

# Certification Practice Statement of the Federal Reserve Banks' Services Public Key Infrastructure

## 1.0 INTRODUCTION

### 1.1 Overview

The Federal Reserve Banks operate a public key infrastructure (PKI) that manages digital certificates and the associated cryptographic keys of parties requiring access to Federal Reserve business applications. Digital certificates issued from the Federal Reserve Banks' Services Certification Authority enable authentication, key management, and digital signing capabilities in both client-to-server and server-to-server interactions. This document, a Certification Practice Statement (CPS) for the Federal Reserve Banks, describes the requirements for the issuance, management and usage of those certificates, including the practices to be used by the Federal Reserve Banks and the obligations of certificate users.

For purposes of this CPS, the requirements, practices, and obligations it contains are intended to apply to operations of the Federal Reserve Banks' Services CA (FRBS-CA).

This CPS applies to operations and services of the above-stated domain to the exclusion of all others, and sets out to identify the roles, responsibilities, and practices of entities involved in the lifecycle, use, and reliance on certificates it issues.

This CPS follows the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, *Certificate Policy and Certification Practice Framework*, with regard to content and organization. While certain topics are included in this CPS in accordance with RFC 3647, those topics may not necessarily apply to the implementation of certificate management services provided by the CA identified above. For those topics where the FRBS-CA imposes no requirement or elects not to disclose requirements through this CPS, the document will state "no stipulation".

Unless indicated otherwise, the certificates issued under this CPS are intended only to be used to authenticate the identity of the Subscriber to those established and recognized as Relying Parties. The CA operated by the Federal Reserve Banks promotes that service by providing confirmation to Relying Parties of the unique association between the Subscriber and her or his public key, as established during registration. Therefore, the requirements, practices, and obligations described in this document exist to provide adequate and positive confirmation of Subscriber identities for specified purposes and for a specified period of time.

This CPS represents only one document relevant to the Federal Reserve Banks' Services PKI, and may be joined by other documents including ancillary security and operational documents necessary to facilitate certificate management practices.

## 1.2 Document Name and Identification

This CPS is to be recognized as the *Certification Practice Statement for the Federal Reserve Banks' Services Public Key Infrastructure*. The current issue is version 1.0, and is dated February 22, 2011.

The certificates issued under this CPS will be differentiated by intended use and the associated form factor, as designated by distinct policy Object Identifiers (OID). The policy OIDs covered by this CPS are limited to the following:

Policy	OID Value
FR-certpolicy OBJECT IDENTIFIER	::={1.3.6.1.4.1.7611.100.1}
prod- softcert	::={FR-certpolicy 1}
prod- usbtokencert	::={FR-certpolicy 2}
prod-testtoolcert	::={FR-certpolicy 3}

Other certificate types may be defined and issued under this CPS, including those designated through the creation of additional policy OIDs, as necessary to meet business requirements of the Federal Reserve Banks. These may include but are not limited to server certificates and object signing certificates.

No policy OID has been assigned to this CPS, as use of policy OID by the Federal Reserve Banks will remain consistent with IETF and X.509 standards to only distinguish certificates by type or class.

## 1.3 Roles Defined under this CPS

### 1.3.1 Certification Authority

For purposes of this CPS, all references to Certification Authority mean the FRBS-CA as operated on behalf of the twelve Federal Reserve Banks in the United States of America. FRBS-CA has been established to issue certificates within a specified context and is limited to the issuance and management of end-entity certificates, including the facilitation of certificate validation by Relying Parties. The FRBS-CA is not authorized to issue root certificates, cross certificates, or to otherwise establish trust or hierarchical relationships with other CAs independent of the Federal Reserve Banks' Services Root CA.

In accordance with its stated purpose, the responsibilities of the FRBS-CA comprise the management of certificates it issues, including:

- Issuance
- Revocation
- Rekey/Modification
- Status Validation
- Directory Services

The FRBS-CA is specifically responsible for the following:

- Acting in accordance with policies and procedures designed to safeguard the certificate management process (including certificate issuance, key roll-over, certificate revocation, and audit trails) and to protect the private key of the FRBS-CA.
- Validating information submitted by a Federal Reserve Bank Information Security Officer that gives appropriate officials of the Federal Reserve Banks certain RA responsibilities.
- Ensuring that there is no duplication of a Subscriber's name (as defined in the distinguished name of the Subscriber's certificate).
- Issuing a certificate to a Subscriber after a properly formatted and verified certificate request is received.
- Creating and maintaining an accurate Certificate Revocation List (CRL).
- Notifying the Participant of a revoked FRBS-CA server certificate used for special connectivity purposes.
- Maintaining the CPS.
- Creating and maintaining an accurate audit trail.

### **1.3.2 Registration Authority**

Certain responsibilities and practices described in this CPS apply to a Registration Authority (RA), which has been established in the Federal Reserve Banks for purposes of collecting and processing Subscriber requests for digital certificates and to facilitate issuance where appropriate. In fulfilling its responsibilities, the RA will also interact with the FRBS-CA to request certificate revocation according to the requirements specified in this CPS.

