Fannie Mae™

Fannie Mae Public Key Infrastructure Certificate Policy (CP)

Version: 01.10

Publication Date: Jan 23, 2018

© 2018 Fannie Mae. Trademarks of Fannie Mae.

Change History

The following Change History log contains a record of changes made to this document:

Published / Revised	Version #	Author (optional)	Section / Nature of Change
03 Jan 2016	1.0	Fecteau, Louie	Initial Draft
01 Nov 2016	1.1	Fecteau, Louie	Many changes
15 Nov 2016	1.2	Fecteau, Louie	Font and Text
1/24/2017	1.3	FM Legal	
1/27/2017	1.4	Fecteau, Louie	Font and Text
3/06/2017	1.5	FM Internal Legal with external council	Font and text
3/16/17	1.6	Fannie Mae Legal	Section 9 and other references re. certain provisions of the Fannie Mae Software Subscription Agreement governing liability etc. vis-à-vis Subscribers and Relying Parties
3/19/2017	1.7	Fecteau, Louie	Various wording clarifications
4/13/2017	1.8	Fecteau, Louie	FM Legal final approval of language
4/23/2017	1.9	Fecteau, Louie	Added CRL URLs, and Request URL
7/10/2017	1.10	Fecteau, Louie	Added Vulnerability Assessment Language (5.4.8)

© 2018 Fannie Mae.

Table of Contents

© 2018 Fannie Mae.

© 2018 Fannie Mae.

© 2018 Fannie Mae.

© 2018 Fannie Mae.

© 2018 Fannie Mae.

© 2018 Fannie Mae.

© 2018 Fannie Mae.

1. Introduction

1.1. Overview

This Fannie Mae Public Key Infrastructure (PKI) Certificate Policy (CP) (“Fannie Mae KPI CP,” or, “CP”) describes the protocols governing the issuance of digital certificates by the Fannie Mae Certification Authority (CA) and their use by Subscribers and Relying Parties.

This CP is applicable to all entities that have relationships with the Fannie Mae PKI, including Subscribers, Relying Parties, Registration Authorities (RAs), and Fannie Mae (CA) Vendors. This CP provides those entities with a clear statement of the roles and responsibilities of the Fannie Mae CA and those of each entity dealing with the Fannie Mae CA.

This CP consists of policy statements that outline the principles and requirements that govern the Fannie Mae PKI.

A CP specifies “what” requirements will be implemented, while a corresponding Certification Practice Statement (CPS) describes “how” those requirements are met for a specific CA. This CP is therefore not designed to detail the processes and procedures that are involved in the management and governance of the Fannie Mae PKI; this information is detailed in the Fannie Mae Public Key Infrastructure Certification Practice Statement (Fannie Mae PKI CPS).

Pursuant to the IETF RFC 3647 CP/CPS framework, this CP is divided into nine parts that cover the security controls and practices and procedures for the PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement “Not applicable” or "No stipulation."

This CP is only one of several documents that govern the PKI. Other important documents include the CPS, Registration Authority agreements, Enterprise Service agreements, End Entity Agreements, other customer agreements, privacy policies, and memoranda. Fannie Mae may publish additional certificate policies or certificate practice statements as necessary to describe other product and service offerings. These supplemental policies and statements are available to applicable users or Relying Parties.

1.2. Identification

This document shall be known as the Fannie Mae Public Key Infrastructure Certificate Policy (or “Fannie Mae PKI CP” or “this CP”).

1.3. PKI Participants

1.3.1. Certification Authorities

The Fannie Mae PKI is comprised of a single Root CA. The Root CA is an on-line CA from which certificates are issued to Fannie Mae users and IT Systems for authentication, devices, and applications, document signing, as well as Fannie Mae business partner(s), and Fannie Mae CA Vendor(s).

Where necessary, this CP distinguishes the different users and roles accessing the CA functions. Where this distinction is not required, the term Certification Authority is used to refer to the total CA entity, including the hardware, software, personnel, processes, and its operations.

The Fannie Mae Production CA and all associated Intermediate CAs will have the following name:

CN = Fannie Mae Root CA

O = Fannie Mae

C = US

© 2018 Fannie Mae.

1.3.2. Registration Authorities (RA/SAS)

The Registration Authorities (RAs) collect and verify each Trusted User or End Entity's identity and information to be entered into the End Entity's public key certificate. While the RAs initiate the process to cause the CA to issue Certificates, they do not sign or issue Certificates. The RAs shall perform their functions in accordance with the approved Fannie Mae PKI CPS. The RAs shall be responsible for:

- Maintaining control over the registration process
- Maintaining the identification and authentication process

The RAs shall only perform the functionality delegated by the CA per the CPS.

1.3.3. Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, and who is approved by Fannie Mae to hold that certificate.

1.3.3.1. Designated Certificate Holders

No stipulation.

1.3.4. Relying Parties

Under the Fannie Mae PKI, a Relying Party is the entity that relies on the validity of the binding connection of the Subscriber's name to a Public Key. The Relying Party shall be responsible for deciding whether or how to check the validity of the Certificate by checking the appropriate Certificate status information.

A Relying Party may use information in the Certificate (such as Certificate policy identifiers) to determine the suitability of the Certificate for a particular use.

1.3.5. Other Participants

Participant	Role
PKI Policy Authority (PA)	Fannie Mae will fulfill the PA role. The PA is the custodian of the Fannie Mae PKI CP and CPS and is responsible for PKI policy administration including the approval of policy changes.
Support Services	Support Services shall be performed by Fannie Mae Information Security in conjunction with Fannie Mae CA Vendor(s) under their contract with Fannie Mae to support the Fannie Mae PKI.
Fannie Mae PKI Customer Contract Officer	Fannie Mae is responsible for designating a Contract Officer(s) responsible for performing key functions regarding the overall operation of the Fannie Mae PKI. These functions include processing CA application and lifecycle management for any Local Registration Authorities (LRAs), submitting change requests for any modifications to the Certificate contents and submitting change requests for any modifications to the security policies enforced through the Fannie Mae PKI.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

All Certificates issued by the Fannie Mae Enterprise Certificate Service (ECS), through the Fannie Mae CMA, are to be used by IT systems and Subscribers for the sole purpose of conducting business with or for Fannie Mae. All uses of Certificates must be in accordance with this CP.

1.4.2. Assurance Levels

This CP specifies one security requirement: Basic Assurance Certificates issued under this CP are not intended to protect classified information.

There is only one level of assurance and it is defined as follows:

Assurance Level	Acceptable Use
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise not considered to be of major significance. This may include access to private or other confidential information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.

1.4.2.1. Basic Assurance

At Basic Assurance there is confidence that an asserted identity is accurate.

1.4.3. Factors in Determining Usage

This is pre-determined by Fannie Mae for:

- Transmission Layer Security
- User and Device Identity and Authentication
- Code and Document Digital Signature (Integrity)
- Virtual Private Network (VPN) Services
- Data Encryption

1.4.4. Prohibited Certificate Uses

In general terms, applications for which Fannie Mae PKI issued digital certificates are prohibited are those where:

- Business activities are conducted, other than for Fannie Mae or Fannie Mae sponsored Business Partners or third parties;
- Usage contravenes this CP and other governing Fannie Mae policies; or
- Usage contravenes relevant law.

1.5. Policy Administration

1.5.1. Organization Responsibilities for this Certificate Policy

Fannie Mae shall be the custodian of this CP and responsible for its maintenance and publication.

1.5.2. Contact Information

Questions regarding this CP shall be directed to:

Fannie Mae Policy Authority (PA)
Chief Information Security Officer
3900 Wisconsin Avenue NW, Washington DC 20016

1.5.3. Person Determining CPS Suitability for the Policy

The Fannie Mae Policy Authority (PA) shall approve the Fannie Mae PKI Certification Practice Statement.

1.5.4. CP Approval Procedures

Fannie Mae Information Security will present this document to Fannie Mae {CISO/CIO ?} once per year for review / approval. The PA may propose amendments to this CP, or any part thereof, at any time at his/her discretion. All policy changes under consideration shall be disseminated to interested parties (e.g., Fannie Mae stakeholders). All interested parties shall provide their comments to the originating PA or their delegate, in a fashion to be prescribed by the originating PA. Distribution of potential policy changes to a Relying Party, a Subscriber or an End Entities is not the responsibility of the PA. The PA will make a reasonable effort to ensure that such information about adopted changes is accessible to those communities through normal distribution channels (such as placement on the website mentioned in Section 2.2 below).

