys before the periods listed above to accommodate key changeover processes.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data is generated in accordance with the specifications of the HSM. This hardware is certified by FIPS 140-2 to at least Level 3.

6.4.2 Activation Data Protection

Data used to unlock private keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms. These include locked safe storage at designated sites. Locations of storage are at designated sites and follow this CPS.

Activation data may be:

- Biometric in nature
- Recorded and secured at the level of assurance associated with the cryptographic module and is not stored with the cryptographic module.

6.4.3 Other Aspects of Activation Data

Tokens and split passphrases are stored in these secure locations and secured as same level as that of the associated cryptographic module and not stored with the cryptographic module.

6.5 Computer Security Controls

Pfizer Enterprise PKI performs all CA functions using systems that meet the requirements of Pfizer's corporate standards. All Issuing CA system information is protected from unauthorized access either through protections provided by its operating system, or through a combination of operating system, physical safeguards, and network safeguards.

6.5.1 Specific Computer Security Technical Requirements

Computer security controls are required to ensure CA/RA operations are performed as specified in this CPS.

The following computer security functions pertaining to the Pfizer Enterprise PKI may be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Require authenticated logins.
- Provide discretionary access control.
- Provide a security audit capability.
- Enforce access control for CA services and PKI roles.
- Require identification and authentication of PKI roles and associated identities.

- Prohibit object reuse or require separation for CA random access memory.
- Require use of cryptography for session communication and database security
- Archive CA history and audit data.
- Require a trusted path for identification of PKI roles and associated identities.
- Require a recovery mechanism for keys and the CA system.
- Enforce domain integrity boundaries for security-critical processes.

For other CAs operating under this CPS, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts include the following functionality:

- Authenticate the identity of users before permitting access to the system or applications.
- Manage privileges of users to limit users to their assigned roles.
- Generate and archive audit records for all transactions; (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications.
- Manage privileges of users to limit users to their assigned roles.
- Generate and archive audit records for all transactions.
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The CA uses software that has been designed and developed by a formal methodology and supported by Pfizer. Hardware and software procured to operate the Pfizer Enterprise PKI is purchased in a fashion to reduce the likelihood that any component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).

Hardware and software developed specifically for the Pfizer Enterprise PKI is developed in a controlled environment, and the development process is defined and documented. Security requirements were achieved through a combination of software verification and validation. The foregoing requirement does not apply to commercial off-the-shelf hardware or software.

All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the Pfizer Enterprise PKI physical location.

The hardware and software shall be dedicated to meeting the obligations of the Pfizer Enterprise PKI in accordance with this CPS. There shall be no other applications, hardware devices, network connections, or component software installed, which are not part of the Pfizer Enterprise PKI operation.

Only applications required to perform the operation of the CA are obtained from sources authorized by local policy. CA and RA hardware and software are scanned for malicious code on first use and periodically thereafter.

Hardware and software updates are purchased or developed in the same manner as original equipment and installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the CA and RA shall be documented and controlled. A change management methodology is used for installation and ongoing maintenance of CA and RA systems. The Issuer CA's change control processes include procedures to detect unauthorized modification to the Issuer CA's systems and data entries that are processed, logged, and tracked for any security-related changes to CA systems, firewalls, routers, software, and other access controls.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The Pfizer Enterprise PKI Root CA will never be connected to any network at any time. Although never connected to a network, the Root CA private keys are kept offline and accessed only when brought online (powered on and connected to an offline cryptographic module FIPS 140-2 Level 3) to process subordinate CA requests or to publish a new CRL. All ports, including wireless ports, excepting connecting port to the HSM are disabled. CD-ROM and NICs are disabled, and no cables are ever connected to the Root CA. Offline means OFFLINE.

Pfizer Enterprise PKI performs all Issuing CA functions using networks secured in accordance with Pfizer's security policy to prevent unauthorized access and other malicious activities. Pfizer's Enterprise PKI security policy is to block all ports and protocols and open only ports necessary to enable issuing CA functions.

6.8 Time Stamping

All CA and RA components regularly synchronize with a time service inside Pfizer network. Time derived from this service shall be used for establishing the time of:

- Initial validity type of an issued certificate
- Revocation of an issued certificate
- Posting of CRL updates

The time within three minutes shall be manually set on the Pfizer Enterprise PKI Root CA upon start based on network time service inside Pfizer network. Clock adjustments are an auditable event, see Section 5.4.1. Time verification and adjust shall be performed at every operation of the Root CA.

7 Certificate and CRL Profiles

7.1 Certificate Profile

CA Certificates within the Pfizer Enterprise PKI shall be X.509 Version 3 and shall conform to RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, dated May 2008 and RFC 6818 - Updates to the Internet X.509 Public key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013.

At a minimum, the following basic fields and prescribed field attributes are utilized within the CA Certificate profile. These include:

- Version number of the Certificate
- The Certificate's identifying serial number.

- The signature algorithm used to sign the Certificate.
- The issuer's distinguished name
- The validity period of the Certificate
- The subject's distinguished name
- Information about the subject's private key
- Extensions as defined in this CPS.