It is primarily the responsibility of the RA to submit to the FRBS-CA all data necessary for the generation and revocation of certificates. In doing so, the RA:

- Accepts requests for certificates
- Follows its internal procedures to validate those requests
- Registers Subscribers with the FRBS-CA's certification services
- Notifies the FRBS-CA to issue certificates in response to validated requests
- Provides Subscribers and EUACs with information necessary to retrieve certificates issued from the FRBS-CA
- Initiates the process to suspend, reinstate, or revoke certificates where required

The RA performs these functions under delegation from the FRBS-CA and acts in accordance with approved practices, procedures, and policies of the FRBS-CA, including those provided in this CPS. As noted in section 1.3.5, with approval of the FRBS-CA, some functions assigned to the RA may be further delegated to other participating entities in order to facilitate certificate issuance or other aspects of certificate lifecycle management.

### **1.3.3 Subscribers and Participants**

Under this CPS, a Subscriber is a named individual employee or agent of a Participant who will use certificates issued by the FRBS-CA for access to business applications of the Federal Reserve Banks. Subscribers are expected to be natural persons that have successfully completed all certificate issuance requirements. A Participant is a depository institution or other authorized entity seeking access to Federal Reserve Bank business applications. The Participant has overall responsibility and is liable, as described in this CPS, for all certificates issued to that Participant's Subscribers. A Participant's End User Authorization Contacts (EUAC) are solely responsible for the identification, authentication and notification processes between the Participant and the RA with respect to Subscribers.

Under specific circumstances involving special connectivity requirements such as file transfer and messaging utilities, a Technical Contact that is not named in the certificate but is authorized to receive a certificate will be considered a Subscriber and is, therefore, subject to the obligations of a Subscriber.

For other specific circumstances, a Subscriber may be a named individual employee or contractor of a Federal Reserve Bank who will use certificates issued by the FRBS-CA in the conduct of her or his assigned roles and responsibilities. Certain provisions of this CPS, including those in section 9.0 of this document, do not apply to Subscribers who are employees or contractors of a Federal Reserve Bank. Other processes related to the issuance of certificates to employees or contractors of the Federal Reserve Banks may also be tailored based on organizational requirements.

Subscribers must comply with all the provisions of this CPS, including but not limited to the following specific Subscriber obligations:

- (a) Maintaining, for server-based and browser-based certificates, the confidentiality of the authorization code obtained from the Participant's EUAC and the reference number obtained from the RA. The authorization code and reference numbers are for the exclusive use of the Subscriber to generate a server-based or browser-based certificate, or to recover a browser-based or token-based certificate.
- (b) Maintaining, for token-based certificates, the security of the token and the confidentiality of the token-pass phrase, which are for the exclusive use by the Subscriber to access and use the token-based certificate.
- (c) Retaining exclusive control of the private key associated with each certificate issued by the FRBS-CA to that Subscriber. The Subscriber shall not divulge the contents or any other data of the private key, or the applicable password or token-pass phrase protecting the private key, to any other person or entity.
- (d) For server-based and browser-based certificates, specifying and always using with applicable software, a password of at least eight alphanumeric characters to protect any and all private keys associated with the FRBS-CA. Software that does not allow the use of passwords to protect the private key may be used by the Participant and Subscriber, but the risk of use of such software by the Participant and Subscriber, namely the greater risk of the occurrence of a Private Key Compromise Event, is strictly that of the Participants.
- (e) Notifying the EUAC immediately if the Subscriber is unable to recall the password for the Web browser, Web server, or other storage media that protects the Subscriber's private key, or knows or suspects that a Private Key Compromise Event has occurred. The Participant shall be wholly responsible for all Private Key Compromise Events.
- (f) Discontinuing, if a Private Key Compromise Event occurs, use of a compromised private key and destroying the private key and any related certificate.
- (g) Notifying the EUAC if the Subscriber has not received the reference number for a server-based or a browser-based certificate, or the token-pass phrase for a token-based certificate within seven (7) business day of submitting the Subscriber request.
- (h) Notifying the EUAC immediately if the reference number, the token, or token-pass phrase is received by a physical means that displays evidence of tampering.

- (i) Notifying the EUAC immediately if a Subscriber attempts to use the reference number and authorization code provided to the Subscriber, but is unable to generate or recover a server-based or a browser-based certificate, or if a Subscriber attempts to use the token-based certificate and other applicable security procedures, but is unable to access an authorized Federal Reserve Bank business application.
- (j) UTILIZING CERTIFICATES AND PRIVATE KEYS SOLELY IN THE MANNER FOR WHICH THEY ARE INTENDED, I.E., ONLY TO ACCESS A FEDERAL RESERVE BANK BUSINESS APPLICATION.

Once the FRBS-CA has issued a certificate to the Subscriber, thereby granting the Subscriber access to a Federal Reserve Bank business application, any instructions sent thereafter which utilize that certificate will bind the Participant as fully as if the instructions had been expressly authorized and sent by the Participant. The Participant will be solely responsible for the use or misuse of any certificate issued by the FRBS-CA to any Subscriber authorized by the Participant.