Fannie Mae CA Vendor(s) shall determine if a CPS sets out, in a satisfactory manner, how the CA will implement the requirements of this CP, and recommend approval when appropriate to the PA originating the proposed change. The PA shall approve the Certification Practice Statement and any amendments thereto.

Updates to this CP must be approved by Fannie Mae and implemented, as applicable, by Fannie Mae CA Vendor(s).

1.6. Definitions and Acronyms

1.6.1. List of Definitions

Authority Revocation List: A list of revoked Certification Authority cross-certificates and root certificates.

Activation Data*: Data values, other than Keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held Key share).

CA Certificate: A Certificate for one CA's Public Key issued by another CA.

CA Private Signing Key: The Private Key corresponding to a Public Key listed in a CA Certificate and is used to sign Fannie Mae PKI certificates.

CA Private Primary Key: The Private Key used to sign CA Certificates.

CA Vendor: Service supplier retained by a business to provide technical and support services in connection with a PKI.

Certificate: A computer-based record or electronic message that identifies the issuing Certificate Authority, the name or identity of the Subscriber, contains the Public Key of the Subscriber, lists a validity period, is digitally signed by a Certification Authority, and has meaning given in this Certificate Policy and applicable standards. A Certificate includes not only the actual information contained within, but also all documents expressly referenced or incorporated into the Certificate.

Certificate Revocation List (CRL): A list of Certificates revoked prior to the expiration of their Validity Periods

Certification Authority (CA): An entity that creates, issues, manages and revokes Certificates

Certificate Policy*: The set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of Certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification Practice Statement (CPS)*: A statement of the practices that a Certification Authority employs in issuing, managing, revoking, and renewing or Re-Keying Certificates.

Crypto-module: Either software, a device, or a utility that generates Key Pairs, stores cryptographic information, and/or performs cryptographic functions.

Digital Signature, Digitally Sign: The transformation of an electronic record by one person using a Private Key and Public Key Cryptography so that another person having the transformed record and the corresponding Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the Public Key and whether the record has been altered since the transformation was made.

Distinguished Name (DN): The unique identifier for a Subscriber so that s/he can be located in a directory based on the ITU/CCITT X.500 (e.g. the DN for a Subscriber might contain the following attributes: common name (cn), e-mail address (mail), Organization name (o), Organizational unit (ou), locality (l), state (st) and country (c)).

End Entity: A Subscriber and/or authorized Relying Party.

Enterprise Service Agreement: An agreement between a business (namely Fannie Mae under this CP) and a Vendor or Supplier (namely a Fannie Mae CA Vendor under this CP) retained by a business to provide support services in connection with a CA PKI. Enterprise Service Agreement includes related Service Orders and Service Requests approved by the CA Vendor.

Fannie Mae CA Vendor: CA Vendor retained by Fannie Mae in support of the Fannie Mae PKI.

Fannie Mae PKI Certificate: A Certificate issued pursuant to this CP.

Issue Certificates, Issuance: The act performed by a CA in creating a Certificate listing with the CA as "Issuer," and notifying the Applicant of the contents and that the Certificate is ready and available for Acceptance.

Issuing Certification Authority (Issuing CA)*: In the context of a particular Certificate, the issuing CA is the CA that issued the Certificate (see also Subject Certification Authority).

Key Generation: The process of creating a Key Pair.

Key Pair: Two mathematically related Keys (a Private Key and the corresponding Public Key), with the following properties:

- one "Key" of the key pair can encrypt a communication only capable of decryption by the other Key; and
- deriving or discovering one Key from the other Key is computationally infeasible, assuming likely circumstances including the availability of text encrypted by either of the Keys.

Lightweight Directory Access Protocol (LDAP): A client-server protocol used for accessing X500 directory services over a computer network.

No Stipulation: No condition or requirement that is specified or demanded as part of a subject area.

Object Identifier (OID): The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the PKS established by this CP, they are used to uniquely identify Certificates issued under this CP and the cryptographic algorithms supported.

Online Certificate Status Protocol (OCSP): A protocol that is used to provide real-time validation of a Certificate's status. An OCSP responder is used to respond to Certificate status requests and can issue one of

three responses: Valid, Invalid, and Unknown. An OCSP responder replies to Certificate status requests on the basis of CRLs (Certificate Revocation Lists) provided to it by certification authorities.

Operational Period: A Certificate's actual term of validity, beginning with the start of the Validity Period and ending with the earlier of:

- The end of the Validity Period disclosed in the Certificate, or
- The revocation date of the Certificate.

PKI Sponsor: Formal business leader of an organization that requests, receives, and maintains certificates for IT use within their area of responsibility.

Private Key: The sensitive Key in the Key Pair protected by the Subscriber and kept secret. The Private Key creates Digital Signatures or decrypts data previously encrypted using the corresponding Public Key.

Public Key: The non-sensitive Key in the Key Pair disclosed by the Subscriber holding the corresponding Private Key. The Public Key verifies Digital Signatures created using the corresponding Private Key, or encrypts data meant for decryption with the corresponding Private Key.

Public Key Cryptography: A type of cryptography also knows as asymmetric cryptography. This cryptography uses a Key Pair rather than a single Key to secure the authentication and/or confidentiality of data.

Public Key Infrastructure (PKI): The architecture, technology, practices, and procedures that support operation of a security system employing Certificates and Public Key Cryptography.

Public Key Service (PKS): This is identical with Public Key Infrastructure, with the word Service used to emphasis on leveraging the environment to service Fannie Mae customers.

Registration Authority (RA): An individual or organization responsible for verifying the identity of a Subscriber or, in the case of another Business Unit, a Designated Certificate Holder.

Registration System. People, process and technology used in the validation of requests for certificates.

Relying Party*: A recipient of a Certificate who acts in reliance on that Certificate and/or any digital signatures verified using that Certificate.

Repository: An online system maintained by an Issuing CA for storing and retrieving Certificates and other information relevant to Certificates, including information relating to Certificate validity or revocation.

Revoke (a Certificate): To invalidate a Certificate permanently from a specific time onward. Revocation includes listing the Certificate in a set of revoked Certificates or other directory or database of revoked Certificates (e.g. inclusion in a CRL). The system also prevents users from accessing revoked Certificates once connected to the central infrastructure.

Request For Comments (RFC): Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by Internet Architecture Board as Internet standards.

Secure Personal Security Environment (SPSE): A secure storage area containing information such as Private Keys and related Certificates. The storage area is encrypted and protected using cryptography. The form of storage may vary from files to tamper-resistant cryptographic tokens

Signing Key Pair: Is a Private Key and a Public Key used for creating and validating a Digital Signature.

Subject Certification Authority: In the context of a particular CA-Certificate, the subject CA is the CA whose Public Key is certified in the Certificate (see also Issuing certification authority).

Subject Name: The specific field in a Certificate containing the Distinguished Name (DN) for the Subscriber.

Subscriber: A subject of a Certificate who is issued a Certificate.

End Entity Agreement: An agreement between a CA (namely Fannie Mae under this CP) and a Subscriber or a Relying Party that establishes the right and responsibilities of the parties regarding the issuance and management of Certificates. For purposes of this CP, the end Entity Agreement shall consist of (i) the Software Subscription Agreement governing Subscriber's or the Relying Party's use of Fannie Mae Licensed Applications (as defined in the Software Subscription Agreement) in support of the transactions and operationally implementing the PKI set forth in this CP, and (ii) this CP.

Token: A Crypto-module consisting of a hardware object (e.g., a "smart card"), often with memory and a microchip.

Trusted Role: A role whose execution requires adherence to a policy and procedures to prevent the introduction of security problems. The functions of Trusted Roles form the basis of trust for the entire PKS.

Validity Period: The intended term of validity of a Certificate, beginning with the date of Issuance ("Valid From" or "Activation" date), and ending with the earlier of two dates: the expiration date indicated in the Certificate ("Valid To" or "Expiry" date) or the revocation date asserted in the revocation list specified as the CRL Distribution Point within the certificate.

x.500: A series of computer networking standards covering electronic directory services. These services include Directory Access Protocol (DAP), Directory System Protocol (DSP), Directory Information Shadowing Protocol (DISP), and Directory Operational Bindings Management Protocol (DOP).

x.509: An International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) standard for Public Key Infrastructure which specifies standard formats for public key certificates and certification path validation.