A certificate profile contains fields as specified below:

- Key usage extension field (section 6.1.7).
- Extension criticality field (section 7.1.9).
- Basic constraints extension (section 7.1.7).

SHA 2 End Entity Certificate Profile

End-user Subscriber Certificates shall be X.509 Version 3.

Field	Description
Version	V3
Serial Number	Positive integer uniquely assigned by CA that exhibits at least eight bytes of entropy
Signature Algorithm Identifier	SHA384
Issuer	CN = <Pfizer Issuing CA> O = Pfizer, Inc C = US
Valid From	Date and time of certificate issuance. Time from NTP with 10-minute skew showing validity 10 minutes prior
Valid To	Date and time of Certificate expiration. Time from NTP Maximum Certificate validity period is 12 months from issuance for Fully Qualified Domain Names and public IP Address certificates.
Subject	CN = <DN> OU = <set by Subscriber> O = Pfizer, Inc L= Groton S = Connecticut C = US
Public Key	RSA (2048)
Subject Alternate Name	<DNS Name(s)>
Certificate Policies	1.3.6.1.4.1.6385.509.x
Authority Information Access	[1]Authority Info Access Alternative Name: URL= http://pki.pfizer.com/<"RootCA name">.crt [2]Authority Info Access

Field	Description
Basic Constraints	SubjectType=End Entity Path Length Constraint=None
Key Usage	Digital Signature, Key Encipherment, Data Encipherment
Extended Key Usage	id-kp-serverAuth id-kp-clientAuth id-kp-codeSigning

Less stringent exceptions to the given basic profile must be approved on a case-by-case basis by the Pfizer Enterprise PKI team based on a valid documented business case.

7.1.1 Version Number(s)

All Pfizer Enterprise PKI CAs issue X.509 Version 3 compliant Certificates.

7.1.2 Certificate Extensions

The Pfizer Enterprise PKI supports and uses the following X.509 v3 Certificate extensions:

- Root CA Certificate extensions:
  - Basic Constraints: critical, CA:TRUE
  - Key Usage: critical, CRL Sign, key Cert Sign
  - Subject key Identifier
  - Authority key Identifier
  - CRL Distribution Points
- Issuing CA Certificate extensions:
  - Basic Constraints: critical, CA:TRUE,
  - PathLength=0
  - Key Usage: critical, CRL Sign, key Cert Sign
  - Subject Key Identifier
  - Authority Key Identifier
  - CRL Distribution Points
- End entity Certificate extensions for users:
  - Basic Constraints: critical, CA:FALSE
  - Key Usage: critical, Digital Signature, Key Encipherment, Data Encipherment
  - Extended Key Usage
  - CRL Distribution Points
  - Authority Key Identifier
  - Subject key Identifier
  - Certificate Policies
  - Subject Alternative Name: UPN

7.1.2.1 Key Usage

The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. This extension shall appear in certificates that contain public keys that

are used to validate digital signatures on other public key certificates or CRLs. When this extension appears, it may be marked critical.

7.1.2.2 Certificate Policies Extension

The Certificate Policies extension of Pfizer Enterprise PKI x.509 Version 3 Certificates includes a policy identifier, which indicates a certificate policy asserting Pfizer CA's adherence to and compliance with CA/Browser Forum's SSL Baseline Requirements.

7.1.2.3 Subject Alternative Names

The subjectAltName extension of Pfizer Enterprise PKI x.509 Version 3 Certificates is utilized. This extension shall contain at least one entry containing the Common Name. Additional entries shall be either a dNSName containing the Fully-Qualified Domain Name or an IP Address containing the IP address of a server.

7.1.2.4 Basic Constraints

BasicConstraints extension shall not be present in Pfizer CA end-user subscriber certificates.

7.1.2.5 Extended Key Usage

Pfizer CA shall make use of the ExtendedKeyUsage extension for certain types of X.509 Version 3 certificates. This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension.

7.1.2.6 CRL Distribution Points

Pfizer Enterprise PKI X.509 Version 3 end user subscriber certificates include the CRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the certificate's status. The criticality field of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

Most Pfizer Enterprise PKI X.509 Version 3 end user subscriber certificates include the authority key identifier extension to provide a means of identifying the public key corresponding to the private key used to sign the respective certificate. When used, the criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

Most Pfizer Enterprise PKI X.509 Version 3 end user subscriber certificates include the subject key identifier extension to provide a means of identifying the occurrence of a particular public key. When used, the criticality field of this extension is set to FALSE.

7.1.2.9 Wildcard Certificates

The Pfizer CA shall not issue wildcard certificates. Any exceptions to this requirement shall be approved on a case-by-case basis by the CA based on a valid documented business case and implications to the security of the Pfizer Enterprise PKI.