*As defined in the standard for Certificate Policies (RFC 3647)

1.6.2. 1.6.2. List of Acronyms

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
ECS	Enterprise Certificate Service
FIPS	Federal Information Processing Standard
LDAP	Lightweight Directory Application Protocol
LRA	Local Registration Authority
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure, also known as PKS
PKS	Public Key Services, also known as PKI

RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request for Comment
TA	Trusted Agent
URL	Uniform Resource Locator
US	United States

2. Publication and Repository Responsibilities

2.1. Repositories

Fannie Mae CA shall publish both CA data (CA Certificate, CRLs, and policies) and subscriber certificates to the Fannie Mae CRLs. Where used, the term “Repository” shall refer to this directory, including all required components for certificate and CRL publication.
Relying Parties shall be able to access Fannie Mae CA CRLs published on the Repository. These CRLs shall be available 24x7 under normal conditions.

- FM CRL URL: http://tppcrl.fanniemae.com/ca_425969a17a0fb24325ab2d65402241e2/LatestCRL.crl
- Symantec CRL URL http://pki-crl.symauth.com/ca_425969a17a0fb24325ab2d65402241e2/LatestCRL.crl

2.2. Publication of Certification Information

This Fannie Mae PKI CP is published at the website specified in the Fannie Mae PKI CPS. Business Partners and relying third parties are entitled to obtain a copy of the Fannie Mae PKI CP by visiting the specified website or by contacting their Fannie Mae Business Partner point of contact and requesting a copy. By default, the Fannie Mae CPS will not be distributed to external entities. Exceptions will require approval from the Fannie Mae PA.

Distribution of the Fannie Mae PKI CPS to Fannie Mae employees shall be limited to employees that have a business need and shall be distributed in a manner that requires the identification and authentication of the Fannie Mae employee.

2.3. Time or Frequency of Publication

This Fannie Mae PKI CP and any subsequent changes thereto shall be made publicly available within 30 days of approval.

Publication requirements for CRLs are provided in Sections 4.9.7 of this Fannie Mae PKI CP.

2.4. Access Controls on Repositories

The CA shall protect information not intended for public dissemination or modification. CA certificates and CRLs site information shall be available through the Fannie Mae ECS site. The CPS documents shall detail what information in the Fannie Mae ECS site is to be exempt from automatic availability and to whom, and under what conditions, the restricted information may be made available.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

All CAs operating under this policy shall generate, sign, and process certificates that contain an X.501 Distinguished Name (DN) that clearly and distinguishingly identifies the issuer and the subject of the certificate.

3.1.2. Need for Names to be Meaningful

The identity certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

When DNs are used, it is preferable that the common name represents the Subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Gateway or Organization Y Certificate Authority).

3.1.3. Anonymity or Pseudonymity of Subscribers

The Fannie Mae PKI does not support the use of pseudonyms in subscriber common names.

3.1.4. Rules for Interpreting Various Name Forms

Name forms shall comply with RFC 2822 and X.500 standards for name forms.

3.1.5. Uniqueness of Names

Name uniqueness across the PKI shall be enforced.
The directory will be managed in such a way as to ensure that no two individuals are assigned the same DN and, therefore, the same electronic identity. The CA shall document in its CPS:

- What name forms shall be used
- How the CAs and RAs will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers

3.1.6. Recognition, Authentication and Role of Trademarks

Where permitted or required, the use of a trademark is reserved to the holder of that trademark.

3.2. Initial Identity Validation

Certificate applicants must communicate application requests for certificates to an authorized Fannie Mae Registration Authority (RA) via a trustworthy process. Authority hardware and software may communicate authorizations to issue Certificates directly to the supporting CA electronically, provided all communication is secure.

3.2.1. Method to Prove Possession of Private Key

The Fannie Mae *Certificate Management Authority* (Fannie Mae CMA) must obtain acknowledgment of receipt from the Subscriber of shipment or must revoke any Certificates issued to that Subscriber. When the Fannie Mae CMA delivers keys to Subscribers, they must accomplish delivery in a way that ensures that they provide the correct activation data to the correct people. The Fannie Mae CMA shall maintain a Subscriber receipt validation record. When any mechanism that includes a shared secret (e.g., a password or PIN) is used, the mechanism shall ensure that the applicant and the Fannie Mae CMA are the only recipients of this shared secret.

In cases where the Subscriber causes the system to generate keys (e.g., remote emergency renewal), the Subscriber is required to prove possession of the Private Key that corresponds to the Public Key in the Certificate request to the Fannie Mae CMA.

3.2.2. Authentication of an Organization Identity

A Fannie Mae CA may issue Certificates directly in the name of an organization rather than an individual for those functions and applications performed on behalf of the organization. The Fannie Mae CMA must authenticate the identity of any organization that appears as a component of a subject name appearing in a Certificate issued by the CA before processing the Certificate application. Any organization requesting a Certificate must have a PKI Sponsor to accept the

obligations of the organization. This section pertains only to the authentication and naming of an organization as the subject in a Certificate.

Requests for Certificates in the name of an organization or group shall include the necessary identifying data of the PKI Sponsor, the group or organization name, address, and documentation of the existence of the organization. This information will include but is not limited to the following:

- Organization identification and authorization
- Contact information to enable the Fannie Mae CMA to communicate with the PKI Sponsor as required

The Fannie Mae CMA shall verify this information, in addition to the authenticity and authorization of the requesting PKI Sponsor, authenticate the validity of any authorizations to be asserted in the Certificate, and verify the source and integrity of the data collected to an assurance level commensurate with the Certificate assurance level requested. The CPS will specify acceptable measures for authenticating both the organization and PKI Sponsor's identity and authorizations.

The Fannie Mae CMA shall also include his or her own identity information and authentication declaration as outlined in Section 3.2.3. The PKI Sponsor shall present information sufficient for registration at the level of assurance requested, for both himself or herself and the non-human Entity (i.e., organization or group) requesting a Certificate, and shall authenticate this information in person as prescribed in Section 3.2.3.

3.2.3. Authentication of an Individual Identity

Personnel filling Fannie Mae trusted roles shall be authenticated according to the stipulations for a Basic Assurance certificate. All Individual Identity certificates shall only be issued to human Subscribers.

3.2.3.1. Applicants for Basic Assurance Certificates

Applicants requesting a Basic Assurance Certificate must be validated and approved by Fannie Mae CMA before Certificates can be issued.

3.2.3.2. Authentication of Devices

Some computing and communications devices (routers, firewalls, servers, etc.) and software applications will be named as Certificate subjects. In such cases, the device must have a human sponsor. These Certificates shall be issued only to devices under the issuing entity's control (i.e., require registration and validation that meets Fannie Mae requirements, as well as requiring re-validation prior to being re-issued). In the case a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive Certificates. The CPS shall describe procedures to ensure that Certificate accountability is maintained.

The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys
- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the Fannie Mae CA or RA to communicate with the sponsor when required

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested.

3.2.4. Non-verified Subscriber Information

Information that is not verified shall not be included in Certificates.

3.2.5. Validation of Authority

Whenever a Fannie Mae employee, partner, or customer submits a Certificate application, Fannie Mae shall be responsible for performing a verification of authority to ensure that the individual is authorized to obtain a Certificate.

3.2.6. Criteria for Interoperation

No stipulation.

3.3. Identification and Authentication for Rekey Requests

Re-keying a Certificate means that the Fannie Mae CMA creates a new Certificate that has the same characteristics and level as the old one, except that the new Certificate has a new, different Public Key (corresponding to a new, different Private Key) and a different serial number and possibly different validity period.

Subscribers must periodically obtain new keys and re-establish identity as defined in Section 3.2.

The Fannie Mae PKI CA may re-key Subscribers based on electronically authenticated Subscriber requests. Subscribers must stop using Private Keys before the Public Key expires. Confidential Private Keys do not have a lifetime so Subscribers may use these keys at any time to decrypt information.

For device certificates, identity may be established through the use of the device's current signature key or the signature key of the device's human sponsor, except that identity shall be established through the initial registration process at least once every nine years from the time of initial registration.

3.3.1. Automated Routine Re-Key

Re-keying a Certificate means that the Fannie Mae CMA creates a new Certificate that has the same characteristics and level as the old one, except that the new Certificate has a new, different Public Key (corresponding to a new, different Private Key) and a different serial number and possibly different validity period.

Subscribers must periodically obtain new keys and re-establish identity as defined in Section 3.2.

The Fannie Mae PKI CA may re-key Subscribers based on electronically authenticated Subscriber requests. Subscribers must stop using private keys before the public key expires. Private "Signing" Keys do not have a lifetime so Subscribers may use these keys at any time to validate identity information. As of the date of this Fannie Mae PKI CP, no Subscribers will be issued "individual" keys for data encryption.

For device Certificates, identity may be established through the use of the device's current signature key or the signature key of the device's human sponsor, except that identity shall be established through the initial registration process at least once every three years from the time of initial registration. Fannie Mae Certificates are issues at a "Basic Assurance level", where such keys have a maximum lifetime of three years.

If Fannie Mae implements the capability of associating authorizations with a Certificate, including any conveyed or implied by the subject's **Distinguished Name** (DN), the Subscriber and/or the Subscriber's organization shall notify the appropriate CAs of the withdrawal of authorization. The CPS shall document the mechanisms used to notify the appropriate CAs of this action. In such instances, withdrawal of authorization may result in revocation of the old Certificate and, if necessary, the issuance of a new Certificate with a different Public Key and the appropriate associated authorizations.

3.3.2. Manual Re-Key Requests

No stipulation.

3.3.3. Identification and Authentication for Re-key after Revocation

For all levels of assurance, Subscribers requesting Certificates after revocation, other than during a renewal or update action, must meet initial identity authentication and registration requirements, as indicated in Section 3.2 to obtain a new Certificate.

3.4. Identification and Authentication for Revocation Requests

Requests for Certificate revocation will be submitted and reviewed through Fannie Mae's approved process. The Fannie Mae CMA may authenticate requests to revoke a Certificate using signatures generated with that Certificate's associated Private Key, regardless of whether or not the Private Key has been compromised.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

Subscribers shall be limited to those individuals filling Trusted Roles within the PKI and the employees, contractors, business partners and affiliates of Fannie Mae.

Application for Certificates issued under this CP must be submitted by Fannie Mae or Fannie Mae contracted staff.

The Fannie Mae CA operating under this CP shall establish and document the Certificate application and enrollment process in its CPS.

4.1.1. Who Can Submit a Certificate Application

4.1.1.1. CA Certificates

The Fannie Mae CA will not issue Certificates to any CA external to the Fannie Mae environment.

4.1.1.1.1. Cross-Certification Certificate Application

Within Fannie Mae, only the Fannie Mae Chief Information Security Officer shall apply for cross certification with any external PKI/CA.

Only the Fannie Mae CA shall cross certify with external CAs. A Certification Practices Statement, written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647) shall accompany all such requests.

Entities applying for cross certification are responsible for providing accurate information on their certificate applications. The Fannie Mae CMA shall authenticate, and protect from modification, communications among PKI authorities supporting the Certificate application and issuance process.

4.1.1.2. User Certificates

Authorized Fannie Mae employees as well as Fannie Mae managed service providers and contractors approved by Fannie Mae are permitted to apply for a Subscriber Certificate.

Personnel that are approved by Fannie Mae to serve in a Fannie Mae PKI Trusted Role, are permitted to apply for a Trusted User Certificate (Security Officer, etc.).

4.1.1.3. Device Certificates

An application for a device Certificate shall be submitted by the sponsor of the device as outline in section 3.2.3.2.

4.1.2. Enrollment Process and Responsibilities

Subscriber enrollment will be processed using the Self-Administration Service (SAS).

Creation of Trusted Roles will be processed via the Registration Authority (RA).

The Fannie Mae CMA shall verify the accuracy of Certificate application information, using procedures as specified in the applicable CPS, before issuing Certificates.

4.2. Certificate Application Processing

The following steps are required when processing a Certificate application from a potential Subscriber:

- Establish authorization to receive a Certificate
- Establish and record identity of the Subscriber
- Provide a point of contact for verification of any roles or authorizations requested

These steps may be performed in any order that is convenient for the RA and applicants, as long as it does not defeat security controls, and all steps must be completed before Certificate issuance.

4.2.1. Performing Identification and Authentication Functions

The applicant and the Fannie Mae CMA must perform the steps outlined in the applicable CPS when an applicant applies for a Certificate. The Fannie Mae CMA and Subscribers may perform these steps in any order that is convenient and that does not defeat security controls; however, they must complete all steps before Certificate issuance.

The Fannie Mae CMA shall authenticate and protect from modification all communications supporting the Certificate application and issuance process using mechanisms commensurate with the protection requirements of the data to be encrypted. The Fannie Mae CMA shall protect from unauthorized disclosure, any electronic transmission of this data (i.e., encryption) commensurate with the protection requirements of the data.

4.2.2. Approval or Rejection of Certificate Applications

The approval or rejection of Certificate applications shall be at the discretion of Fannie Mae.

The Time to Process Certificate Applications.
Certificate applications are processed in accordance with the Fannie Mae on boarding processes.

4.3. Certificate Issuance

Subscribers will utilize the Self-Administration Server (SAS) to authenticate using their Fannie Mae “ID”, Fannie Mae ID “password”, and validation questions and answers. Upon receipt of a valid request, the Fannie Mae CA issues the Certificate in the form of key pairs (encryption and/or verification) for that Subscriber’s Certificate, which can be manually recovered in case of corruption or reimaged workstation via the FM ECS Key Recovery Process.
MyServices link https://fanniemae.service-now.com/ess/
Search for SSL Cert for Web or App Server

Upon manual recovery, only the verification Private Key is updated with new lifetime. Encryption Certificates will only be updated upon expiration and creation of a new Certificate.

The Fannie Mae CA binds the identity information in the Certificate application with the Subscribers keys during the Certificate issuance process.

4.3.1. CA Actions During Certificate Issuance

Upon receiving the request, the CA/RA shall:

- Verify the identity of the requester.
- Verify the authority of the requester and the integrity of the information in the Certificate request.
- Build and sign a Certificate if all requirements have been met (in the case of an RA, the CA signs the Certificate).

All authorization information received from a prospective Subscriber are verified before the Certificate is issued. The responsibility for verifying prospective Subscriber data is described in section 3.2 of the CPS.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

The Fannie Mae CA/RA operating under this CP shall inform the Subscriber of the creation of a Certificate and make the Certificate available to the Subscriber.

4.4. Certificate Acceptance

Before a Subscriber can make effective use of a Private Key, the Fannie Mae CMA shall convey their responsibilities via email and/or reverencing published documentation, to the Subscriber (or Sponsor in the case of group/organization or device certificates).

4.4.1. Conduct Constituting Certificate Acceptance

A user who enrolls into the Fannie Mae CA is deemed accepting the Certificate and the terms associated with it.

4.4.2. Publication of the Certificate by the CA

The Fannie Mae CA(s) shall publish both CA information and Subscriber Certificates to the Fannie Mae Repository (see section 2.1).
https://tppcrl.fanniemae.com/VEDAdmin/
https://tppcrl.fanniemae.com/Aperture

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

No stipulation.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers shall protect their Private Keys from access by unauthorized parties as confidential information and as Authentication Credentials under their Software Subscription Agreement.

The Fannie Mae PKI CA shall specify restrictions in the intended scope of usage for a Private Key through Certificate extensions, including the key usage and other extensions as needed, in the associated Certificate.

4.5.2. Relying Party Public Key and Certificate Usage

The CA operating under this CP shall issue CRLs specifying the current status of all unexpired Certificates. Relying Parties should process and comply with this information whenever using Fannie Mae PKI CA-issued certificates in a transaction.

4.6. Certificate Renewal

Certificate renewal consists of issuing a new Certificate with a new validity period and serial number while retaining all other information in the original Certificate including the Public Key. As of the data of this CP, Fannie Mae will not "renew" Fannie Mae issued Certificates after their initially issued expiration date, only revoke and issue new Certificates.

4.6.1. Circumstance for Certificate Renewal

Subscriber Certificates issued under this CP shall not be renewed.
Note: Certificates will only be "revoked" or expire, and new Certificates issued where appropriate.

4.6.2. Who May Request Renewal

Certificates issued under this CP shall not be renewed.

4.6.3. Processing Certificate Renewal Requests

No stipulation.

4.6.4. Notification of New Certificate Issuance to Subscriber

The Fannie Mae CA shall proactively notify affected Subscribers of Certificate status by any appropriate and secure means.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

As of the date of this CP, Fannie Mae issued certificates are not renewed, only revoked and new certificates issued..

4.6.6. Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.7. Certificate Re-Key

No Stipulation

4.7.1. Circumstance for Certificate Re-key

No Stipulation.

4.7.2. Who May Request Certification of a New Public Key

No Stipulation

4.7.3. Processing Certificate Re-keying Requests

No Stipulation

4.7.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

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

No stipulation.

4.8. Certificate Modification

No stipulation

4.8.1. Circumstance for Certificate Modification

No Stipulation.