7.1.3 Algorithm Object Identifiers

All certificates issued under this Certificate Policy will be signed using the hash algorithm sha384 – 2.16.840.1.101.3.4.2 from RFC 5754:

Sha384- joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2

Available for specific use cases is sha256 - 2.16.840.1.101.3.4.2 from RFC 5754

Sha384- joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1

7.1.4 Name Forms

The subject and issuer fields in Pfizer Enterprise PKI certificates issued under this CPS are populated with an X.500 distinguished name as specified in section 3.1.1.

Each certificate includes a unique serial number that is never reused. The Issuing CA shall restrict OU fields from containing Subscriber information that is not verified in accordance with Section 3.1

7.1.5 Name Constraints

The Pfizer CA may assert name constraints in CA certificates for restrictions to domains, EKU enrollment and certain template publications.

7.1.6 Certificate Policy Object Identifier

Pfizer uses policy OIDs under the arc:

1.3.6.1.4.1.6385.509

iso(1)
identified-organization(3)
dod(6)
internet(1)
private(4)
enterprise(1)
Pfizer(6385)
pki(509).

Certificate Profiles	OID
Pfizer Low Certificate Assurance	1.3.6.1.4.1.6385.509.2.1.1
Pfizer Medium Certificate Assurance	1.3.6.1.4.1.6385.509.2.1.2

Pfizer High Certificate Assurance	1.3.6.1.4.1.6385.509.2.1.3
Pfizer Smart Card High Assurance	1.3.6.1.4.1.6385.509.2.1.4
Pfizer Smart Card Assurance	1.3.6.1.4.1.6385.509.2.1.5
Pfizer Enterprise PKI CPS	1.3.6.1.4.1.6385.509.1.2
Pfizer Enterprise Certificate Policy (CP)	1.3.6.1.4.1.6385.509.1.1

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL PROFILE

7.2.1 Version Number(s)

Pfizer CA shall issue X.509 version 2 CRLs in accordance with RFC 5280. The CRL for any certificate issued by Pfizer Enterprise PKI may be found at the URL encoded within the CRLDP field of the Certificate itself.

The profile of the Pfizer Enterprise PKI CRL:

Field	Value
Issuer Signature Algorithm	sha-512WithRSAEncryption [1.2.840.113549.1.1.13]
Issuer Distinguished Name	Pfizer Enterprise PKI Issuing CA
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked Certificates, including the serial number and Revocation date
Issuer's Signature	[Signature]

7.2.2 CRL and CRL entry extensions

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the authority key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for Revocation

7.3 OCSP PROFILE

OCSP is not deployed in the Pfizer Enterprise PKI.

7.3.1 Version Numbers

No stipulation

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and Other Assessment

This CA is subject to Pfizer's Internal Audit following the requirements of the CPS.

8.1 Frequency or Circumstances of Assessment

CAs subject to this CPS will undergo a yearly assessment to determine compliance to this CPS and the Pfizer Enterprise PKI certificate policies.

8.2 Identity or Qualifications of Security Auditor

The security auditor does not act in any other trusted role. See Section 5.2.1.4. Auditors shall be an internal entity with proficiency in public key infrastructure technology, information security tools and techniques, security auditing.

8.3 Security Auditor's Relationship to Assessed Entity

The security auditor does not hold any another trusted role in the PKI managed under this CPS.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a Pfizer CA and its recognized RAs comply with all the requirements of the current versions of this CPS. All aspects of the CA/RA operation shall be subject to compliance audit inspections. These include, but are not limited to the following:

- Business Practices Disclosure, meaning:
  - The CA provides its services in accordance with its CPS.
- Key Lifecycle Management, meaning:
  - The CA maintains effective controls to provide reasonable assurance that the integrity of keys and certificates it manages is established and protected throughout their lifecycles.
- Certificate Lifecycle Management, meaning:
  - The CA maintains effective controls to provide reasonable assurance that subscriber information was properly authenticated for specific registration activities.
  - The CA maintains effective controls to provide reasonable assurance that subordinate CA certificate requests are accurate, authenticated, and approved.
- CA Environmental Control, meaning that:
  - The CA maintains effective controls to provide reasonable assurance that:
    - Logical and physical access to CA systems and data is restricted to authorized individuals.
    - The continuity of key and certificate management operations is maintained.
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

8.5 Actions Taken for Deficiencies

When the Security Auditor finds a discrepancy between the requirements or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions are performed:

- The security auditor shall note the discrepancy.
- The security auditor shall notify the parties identified in section 8.6 of the discrepancy.
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to Pfizer Corporate Information Security (CIS) and appropriate CA management authority.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Pfizer Enterprise PKI Engineering team may decide to:

- Temporarily halt operation of the CA or RA
- Revoke a certificate issued to the CA or RA
- Take other actions it deems appropriate.

8.6 Communication of Results

Results shall be communicated to the relevant governance teams determined by the Security Auditor

9 Other Business and Legal Matters

9.1 Fees

Pfizer CAs subject to this CPS will not charge for services at this time.

9.2 Financial Responsibility

No Stipulation.

9.3 Confidentiality of Business Information

CAs information not requiring protection may be made publicly available. Public access to organizational information is determined by the Pfizer Enterprise PKI administrators and relevant Pfizer policy. Certificate or certificate-related information will not be disclosed to any third-party except when:

- Authorized to do so by this CPS.
- Required to be disclosed by law or court order.

9.3.1 Scope of Confidential Information

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

- Private keys, whether held by subscribing customers (including Individuals representing subscribing customers), CAs, RAs, repositories must be held in the strictest confidence. Each party is responsible for keeping its own private key confidential and, after certificate issuance, no other party will have access to or be responsible for another's private key; Activation data used to access private keys or to gain access to the CA and HSM systems.

- All PKI documentation.
- Subscriber agreements.
- Certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- Business continuity, incident response, contingency, and disaster recovery plans.
- Other security practices used to protect the confidentiality, integrity, or availability of information.
- Information held by Pfizer as private information in accordance with Section 9.4.
- Audit logs and archive records.
- Internal tracks and records on the operations of Pfizer infrastructure, certificate management and enrollment services and data.
- Transaction records, financial audit records, external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS).

9.3.2 Information not Within the Scope of Confidential Information

PKI documentation, public keys, or CRLs made publicly available in the regular business of the Pfizer Enterprise PKI are not within scope of confidential information.

9.3.3 Responsibility to Protect Confidential Information

All personnel in trusted positions shall handle all confidential information in strict confidence in accordance with federal and state law as well as relevant Pfizer security policies.

9.4 PRIVACY OF PERSONAL INFORMATION

This section is subject to applicable privacy laws.

9.4.1 Privacy Plan

Subscribers identifying information is reasonably protected from unauthorized disclosure as set forth by the current Pfizer privacy policy.

9.4.2 Information Treated as Private

Information that is not contained in the public certificates is treated as private.

9.4.3 Information not Deemed Private

Private information does not mean to include certificates, CRLs, or their contents.

9.4.4 Responsibility to Protect Private Information

Recipients of private information shall secure it from unauthorized access and disclosure to third parties and shall comply with all applicable local privacy laws and Pfizer privacy policies.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CPS, the applicable privacy policy or by agreement, private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Pfizer Enterprise PKI is entitled to disclose confidential/private Information if, in good faith:

- Disclosure is necessary in response to subpoenas and search warrants.
- Disclosure is necessary in response to judicial, administrative, or other legal process.
- Disclosure is necessary in a discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

9.5 *Intellectual Property Rights*

Pfizer Enterprise PKI will not knowingly violate intellectual property rights held by others.

9.6 *Representations and Warranties*

The Pfizer Enterprise PKI Engineering team shall:

- Approve this CPS.
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all Certificates issued under this CPS.
- Revise this CPS to maintain the level of assurance and operational practicality.

9.6.1 CA Representations and Warranties

Pfizer CAs operating under this CPS shall warrant that their procedures are implemented in accordance with this CPS, and any Certificate issued that assert the policy OIDs identified in this CPS were issued in accordance with the stipulations of this CPS.

A Pfizer CA that issues certificates that assert a policy defined in the document shall conform to the stipulations of this document, including:

- Maintaining its operations in conformance to the stipulations of this CPS.
- Ensuring that registration information is accepted only from approved RAs operating under this CPS.
- Including only valid and appropriate information in certificates and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3.
- Operating or providing for the services of an on-line repository and informing the repository service provider of their obligations if applicable.
- There are no material misrepresentations of fact in the certificate known to or originating from the entities approving the certificate application or issuing the certificate.
- There are no errors in the information in the certificate that were introduced by the entities approving the certificate application or issuing the certificate because of a failure to exercise reasonable care in managing the certificate application or creating the certificate.
- Their certificates meet all material requirements of this CPS.
- Revocation services and use of a repository conform to all material requirements of this CPS.

9.6.2 RA Representations and Warranties

An RA that performs registration functions as described in this CPS complies with the stipulations of this CPS.

An RA supporting this policy conforms to the stipulations of this document, including:

- Maintaining its operations in conformance to the stipulations of the approved CPS.

- Including only valid and appropriate information in Certificates and maintaining evidence that due diligence was exercised in validating the information contained in the Certificates.
- Ensuring that obligations are imposed on Subscribers, in accordance with section 9.6.3, and Subscribers are informed of the consequences of not complying with those obligations.
- There are no material misrepresentations of fact in the certificate known to or originating from the entities approving the certificate application or issuing the certificate.
- There are no errors in the information in the certificate that were introduced by the entities approving the certificate application or issuing the certificate because of a failure to exercise reasonable care in managing the certificate application or creating the certificate.
- Their certificates meet all material requirements of this CPS.
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CPS in all material aspects.

9.6.3 Subscriber Representations and Warranties

A Subscriber shall:

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private key(s) at all times, in accordance with this CPS, as stipulated in their certificate acceptance agreements and local procedures. See Section3.2.3
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification shall be made directly or indirectly through mechanisms consistent with this CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s)
- Confirm the accuracy of certificate date prior to using the certificate.
- Promptly cease using a certificate and notify Pfizer Enterprise PKI if any certificate information changes, becomes misleading or there is any actual or suspected misuse or compromise of the private key associated with the certificate.
- Use the certificate only for authorized and legal purposes.