4.8.2. Who May Request Certificate Modification

No Stipulation

4.8.3. Processing Certificate Modification Requests

No Stipulation

4.8.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6. Publication of the Modified Certificate by the CA

No stipulation.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9. Certificate Revocation and Suspension

The Fannie Mae CA operating under this CP shall issue CRLs covering all unexpired Certificates issued under this CP. Revocation requests must be authenticated. Certificate suspension for Fannie Mae issued Certificates is not allowed by this CP.

4.9.1. Circumstances for Revocation

A Certificate shall be revoked when the bound between the subject and the subject's Public Key contained within a Certificate is no longer considered valid. Examples of circumstances that invalidate the bound include:

- Subscriber's Private Key is lost, stolen, or compromised
- Subscriber no longer transacts with Fannie Mae and no longer needs the Certificate
- Subscriber is no longer affiliated with the operation or maintenance of the CA
- Subscriber leaves the employ of Fannie Mae
- Subscriber's identifying information contained in the Certificate is no longer valid
- Subscriber forgets the {Fannie Mae Directory} password and no recovery is possible
- Subscriber or other authorized party asks for Subscriber's Certificate to be revoked.
- A device supporting Fannie Mae Data or IT services has been lost or compromised.

Whenever any of the above circumstances occur, the associated Certificate shall be revoked through the Fannie Mae Enterprise Security Services authorized staff, and placed on the CRL. Revoked Certificates shall be included on all new publications of the Certificate status information, until the Certificates expire.

For Certificates that express an organizational affiliation, the Fannie Mae CMA shall require that the organization must inform the Fannie Mae CMA of any changes in the Subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a Subscriber, the Fannie Mae CMA shall revoke any Certificates issued to that Subscriber containing the organizational affiliation. If an organization terminates its relationship with the Fannie Mae CA such that it no longer provides affiliation information, the Fannie Mae CMA shall revoke all Certificates affiliated with that organization. Whenever any of the above circumstances occur, the Fannie Mae CMA revokes the associated Certificate and places it on the CRL. Once revoked, a Certificate will remain on the CRL at least until the certificate expires.

4.9.2. Who Can Request Revocation

The RA can request the revocation of a Subscriber's Certificate on behalf of any authorized party as specified in the CPS. A Subscriber may request that its own Certificate be revoked. Other authorized officials may request revocation as described in the CPS.

4.9.3. Procedure for Revocation Request

Requests for Certificate revocation will be submitted by Fannie Mae authorized personnel.
Fannie Mae does not require that the Subscriber be notified of Certificate revocation.

4.9.4. Revocation Request Grace Period

- Revocation shall take effect upon the publication of status information (identifying the reason for the revocation, which may include loss, compromise, or termination of employment). Information about a revoked certificate shall remain in the status information at least until the certificate expires. For revocations involving "termination of employment, the CRL will list the reason as "Entity or subject no longer associated with Fannie Mae or Fannie Mae business".

There is no grace period for certificate Revocation under this Policy.

4.9.5. Time within which CA Must Process the Revocation Request

The CA shall revoke Certificates per any Fannie Mae contractual obligation.

4.9.6. Revocation Checking Requirement for Relying Parties

No stipulation.
Note: Use of revoked Certificates can have damaging consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, who must consider the risk, responsibility, and consequences for using a Certificate the status of which cannot be guaranteed.

4.9.7. CRL Issuance Frequency

CRLs shall be published periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be published more frequently than the issuance frequency described below.
The Fannie Mae CA CRL lifetime shall be a maximum of 4 hours.

Practice Note: Since many applications only check for a new CRL at *nextUpdate*, a longer *nextUpdate* time may result in applications continuing to rely on older CRLs even when a newer CRL is available. A longer *nextUpdate* time also increases the potential of a replay attack to validate a newly revoked Certificate.

4.9.8. Maximum Latency for CRLs

CRLs shall be published within 4 hours of generation.

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

User reports will be generated and utilized for notification of user expiry.

4.9.12. Special Requirements re: Key Compromise

In the event of a Private Key compromise, the CA will follow the procedures outlined in Section 5.7.3 –CA Key Compromise.

4.9.13. Circumstances for Suspension

No Stipulation

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

4.10.1. Operational Characteristics

When a Certificate is revoked, the status information must be updated and available to Relying Parties within 4 hours.

4.10.2. Service Availability

Service availability is dependent upon availability of the Fannie Mae CRLs.

- FM CRL URLs: http://tppcrl.fanniemae.com/ca_425969a17a0fb24325ab2d65402241e2/LatestCRL.crl
- Symantec CRL URL: http://pki-crl.symauth.com/ca_425969a17a0fb24325ab2d65402241e2/LatestCRL.crl

Availability is dependent on a number of factors, including events beyond Fannie Mae CA's reasonable control.

4.10.3. Optional Features

No stipulation.

4.11. End of Subscription

The Fannie Mae Certificate Service shall consider the revocation or expiration of a Certificate without issuance of a new Certificate as the termination of the Subscriber's Certificate subscription. There is no requirement for the Fannie Mae CA to provide notification of the termination of the Subscriber's Certificate subscription.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Management, Operational and Physical Controls

The Fannie Mae CA shall be operated under the Management, Operational and Physical Security Controls stipulated in the CP and, with respect to Fannie Mae CA Vendors, those of this CP and the applicable Enterprise Service Agreement

5.1. Physical Security Controls

Physical security of all hardware will follow the Fannie Mae Data Center requirements.

5.1.1. Site Location and Construction

The location and construction of the facility housing Fannie Mae PKI CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be 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, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to CA equipment and records.

5.1.2. Physical Access

The CA equipment shall be protected from unauthorized access. Physical access controls will follow Fannie Mae requirements. In addition to Fannie Mae Data Center requirements, a lockbox and/or Physical Safe will be utilized to control access to the hardware encryption module.

Physical access controls and procedures shall be implemented to:

- Ensure no unauthorized access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers
- Ensure an access log is maintained and inspected periodically

A security check of the facility housing the CA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation
- Physical security systems i.e. (door locks, windows, etc.) are functioning properly
- The area is secured against unauthorized access
- Visitors must be authorized by Fannie Mae prior to their visit.
- Visitors will be escorted at all times by authorized personnel.
- Visitor entry and exit will be controlled

Access to the cryptographic module (HSM) requires two person physical access control.

When not in use, the Fannie Mae CMA staff or Fannie Mae contracted CMA vendors supporting Fannie Mae CA systems, shall place removable Fannie Mae CMA cryptographic modules, removable media, and any activation information used to access or enable Fannie Mae CMA cryptographic modules or Fannie Mae CMA equipment, or paper containing sensitive plain-text information, in locked containers. Such containers shall be sufficient for housing equipment and information commensurate with the classification, sensitivity, or value of the information protected by the Certificates issued by the Fannie Mae CA. Fannie Mae CMA staff or Fannie Mae CA Vendors, shall either memorize or record and store activation data in a manner commensurate with the security afforded the cryptographic module, and shall not store such data with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated RA cryptographic tokens shall be protected against theft, loss, and unauthorized use. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.3. Electrical Power

An uninterruptible source of power will be provided which will supply the required level of power for sufficient duration to ensure that the CA and supporting equipment shall have the capability to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.

5.1.4. Water Exposures

Water exposure controls are covered in Fannie Mae Data Center requirements.

5.1.5. Fire Prevention and Protection

An automatic fire extinguishing system shall be installed in accordance Fannie Mae Data Center requirements.

5.1.6. Media Storage

CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains archive, or backup information shall be stored in a location separate from the Fannie Mae CA Equipment.

5.1.7. Waste Disposal

Waste containing sensitive information shall be destroyed, such that the information is unrecoverable, prior to disposal. Media used to store sensitive data shall be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8. Off-Site Backup

Backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the CPS. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational Fannie Mae CA.

5.2. Procedural Controls for the CA

5.2.1. Trusted Roles

A Trusted Role is a role that performs functions that are sensitive in nature. The functions performed in these roles form the basis of trust for all uses of the CA and Fannie Mae PKI services.

There are two approaches to increase the likelihood of successfully carrying out these roles. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

At a minimum the following roles will be used:

1. Master User – authorized to perform initial configuration of the CA; start and stop the CA services; and verify and backup the CA's database.
2. Security Officer – authorized to configure the CA policies; configure audit parameters; and perform certificate lifecycle operations for Registration Authorities. Security Officers do not issues certificates to Subscribers.
3. System Administrator – authorized to install, configure, and maintain the server operating system and other non-CA software packages; configure and maintain the networking operations; establish and maintain system accounts; and configure OS audit parameters.
4. Registration Authorities – authorized to request certificates or certificate revocations

The CPS may further define these roles, as well as define additional Trusted Roles to provide further role separation.