In all cases and for all types of Pfizer Enterprise PKI Certificates the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Pfizer Enterprise PKI of any such changes.

9.6.4 Relying Party Representations and Warranties

Subscribers will use the certificates for the purpose for which it was intended and check each certificate for validity. This CPS does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CPS mappings that the relying party may wish to employ in its determination.

9.6.5 Representation and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

CAs operating under this CPS may not disclaim any responsibilities described in this CPS.

9.8 INDEMNITIES

No stipulation

9.9 TERM AND TERMINATION

9.9.1 Term

This CPS is effective immediately upon publication.

9.9.2 Termination

Termination of this CPS is at the discretion of Pfizer Engineering PKI team.

9.9.3 Effect of Termination and Survival

The requirements of this CPS remain in effect through the end of the archive period for the last certificate issued from the Pfizer Enterprise PKI.

9.10 AMENDMENTS

9.10.1 Procedure for Amendment

The Pfizer Enterprise PKI Engineering team may amend this CPS. Amendments can be an update, revision, or modification to this CPS, and can be detailed in this CPS or in a separate document. Additionally, amendments supersede any designated or conflicting provisions of the amended version of the CPS. Amendments shall be published in the Pfizer PKI Repository.

9.10.2 Notification Mechanism and Period

Proposed changes to this CPS shall be distributed electronically to the members of the Pfizer Enterprise PKI. If the changes are not deemed substantial, the subscribers will be notified at the renewal.

9.10.3 Circumstances Under Which an OID Must be Changed

If a change in this CPS is determined by the Pfizer Enterprise PKI team to warrant a change in the currently specified OID for a particular type of certificate, then the revised version of this CPS will also contain a revised OID for that type of certificate.

9.11 DISPUTE RESOLUTION PROVISIONS

The Pfizer Enterprise PKI team shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this CPS.

9.12 COMPLIANCE WITH APPLICABLE LAW

This CPS shall be subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including but not limited to restrictions on exporting or importing software, hardware, or technical information. In delivering its PKI services Pfizer complies in all material respects with high-level international standards and the relevant law on electronic signatures and all other relevant legislation and regulation.

APPENDIX A: GLOSSARY

Active Directory Certificate Services (ADCS):
Active Directory® Certificate Services (AD CS) is an Identity and Access Control security technology that provides customizable services for creating and managing public key certificates used in software security systems that employ public key technologies.

Authority Information Access (AIA) is an X.509 certificate extension that contains CA certificate access information. Systems use the AIA location to retrieve a copy of the issuing CA's certificate to form a validation chain. This can point to an LDAP and an HTTP location.

Advanced Encryption Standard (AES): AES superseded the DES standard. It is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting data. It improved on DES by its ability to use 128-256-bit key sizes and as a symmetric-key algorithm can encrypt large amounts of data quickly. This is also applicable for key-archival to protect user private keys protected in transit to a CA.

Asymmetric Encryption:
Encryption system that uses a public-private key pair for encryption and decryption, as well as for digital signatures. Also known as a public-key algorithm. Common asymmetric algorithms are RSA, Diffie-Hellman, and ECDSA, and DSS/DSA. The public key is used to encrypt a message and the associated private key is used to decrypt the message. For example, Bob wants to send an encrypted message to Alice. Alice sends her public key to Bob who encrypts the message and sends it to Alice. Alice then decrypts the message with her private key. Helen who has been listening in and also has the public key (it is public, after all!) but she is unable to decrypt Bob's message since she doesn't have Alice's private key.

Certificate Revocation Lists (CRLs):
A list of Certificates which were issued by a given CA, but have since been revoked, and should therefore not be trusted. CRLs are published by the CA which originally issued the Certificates.

Certificate Policy (CP):
A document specifying the requirements and provisions which must be met by the participants in a given PKI. CPs are often used to establish a level of trust for the PKI in question.

Certification Authority (CA):
A trusted authority that binds a vetted name to a vetted key by signing a standardized data structure containing the name and key. This "standardized data structure" is called an "X.509 certificate," or more commonly a "digital certificate."

CA (Certification Authority) Hierarchy:
A certificate hierarchy is the functional design and placement of CA servers in a PKI infrastructure. Common examples are single, two-tier, and three-tier hierarchies. The CA certifies the identity of a certificate request, issues and validates certificates, and manages certificate revocation. It is also responsible for attesting to the identity of users, computers, and organizations. This encompasses both root CA and subordinate CAs. CA's may be operated by different entities and are configured to reflect the trust boundaries of their operators.

Certification Practices Statement (CPS):
A document stating the practices used in all aspects of operating a given CA within a given PKI. Certification practices statements are often used to show compliance with a governing CP.

Certificate Revocation List (CRL):
A published list of Certificates that have been revoked.

Certificate Status Server (CSS):
Identified in Certificates as the authoritative source for Revocation information. An example of a CSS is a CDP (CRL Distribution Point) server.

CRL Distribution Points (CDP):
A CDP is the place for the retrieval of the latest CA CRLs. This is usually a Lightweight Directory Access Protocol (LDAP) server for AD lookup or HTTP (web) server for a public URL.

Certificate AutoEnrollment:
AutoEnrollment is the capability to automatically enroll AD users and computers for certificates. This is accomplished by certificate template configuration and Active Directory group policy.
End Entity: Any non-CA party to whom an X.509 Certificate is issued. The end entity can be a person, computer, software application or device. This entity is sometimes called the "Certificate Subscriber."

Certificate Extensions
Shown in the certificate data, certificate extensions provide additional information about the certificate. Extensions include what the certificate can be used for, basic constraints, revocation locations, OSCP locations, details about the issuers' Signing Key, etc. An extension can be configured to specifically designate enforcement and use policies as well as key usage such as Code Signing, server and/or client authentication, and digital signing.

Certificate Chain
A certificate chain is a hierarchal collection of certificates where the root of trust is at the top of the PKI hierarchy. Trust is further gained by verifying that each certificate in the chain:

- Shows the validity period, including current date and time.
- Is not in the local Untrusted Certificate store.
- Shows that policies from the issuing CA and above are in place.

Certificate Stores
Certificate stores are a combination of logical groupings and physical storage. Common stores include Personal, Trusted Root Certification Authorities, Intermediate Certification Authorities, and Untrusted Certificates. These stores identify the descriptions and purposes of certificates found within. For example, the personal store will show the certificates issued to the local user or computer and associated with a private key. The Intermediate Certification Authorities store will contain subordinate CA certificates.

Certificate Template
Certificate templates define the format and content of a certificate. Configurations include enrollment permissions, renewals, certificate purpose, lifetime, key length, extensions, issuance requirements, etc. They exist in the certificate templates container of Active Directory. X.509 attribute extensions are used to define a template's structure.

CN – Common Name
The common name is the name of the End-Entity or subscriber in a certificate.

CNG/KSP – Cryptography API: Next Generation
Windows Cryptography API: Next Generation (CNG) (KSP = Key Storage Provider) and features support for Suite B algorithms, hardware security modules, and more. The CNG API replaces the CryptoAPI but is backward compatible with all its algorithms.

Code Signing
Code signing provides a digital signature to executable files (.exe), dynamic link libraries (.dll), ActiveX controls (.ocx), Microsoft Visual Basic documents (.vbd), Cabinet files (.cab), Java Archive files (.jar), Windows Installer files (.msi or .msp), driver files (.sys), and scripts. This signature provides verification of the signing individual and ensures the contents haven't been manipulated.

CPS – Certification Practice Statement
A Certification Practice Statement, based on RFC 3647, is a public document describing the framework of the management of the PKI and its CAs. The CPS states the procedures, practices, and requirements employed

in all areas of the PKI. Its location (CDP) is configured at the build of all Issuing CAs and specified in certificates issued by the CAs in the PKI covered by the CPS.

CRL – Certificate Revocation List
A CRL is a signed, time-stamped list of certificate serial numbers and reason codes of revoked certificates by the Certification Authority. CRLs are normally published to a publicly available website for revocation checking. Once revoked a certificate is invalid prior to its expiration.

Cross Certification
Cross certification enables entities in one public key infrastructure (PKI) to trust entities in another PKI and establish an agreement of responsibilities and liability of each party. This doesn't join separate PKI hierarchies however, entities in each PKI are subject to the policies specified in the certificates.

CSP – Crypto Service Provider
Crypto Service Providers are typically a .dll and signature file referenced in the registry and provide cryptography services used in data signing and hashing along with the generation, protection, and storage of key material.

CSR – Certificate Signing Request
A Certificate Signing Request (CSR) (PKCS#10) is a request file sent to a Certificate Authority (CA) to receive a certificate and contains information about the subject making the request, the subject's public key, a set of attributes, a set of X.509 extensions, and a signature. These can be generated on non-Windows devices and by using OpenSSL or a method using CMP (Certificate Management Protocol).

Digital Certificate
A digital certificate represents the identity of a user, computer, or program. It contains information about the issuer and the subject and also certificate-specific data such as the CA signature and its validity period. It is signed by a certification authority (CA) which vouches for the identity of the user, computer, or program based on the information in the certificate. A minimum of verified information includes Subject Name identity, the issuing authority, and validity period.

Digital Signature
A digital signature is a cryptographic technique that uses a mathematical algorithm that binds a sender's identity to a digital message or document based on a subscriber's private key. It secures the message or document and verifies the integrity of the signature allowing a Relying Party to be sure that the file or document has not been altered or interfered with.

Document Signing
Document signing applies a digital signature to a document. The digital signature provides nonrepudiation where someone can't deny later that they ever signed it. Also, it denies the ability to fake a valid signature.