5.2.1.1. Separation of Roles

Individual CA personnel shall be specifically designated to the four roles defined in section 5.2.1. Individuals may assume more than one role, however, individuals who assume a Security Officer role may not assume a System Administrator role and associated function.

5.2.2. Number of Persons Required Per Task

Two or more persons are required for the following tasks:

- CA Key Generation
- CA Signing Key Activation
- CA Key Backup.
- Direct physical access to any HSM

All participants in the operation and management of the Fannie Mae PKI services must serve in a trusted role as defined in section 5.2.1. Multiparty control shall not be achieved using personnel that serve in the System Administrator role.

5.2.3. Identification and Authentication for Each Role

At all assurance levels other than Rudimentary, an individual shall identify and authenticate him or herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4. Roles Requiring Separation of Duties

Individuals who assume a Security Officer role may not assume a System Administrator role.

The CPS shall specifically designate individual CA personnel to the four roles defined in Section 5.2.1. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but generally, any individual may assume the Operator role. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and/or assume both the Auditor and Officer Roles. No individual shall have more than one identity.

Under no circumstances shall the incumbent of a Fannie Mae CMA or Fannie Mae CA Vendors role perform its own external compliance auditor function. Only a CA Auditor may perform internal compliance auditor functions. The Fannie Mae CA shall operate at the High Assurance level.

5.3. Personnel Controls

5.3.1. Background, Qualifications, Experience, and Security Clearance Requirements

The requirements governing the qualifications, selection and oversight of individuals who operate and manage the CA shall be set forth in the CPS.

5.3.2. Background Check Procedures

Background checks will be handled by standard Fannie Mae Human Resources hiring practices.

5.3.3. Training Requirements

All personnel performing duties with respect to the operation of the Fannie Mae CA or RA shall receive training in all operational duties they will perform, including disaster recovery and business continuity procedures. Training shall be conducted in all PKI duties they are expected to perform.

5.3.4. Retraining Frequency and Requirements

Individuals responsible for CA roles shall be made aware of changes in the CA operation. Any significant change to the operations shall include the appropriate training.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

Fannie Mae CA Vendors and Fannie Mae shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its repository which are not authorized in this CP, the CPS, or other procedures approved and made available by Fannie Mae to these individuals.

5.3.7. Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to the Fannie Mae CA shall meet applicable requirements as set forth in this CP and the applicable Enterprise Service Agreement.

5.3.8. Documentation Supplied to Personnel

Fannie Mae CA Vendors and Fannie Mae shall make available the Certificate policies, relevant parts of the CPS, and any relevant statutes, policies or contracts to those personnel supporting the Fannie Mae CA and associated Fannie Mae CA Systems and Services.

5.4. Audit Logging Procedures

5.4.1. Event Capture Criteria

The security auditing capabilities of CA operating system and CA applications shall be enabled during installation. At a minimum, the audit record shall include the following:

- The type of event;
- The date and time the event occurred;
- A success or failure indicator when executing the CA's signing process;
- A success or failure indicator when performing Certificate revocation; and
- The identity of the entity and/or operator that caused the event.
- Meet Fannie Mae Logging and Monitoring Standards.

5.4.2. Frequency of Processing Data

No stipulation.

5.4.3. Retention Period for Security Audit Data

The Fannie Mae CA services shall meet Fannie Mae Logging and Monitoring Standards.

5.4.4. Protection of Security Audit Data

The CA system configuration and procedures must be implemented together to ensure that:

- Only authorized people have read access to the logs;
- Only authorized people may archive audit logs; and
- Audit logs are not modified

Audit logs shall be moved to a secure storage location separate from the Fannie Mae CA systems equipment.

5.4.5. Security Audit Data Backup Procedures

The audit logs generated on the PKI equipment may be backed up on the same schedule as the rest of the data on the PKI equipment, but at a minimum must be backed up at least once per month. Audit log backups shall be moved once per week to a safe, secure storage location separate from the PKI equipment.

5.4.6. Security Audit Collection System (Internal vs. External)

There is no requirement for the audit log collection system to be external to the PKI. Audit processes shall be invoked at system startup, and cease only at system shutdown.

5.4.7. Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

5.4.8. Vulnerability Assessments

Vulnerability assessments of the Fannie Mae Enterprise Certificate Service are performed according to Fannie Mae's enterprise vulnerability assessment program and standards.

5.5. Records Archival

5.5.1. Types of Records Archived

CA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any Certificate (including those revoked or expired) issued by the CA.
At a minimum, the following data shall be archived in accordance with this CP and the applicable CPS:

Data To Be Archived
Certificate Policy
Certification Practice Statement
System and equipment configuration
Modifications and updates to system or configuration
Audit Logs

5.5.2. Retention Period for Archive

No stipulation.

5.5.3. Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. The contents of the archive shall not be released except as determined by Fannie Mae or as required by law. Records of individual transactions may be released upon Fannie Mae approval. Archive media shall be stored in a safe, secure storage facility separate from the CA.

5.5.4. Archive Backup Procedures

The CA system is backed up and archived as described in the CPS.
Archive copies are stored as described in 5.5.3

5.5.5. Requirements for Time-Stamping of Records

CA archive records shall be date and time-stamped.

5.5.6. Archive Collection System (Internal or External)

Archive data shall be collected in as described in the CPS.

5.5.7. Procedures to Obtain and Verify Archive Information

Procedures detailing how to obtain and verify archive information shall be published in the CPS.

5.6. Key Changeover

No Stipulation.

5.7. Compromise and Disaster Recovery

The CA shall has recovery procedures in place in the event of a catastrophic failure, as described in section 5.7.1 to 5.7.4.

5.7.1. Incident and Compromise Handling Procedures

The Fannie Mae CA Vendors and Fannie Mae Leadership shall be notified by Fannie Mae CMA Operations Staff and /or Fannie Mae Vendor CA staff if the CA experiences the following:

- Suspected or detected compromise of the CA
- Any incident preventing the CA from issuing a CRL within 8 hours.

Fannie Mae CA Vendors and Fannie Mae will take appropriate steps to protect the integrity of the PKI.
Fannie Mae CA Vendors and Fannie Mae shall deploy commercially reasonable efforts to reestablish operational capabilities in accordance with procedures set forth in the CPS.

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

If any of the Fannie Mae CA equipment is damaged or rendered inoperative, but the CA's signature keys are not destroyed, CA operation shall reestablish the ability to generate Certificate status information. Additionally, Fannie Mae shall be notified by Fannie Mae CMA Operations Staff and /or Fannie Mae Vendor CA staff as soon as possible.

5.7.3. Entity Private Key Compromise Procedures

If the CA signature keys are compromised or lost (such that compromise is possible even though uncertain) the CA's certificate shall be revoked per Fannie Mae approval and the revocation information shall be published immediately. In the event that the revocation information cannot be published immediately, Fannie Mae CA Vendors shall securely notify all interested parties as soon as possible. Subsequently, the CA installation shall be re-established. The Fannie Mae CA shall re-issue CA Certificates and notify Fannie Mae when Subscriber certificates can be re-issued.

Fannie Mae CA Vendors shall investigate and report to Fannie Mae what caused the compromise or loss and what measures have been taken to preclude recurrence.

5.7.4. Business Continuity Capabilities after a Disaster

In the case of a disaster whereby the Fannie Mae CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, then Fannie Mae shall be notified as soon as possible by Fannie Mae CMA Operations Staff and /or Fannie Mae Vendor CA staff, and the Fannie Mae PA shall initiate whatever action it deems appropriate.

5.8. CA Termination

In the event of termination of the Fannie Mae CA operation, Certificates signed by the terminated CA shall be revoked.

6. Technical Security Controls

6.1. Key Pair Generation

6.1.1. Key Pair Generation

Cryptographic keying material used by the CA to sign Certificates and CRLs shall be generated and stored in a FIPS 140-2 validated cryptographic module that meets or exceeds Fannie Mae CA Vendor Security Level 3. Multiparty control is required for CA key pair generation.

6.1.2. Subscriber Key Pair Generation

The CA or RAs may perform Subscriber key pair generation.

6.1.3. Key Delivery to Subscriber

A private key shall only be delivered to a Subscriber through authorized means by Fannie Mae CMA staff or automated services under their authority and control..

6.1.4. CA Public Key Delivery to Relying Parties

The Fannie Mae CA shall have its Public Key included in its Certificates for use by Relying Parties.