ECC – Elliptic Curve Cryptography
Elliptic Curve Cryptography is an efficient approach to public key cryptography based on the properties of elliptic curves. The primary advantage of ECC is efficiency. For example, ECC keys between 163 bits and 512 bits are one-sixth to one-thirtieth the size of equivalent RSA keys. As key size increases the efficiency of ECC increases.

ECDSA – Elliptic Curve Digital Signature Algorithm
ECDSA is a Digital Signature Algorithm that uses keys derived from elliptic curve cryptography that efficiently provides equivalent security. It provides RSA-level security but with much smaller key sizes. For example, an ECDSA 256-bit key size secures better than the RSA 2048. The decreased bandwidth in key exchanges is an obvious advantage of ECDSA.

EKU – Enhanced Key Usage
Enhanced Key Usage is both a certificate extension and a certificate extended property value. After a computer's identity, for example, is verifiable by an issued certificate an EKU specifies the uses for which a certificate is valid.

Examples are:

Server Authentication =1.3.6.1.5.5.7.3.1
Client Authentication =1.3.6.1.5.5.7.3.2
Secure E-mail EKU=1.3.6.1.5.5.7.3.4
Code Signing EKU=1.3.6.1.5.5.7.3.3
Time stamping EKU=1.3.6.1.5.5.7.3.8
Encrypting File System EKU=1.3.6.1.4.1.311.10.3.4
Document Signing EKU=1.3.6.1.4.1.311.10.3.12

Federal Information Processing Standards (FIPS):
A set of standards published by the National Institute of Standards and Technology (NIST). NIST standards of cryptographic import include 140-2 (Cryptographic Modules), 46-3 (Data Encryption Standard), 180-2 (Secure Hash Standard), 186 (Digital Signature Standard), and 197 (Advanced Encryption Standard).

Hardware Security Module (HSM):
A hardware device designed to be used as a cryptographic component in a computing system. HSMs can be used to enhance the security of the cryptographic keys, or to perform high-speed cryptographic operations, or both.

Hash Algorithm
An algorithm used to produce a fixed-length hash value of some piece of data, such as a message or session key. Typical hashing algorithms include CMAC, MD2, MD4, MD5, SHA-1, and SHA-2.

Issuing Certification Authority
An Issuing CA is online and issues certificates to users, computers, services, and programs as well as regularly publishing a CRL. It also manages the design and publication of templates that enforce policies and procedures defined either at the Issuing CA (two-tier hierarchy) or from the Policy CA (three-tier hierarchy). An Issuing CA also services Certificate Authority Web Enrollment, NDES, CEP/CES, and others in the enrollment and distribution of certificates in a PKI or to another PKI using cross-certification, for example.

Internet Engineering Task Force (IETF):
A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet's architecture and the continuity of its operation. It is open to any interested individual.

Key Pair
In an asymmetric cryptosystem, a key pair consists of a private key and its mathematically related public key having the property that the public key can verify a digital signature that the private key creates.

Non-Repudiation
Non-repudiation refers to the inability of signers to deny that a signature is theirs. The secure digital signature provides irrefutable evidence of the message's sender as well as the time it was sent, but it is only as defensible as the PKI is strong.

Object Identifier (OID):
A unique numerical identifier. The International Telecommunications Union (ITU) recommends the X.208 (ASN.1) standard as an international format for hierarchically identifying a myriad of telecommunications items. The Internet, for example, has an OID of 1.3.6.1. Companies and other private organizations OIDs are registered and maintained by the Internet Assigned Numbers authority (IANA).

Online Certificate Status Protocol (OCSP):
Protocol which can be used to determine the current Revocation status of a given Certificate.

OpenSSL
OpenSSL is a widely used cryptography library and tool that provides an open-source implementation of the SSL and TLS protocols. It is often used to generate keys and requests for non-Windows devices.

PEM – Privacy Enhanced Mail
A file format for X.509 certificate files using Base64 encoding to store and send keys, certificates, and other data. A PEM certificates file contains the certificate content and adds two boundary lines "—-BEGIN CERTIFICATE—-" and "—-END CERTIFICATE—-". In windows, this is equivalent to a .CER encoded Base-64 certificate file.

PKCS#10:
A message format used to request certification of a public key by a certification authority.

PKIX (Public Key Infrastructure X.509):
A working group within the IETF dedicated to developing standards for Public Key Infrastructure.

Public key Infrastructure (PKI):
PKI is a set of roles, policies, people, software, hardware, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. A PKI establishes a trust hierarchy in the provisioning of digital certificates throughout an organization providing secure authentication and encryption. A PKI consists of Certification Authorities that ensure that entities are who they say they are, use encryption algorithms for the security of data transmissions, and provide nonrepudiation to resolve by digital signature any question of who did what and when.

PQC – Post-Quantum Cryptography
Post-quantum cryptography is the field of cryptography that deals with cryptographic algorithms that can run on classical computers and are secure against an attack by a large-scale quantum computer that runs much stronger and faster. These algorithms have been based on the assumption that the degree to which they are unable to be solved maps to their strength.