6.1.5. Key Sizes

The Fannie Mae CA Certificate Public Keys shall be at least 2048 bits, and be signed with the corresponding Private Key. All Certificates issued under this CP shall comply with the Fannie Mae Data Encryption Standard.

6.1.6. Public Key Parameters Generation and Quality Checking

All Certificates issued under this CP shall comply with the Fannie Mae Data Encryption Standard.

6.1.7. Key Usage Purposes

- Transmission Layer Security
- User and Device Identity and Authentication
- Code and Document Digital Signature (Integrity)
- Virtual Private Network (VPN) Services
- Data Encryption

6.2. Private Key Protection

6.2.1. Standards for Cryptographic Module

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules FIPS 140-2 level 3. The minimum FIPS 140-2 Level 3 requirements for a cryptographic module is as follows:

- CA Certificates issued under this CP shall use a FIPS 140-2 Level 3 hardware cryptographic module or higher.
- Subscribers shall use a FIPS 140-2 Level 1 or higher validated cryptographic module or higher.

6.2.2. Private Key Multi-Person Control

The CA private signing key may only be backed up under two-person control as set forth in 5.2.2.

6.2.3. Private Key Escrow

The Fannie Mae CA shall not escrow its signature keys. The Fannie Mae CA may escrow Subscriber Private Keys used for encryption, in order to provide key recovery, and for Fannie Mae Information Security Services indicated in Section 1.4.1

6.2.4. Private Key Backup

The CA shall be configured so that Subscriber private keys cannot be exported out of the Microsoft Cryptographic Service Provider.

6.2.5. Private Key Archival

CA private signature keys and Subscriber private signatures keys shall not be archived. Private Keys used for encryption may be archived in order to provide key recovery, and for Fannie Mae Information Security Services indicated in Section 1.4.1

6.2.6. Private Key Transfer into or from a Cryptographic Module

In the event that the CA root private key needs to be transported from one cryptographic module to another, the CA root Private Key must be encrypted during transport. Private Keys must never exist in plain text form outside of the cryptographic module boundaries.

6.2.7. Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS-140-2.

6.2.8. Method of Activating Private Key

CA signing key activation requires multiparty control as specified in 5.2.2.
Acceptable means of authentication shall be by PIN. Entry of activation data shall be protected from disclosure (i.e., data shall not be displayed while it is entered).

6.2.9. Method of Deactivating Private Key

CA Private Keys may be deactivated through any means defined by the cryptographic module provider. All cryptographic modules and/or controlling software shall include a timer which locks or deactivates Private Keys after a specified idle period. Hardware cryptographic modules shall deactivate CA Private Keys when disconnected from a power source.

6.2.10. Method of Destroying Private Key

Private signature keys shall be destroyed by the subscriber on their local system and by the FM CMA staff when they are no longer needed, or when the Certificates to which they correspond to expire or are revoked.

For CA Private Keys stored in the hardware cryptographic module, a “zeroize” command or passes of “1s” and “0s”, with a minimum of 3 passes will be executed. Physical destruction of hardware is not required.

6.2.11. Cryptographic Module Rating

Cryptographic modules shall be validated to the FIPS 140-2 Level 3 as identified in 6.2.1

6.3. Other Aspects of Key-Pair Management

Human Subscribers shall typically have one key-pair for digital signature, and a separate key-pair for encryption. A Subscriber's digital signature key-pair shall never be escrowed, archived, or backed-up, to maintain technical non-repudiation of transactions. For business continuity and security reasons, the CA may escrow, archive, or back-up encryption key-pairs.

6.3.1. Public Key Archival

No stipulation.

6.3.2. Usage Periods for the Public and Private Keys

The maximum key/certificate lifetime for the Fannie Mae CA shall be 20 (twenty) years.
The CA shall not issue Certificates that extend beyond the expiration dates of its own Certificates and Public Keys. Therefore, the CA Certificate validity period must be greater than those for Subscribers.
The maximum key / certificate lifetime for Subscribers may not exceed 3 years.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The activation data used to unlock CA Private Keys, shall have an appropriate level of strength for the keys or data to be protected. Activation data may be selected by Fannie Mae CA Vendors.

6.4.2. Activation Data Protection

Data used to unlock CA Private Keys shall be protected from disclosure via physical access control mechanisms. Activation data should be secured and not be stored with the cryptographic module.

The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CPS.

Subscribers must never share activation data for Private Keys associated with Certificates asserting individual identities. PKI Sponsors shall restrict activation data for Private Keys associated with Certificates asserting group, organizational, non-human component identities to those in the organization authorized to use the Private Keys.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its components shall include the following functionality:

- Require authenticated logins
- Restrict access control to CA services and PKI roles
- Archive audit logs
- Require a recovery mechanism for the CA system
- Be in compliance with Fannie Mae Access Control Standard

For remote workstations used to administer the any Fannie Mae CA and associated components, 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; (see section 5.4)
- Enforce domain integrity boundaries for security critical processes;
- Support recovery from key or system failure; and
- All communications between any PKI trusted role and the CA shall be authenticated and protected from modification.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life-Cycle Technical Controls

6.6.1. System Development Controls

The System Development Controls for the Fannie Mae CA and RA are as follows:

- The CA shall use software that has been designed and developed under a formal, documented development methodology.
- Software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented (this requirement does not apply to commercial off the shelf hardware or software)
- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software, which are not part of the CA operation
- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA shall be loaded.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel.

6.6.2. Security Management Controls

The configuration of the Fannie Mae CA system as well as any modifications and upgrades shall be documented and controlled.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

The Fannie Mae CMA shall employ and validate network security controls to protect the Fannie Mae CA, the Fannie Mae CA Certificate repositories, and Certificate Status Servers. The Fannie Mae CMA shall assure that all Fannie Mae CMA equipment is protected against known network attacks. The Fannie Mae PKI CA system administrator and or Fannie Mae CA Vendors shall turn off all unused network ports and services on the Fannie Mae CMA, and ensure that similar measures are taken on all guards, routers, and firewalls. Any network software present on Fannie Mae CMA equipment shall be necessary to the functioning of the Fannie Mae CMA application.

6.8. Time-Stamping

Asserted times shall be accurate to within three minutes. The Fannie Mae PKI CMA team, including any contracted Fannie Mae CA Vendors, may use electronic or manual procedures to maintain system time. Clock adjustments are auditable events.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

7.1.1. Version Numbers

The CA shall issue X.509 v3 certificates.

7.1.2. Certificate Extensions

No Stipulation.

7.1.3. Algorithm Object Identifiers

The CA under this CP MUST use the standard OIDs for both the signatures and subject keys corresponding to the type of asymmetric encryption used.

7.1.4. Name Forms

Certificate name forms shall be x.501 Distinguished Names as described in 3.1.1 Distinguished Names shall be composed of standard attribute types.

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

Certificates issued by the Fannie Mae CA may contain policy OIDs per the CPS.

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 Policy Extension

No stipulation.

7.2. CRL Profile

All CRLs shall be published in accordance with all requirements established by this CP.

7.2.1. Version Numbers

The CA shall operate using X.509 standards.

7.2.2. CRL Entry Extensions

No stipulation.

7.3. OCSP Profile

7.3.1. Version number(s)

No stipulation.

7.3.2. OCSP Extensions

No stipulation.

8. Compliance Audit and Other Assessment

8.1. Frequency or Circumstances of Assessment

No stipulation.

8.2. Identity/Qualifications of Assessor

No stipulation.

8.3. Assessor's Relationship to Assessed Entity

No stipulation.

8.4. Topics Covered By Assessment

No stipulation.

8.5. Actions Taken as a Result of Deficiency

No stipulation.

8.6. Communication of Results

No stipulation.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

Not applicable to End Entities.

There may be fees set forth by the Enterprise Service Agreement(s) between Fannie Mae CA Vendors and Fannie Mae, and applicable Service Orders and Service Requests, as applicable.

9.1.2. Certificate Access Fees

Section 2.4 of this CP requires that CA Certificates and CRLs be publicly available. CAs operating under this CP must not charge additional fees for access to this information.

9.1.3. Revocation or Status Information Access Fees

CAs operating under this CP must not charge additional fees for access to CRLs and OCSP status Information.

9.1.4. Fees for Other Services

Not applicable.

9.1.5. Refund Policy

Not applicable.

9.2. Financial Responsibility

Governed by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity.

9.2.1. Insurance Coverage

Not applicable.

9.2.2. Other Assets

Not applicable.