Private Key
The secret half of a key pair used in a public key algorithm, private keys are typically used to encrypt a symmetric session key, digitally sign a message, or decrypt a message that has been encrypted with the corresponding public key.

Public Key Certificates
The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.

Public/private keys:
Cryptographic keys used with Asymmetric (a.k.a. "public key") algorithms, most commonly used for digital signatures and key exchange. Asymmetric keys exist in pairs – with a public and a private portion. Public keys are not cryptographically sensitive and may be widely distributed over unsecured channels. The corresponding private key must be stored securely. Examples of asymmetric algorithms include RSA, Diffie-Hellman, and Elliptic Curve cryptosystems (ECC).

Registration Authority (RA):
An RA is an authority to which the name and key vetting is often delegated. The CA retains responsibly for signing the issued X.509 Certificate.

Relying Party:
A person, computer, device, or application that relies upon data contained in the X.509 Certificate. All Relying Parties rely on the name and key. Most will require that some "additional data" be contained in the Certificate.

Root Certification Authority
The Root CA is the topmost CA in a PKI hierarchy and acts as the trust point for certificates issued by CAs in the environment. In a two or three-tier environment, the Root CA only issues certificates to subordinate CAs, such Policy CAs, and Issuing CAs. The Root CA should be built, maintained, and serviced offline, never connecting to a network. HSMs are often used within a private network to provide hardware-based key storage for the best protection of the Root CA's private keys.

As the beginning of trust in a PKI, the Root CA is the most important entity in the PKI. Policies and procedures should be well planned and designed and managed in accordance with the PKI Certificate Policy (CP).

RSA
RSA was one of the first practical key exchange and public-key cryptosystems and is widely used for secure data transmission. RSA is asymmetrical and its encryption and signing processes are performed through a series of modular multiplications. Security is increased by longer key lengths such as the 2048-bit key size used as a minimum size today.

SCEP – Simple Certificate Enrollment Protocol
SCEP is an enrollment method to allows a device to generate a certificate request and automatically submit it to a CA. It can also support certificate revocation and CRL lookups. SCEP was originally designed by Cisco and can work for most non-Windows devices. NDES (Network Device Enrollment Service) is Microsoft's implementation of SCEP.

Session Key
Session keys are used in single communication settings usually using symmetric encryption. They are short-lived and discarded when no longer needed. Used for encrypting and decrypting large amounts of data, they are also employed in the public-private key exchange for sending and receiving messages in that process.

S/MIME – Secure/Multipurpose Internet Mail Extensions
Originally developed as PKCS#7, S/MIME is a standard to secure MIME data with public key signing and encryption as defined in RFC 5751. A S/MIME template is available in ADCS that incorporates this standard for securing email in an enterprise.

Subject Alternative Name (SAN):
The Subject Alternative Name (SAN) is an X.509 v3 certificate extension that binds additional information to the subject DN of a certificate. Google Chrome, for example, only checks the SAN for identity. Accepted practice now is to include the Subject Name, or Common Name, in the SAN field.

Subject Name
The Subject Name is the Common Name of the certificate referring to the identity of the user, computer, or service it is requested for.

Subordinate CA
A CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. They can be Issuing CAs at the bottom tier of a two or three-tier hierarchy or at the middle tier of a three-tier hierarchy serving as a Policy CA that issues certificates and enforces policies to Issuing CAs. These are sometimes referred to as Intermediate CAs.

Subscriber
A subscriber is an entity that enrolls for a certificate from an Issuing CA and bears ultimate responsibility for the use of the private key associated with the certificate. These responsibilities are detailed in the Certification Practice Statement (CPS).

Symmetric Key
A secret key used with a symmetric cryptographic algorithm and where the same key is used for both encryption and decryption.

Thumbprint
The thumbprint is a unique hash value using the SHA-1 algorithm that uniquely identifies a certificate. It is computed over the complete certificate, which includes all its fields, including the signature, and is unrelated to the hash used in the digital signature, thus it is unique everywhere. Although a serial number is unique to CA, it may not be unique everywhere since the same number could be computed from another CA.

TLS – Transport Layer Security
TLS is a security protocol that supports confidentiality and integrity of messages in client and server applications communicating over open networks.

TPM – Trusted Platform Module
A TPM is a secure crypto-processor implemented in the form of a hardware chip embedded on a computer or device. It generates and protects cryptographic keys and is commonly used to authenticate hardware devices.

Validity Period
The period that is defined within a certificate, during which that certificate is intended to be valid. It begins when the certificate is issued and ends with the completion of the validity or if it's revoked or suspended earlier.

Vetting: In the context of PKI operations, "vetting" refers to the process used to prove a Subscriber's identity. This process, including the required Subscriber information and approvals, is a standard part of PKI operations documentation.

X.509
X.509 is a standard defining the format of public key certificates, revocation lists, and the certification path validation algorithm used in a strict hierarchal PKI infrastructure. Additionally, it defines the extensions, certificate structure, certificate uses, etc. It is standardized in RFC 5280 for version 2 and version 3 certificates.