9.2.3. Insurance or Warranty Coverage for End Entities

The CA does not provide insurance or warranty coverage to End Entities other than specified in the relevant End Entity Agreement.

9.3. Confidentiality of Business Information

Confidentiality provisions and obligations of the participants to the PKI are set forth in this CP and the Enterprise Service Agreements or the End Entity Agreements, as applicable.

PKI information shall be made available at Fannie Mae's discretion. Fannie Mae shall protect the confidentiality of sensitive business information stored or processed on CA systems that could lead to abuse or fraud. For example, Fannie Mae shall protect customer data that could allow an attacker to impersonate a customer.

Public access to CA organizational information shall be determined by Fannie Mae.

9.3.1. Scope of Confidential Information

The scope of confidential information is presented in related CPS documents.

9.3.2. Information not within the Scope of Confidential Information

Any information not listed as confidential in the CPS is considered public information. Published certificate and revocation data is considered public information.

9.3.3. Responsibility to Protect Confidential Information

Confidential information is stored securely by Fannie Mae, and shall only be released in accordance with other stipulations in section 9.4.

9.4. Privacy of Personal Information

No stipulation.

9.4.1. Privacy Plan

Certificates and CRLs are not considered private information for the purposes of this CP. Fannie Mae shall document what personally identifiable information is collected, if any, and how it is stored and processed, and under what conditions the information may be disclosed.

9.4.2. Information Treated as Private

The CA shall not query private information for any purpose other than the issuance and management of Certificates. The CA shall not query any more information than is necessary for that purpose. CAs shall protect all Subscriber personally identifiable information from unauthorized disclosure. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by the CAs operating under this CP shall not be released except as allowed by Fannie Mae.

9.4.3. Information not Deemed Private

The CA shall only use information queried by the CA or RA for the purpose of issuing and managing Certificates under this CP and information included in Certificates shall not be deemed private, and will not be subject to the protections outlined in Section 9.4.2 of this CP.

9.4.4. Responsibility to Protect Private Information

Subject to this Policy, and the limitations and restrictions imposed by applicable law, the CA and any RA may query private information only to assist in the issuance and management of Certificates. All disclosures under this Policy shall be coordinated through Fannie Mae. Sensitive information must be stored securely, and may be released only in accordance with other stipulations in section 9.4.

Any release of specific restricted or confidential information is governed by applicable policies. Any questions concerning the use of confidential information, including personal private information by the CA system should be addressed to Fannie Mae.

9.4.5. Notice and Consent to Use Private Information

The CA may not provide any notice or obtain the consent of the Subscriber in order to release private information in accordance with other stipulations of section 9.4. Personal data contained in a Certificate may be published in online public repositories, and all Subscribers consent to the global publication of any personal data contained in Certificates.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

The CA shall not disclose private information to any third party unless authorized by this CP, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7. Other Information Disclosure Circumstances

Not applicable unless as provided under the Enterprise Service Agreements or End Entity Agreements.

9.5. Intellectual Property Rights

Governed by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity. The CA hereby grants End Entities a limited license to access and use the Certificates for the purposes set forth herein.

9.6. Representations and Warranties

The obligations described below pertain to all participants in the PKI Service. They are governed by this CP and supplemented by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity.

9.6.1. CA Representations and Warranties

Fannie Mae, or an appointed delegate, shall –

- Approve the CPS for the Fannie Mae CA;
- Revise this Fannie Mae KPI CP as necessary to maintain the level of assurance and operational practicality;
- Publicly distribute this Fannie Mae KPI CP as required
- Coordinate modifications to this Fannie Mae KPI CP to ensure continued compliance.

Authorize deviations from defined practices as required in the event of a crisis, as long as the deviations are not contradictory to the approved CP.

CAs operating under this CP warrant that their procedures are implemented in accordance with this CP, and that any certificates issued that assert the policy OIDs identified in this CP are issued in accordance with the stipulations of this CP.

A CA that issues Certificates that assert a policy defined in this document shall conform to the stipulations of this document, including—

- Providing a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an 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.
- 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.

9.6.2. RA Representations and Warranties

Fannie Mae Service Line (CMA) shall –

- Develop, maintain and submit to Fannie Mae, for review and approval, a CPS for the CA that is participating in PKI Service.
- Ensure that the Certificate Authority, Repository, Registration System, and other PKI-related components are operational in accordance with this CP and the applicable CPS.

9.6.3. Subscriber Representations and Warranties

Governed by the applicable End Entity Agreement as between Fannie Mae and a Subscriber.

Further, Fannie Mae, Fannie Mae partners, Fannie Mae contractor and employees, or others authorized by Fannie Mae that are assigned to Trusted Roles will use the same standards as noted in Section 9.4.

A Subscriber (or AOR for device certificates) is required to acknowledge acceptance of the requirements the Subscriber shall meet respecting protection of the private key and use of the Certificate before being issued the Certificate.

Subscribers shall:

- Accurately represent themselves in all communications with the PKI authorities.
- Provide accurate and complete information to the PKI authorities at all times.
- Protect their private key(s) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.

© 2018 Fannie Mae.

- 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 the CA's CPS.
- Use the certificate only for authorized and legal purposes, consistent with the relevant CPS and End Entity Agreement.
- Promptly cease using the certificate and related private key after the certificate's expiration..
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

9.6.4. Relying Party Representations and Warranties

An RA who performs registration functions as described in this CP shall comply with the stipulations of this CP and comply with a CPS approved by Fannie Mae for use with this CP. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

An RA supporting this CP shall conform to the stipulations of this document, including –

- Maintain operations in conformance to the stipulations of the approved CPS
- Include only valid and appropriate information in Certificate requests.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

Governed by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity.

9.8. Limitations of Liability

9.8.1. Severability of Provisions, Survival, Merger, and Notice

Governed by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity..

9.9. Indemnities

Governed by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity.

9.10. Term and Termination

Governed by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity.

9.10.1. Term

This CP becomes effective when approved by the Fannie Mae CISO. This CP has no specified term.

9.10.2. Termination

Termination of this CP is at the discretion of the Fannie Mae CISO.

9.10.3. Effect of Termination and Survival

The archive requirements of this CP remain in effect through the end of the archive period for the last certificate issued. Other requirements concerning the organization and operations of the Fannie Mae PKI; Certificates application, usage, and revocation; physical and technical security controls; audits; and other business and legal requirements shall remain in effect through the expiration date of the last certificate issued and/or cessation of operations and closure of the Fannie Mae PKI.

9.11. Individual Notices and Communications with Participants

No stipulation.

9.12. Amendments

Fannie Mae CA Vendors or Fannie Mae may propose amendments to any part of this document at any time. All proposed changes must be recorded in a change request document that is to be reviewed and approved by Fannie Mae.
Fannie Mae CA Vendors or Fannie Mae are not obligated to notify subscribers of any amendments to any documentation.

The most current version of this CP as published by Fannie Mae shall be the governing version.

Amendments to the Software Subscription Agreement or the Enterprise Service Agreement are governed by those agreements.

9.12.1. Procedure for Amendment

Refer to section 1.5.4 of this CP and associated CPS document.

9.12.2. Notification Mechanism and Period

Refer to sections 1.5.4 of this CP and associated CPS document.

9.12.3. Circumstances under Which OID Must be Changed

No stipulation.

9.13. Dispute Resolution Provisions

Fannie Mae shall resolve any disputes associated with the use of the Fannie Mae PKI service or certificates issued by the Fannie Mae PKI service.

9.14. Governing Law

Governed by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity.

9.15. Compliance with Applicable Law

Governed by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

Except where specified by contract, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party (such consent not to be unreasonably withheld), except that Fannie Mae may assign and delegate this CP to any party of its choosing without approval.

9.16.3. Severability

Governed by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity..

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

Governed by the applicable Enterprise Service Agreement as between Fannie Mae and a Fannie Mae (CA) Vendor, and by the applicable End Entity Agreement as between Fannie Mae and an End Entity. Any failure to exercise any right hereunder by Fannie Mae shall not be construed as a relinquishment of any future exercise of such right.

9.16.5. Force Majeure

No participant to the Fannie PKI under this CP shall be liable for any default or delay (a) if and to the extent the default or delay is caused, directly or indirectly, by fire, flood, elements of nature or acts of God or any other similar cause beyond the reasonable control of the party (a "Force Majeure Event") and (b) provided the non-performing participant is without fault in causing the Force Majeure Event and the default or delay could not have been prevented by reasonable precautions.

9.16.6. Other Provisions

No stipulation.

© 2018 Fannie Mae.