The Participant has overall responsibility and is liable, as described in this CPS, for all certificates issued to that Participant's Subscribers. Specifically, the Participant has the following responsibilities and obligations:

- Identifying the names and contact information for at least two (2) Participant End User Authorization Contacts (EUACs). The identification must be provided to the RA in writing, and must be signed and dated by an authorized Participant representative.
- Informing the RA, in accordance with that RA's then-standard procedures, of all updates and substitutions made for the EUACs.
- Providing the RA all necessary Subscriber information to request a Subscriber certificate.
- Ensuring that the Participant's Subscribers comply with all instructions, guides, or other documentation related to certificates. The Participant is solely responsible for distributing this CPS to its Subscribers, and for ensuring that the Subscribers comply with all the provisions of this CPS.
- For any certificate issued to a Technical Contact, the Participant must notify the RA if the Technical Contact no longer has the responsibility for the Participant's electronic agent or special connectivity requirements. Such notification must be

made prior to the termination or reassignment of any Technical Contact (or if impossible, immediately after) and must include a designation by the Participant's EUAC of the new Technical Contact.

A Participant's End User Authorization Contacts (EUAC) are solely responsible for the identification, authentication and notification processes between the Participant and the RA with respect to Subscribers. The FRBS-CA has no responsibility for, and may rely entirely upon the EUACs to validate the identity and authority of that Participant's Subscribers, and the Subscribers' roles within the Federal Reserve Banks' business applications. For all certificates issued to employees or agents of the Federal Reserve Banks, the activities required of the EUAC will be performed by the Subscriber's management. Specifically, the EUAC has the following responsibilities and obligations:

- All notices provided by an EUAC must be sent to the RA in accordance with that RA's instructions.
- Keeping confidential any authorization codes supplied to the EUAC by the RA.
- Providing any applicable authorization code or token to the Subscriber only after the EUAC has validated the identity of the Subscriber and verified the Subscriber is authorized to access a Federal Reserve business application. Authorized materials should be provided to Subscribers in a timely manner.
- Notifying the RA immediately if a certificate should not be issued to a proposed Subscriber.
- Notifying the RA immediately following the occurrence of any of the following events:
  - (a) The EUAC has not received for a server-based or a browser-based certificate, the authorization code or for a token-based certificate, the token itself, within seven (7) business days of submitting a Subscriber request;
  - (b) The Subscriber has not received, for a server-based or a browser-based certificate, the reference number or, for a token-based certificate, the token-pass phrase within seven (7) business days of the EUAC submitting the Subscriber request;
  - (c) The EUAC or the Subscriber receives, for a server-based or a browser-based certificate, an authorization code, reference number, or, for a token-based certificate, the token or token-pass phrase by a physical means that displays evidence of tampering;

- (d) A Subscriber attempts to use the authorization code and reference number, but is unable to generate or recover a server-based, browser-based certificate; or
  - (e) A Subscriber attempts to use the token-based certificate but is unable to access an authorized Federal Reserve business application.
- Except for certificates issued to a Technical Contact, at least one of the Participant's EUACs must notify the RA prior to (or if impossible, immediately after) the occurrence of any of the following events:
    - (a) a Subscriber's employment with the Participant is terminated;
    - (b) a Subscriber no longer requires or is authorized to have access to any Federal Reserve Bank business applications;
    - (c) for browser-based certificates, a Subscriber is unable to recall the password for the Web browser, Web server or other storage media that protects the Subscriber's private key;
    - (d) for browser-based certificates and token-based certificates, a Subscriber is unable to properly roll-over keys or is unable to properly recover a certificate and associated keys; or
    - (e) the Subscriber knows or suspects that his or her private key or the password used to protect the private key has been disclosed to, or is known by, any other person or entity, or the token or other storage media for the certificate is lost, stolen or compromised.

Any such notice automatically constitutes a Participant's request that the Subscriber's certificate be revoked or, in the case of key roll-over, that the certificates or their associated keys be updated. In addition, for token-based certificates, a Subscriber's certificate may be revoked if the token becomes locked out.

- For any certificate issued to a Technical Contact, the Participant must notify the RA if the Technical Contact no longer has the responsibility for the Participant's electronic agent or special connectivity requirements. Such notification must be made prior to the termination or reassignment of any Technical Contact (or if impossible, immediately after) and must include a designation by the Participant's EUAC of the new Technical Contact.

#### **1.3.4 Relying Parties**

Relying parties to the Federal Reserve Banks' PKI will generally be limited to the Federal Reserve Banks for purposes of permitting Subscriber access to Federal Reserve Bank business applications.

Under other specific but limited circumstances defined by the FRBS-CA, Participants may be Relying Parties to the Federal Reserve Banks' PKI. The Relying Party may be the Participant in situations where the Participant's browser connects to the Federal Reserve Bank server and the Subscriber is sent digitally signed executable object code related to a Federal Reserve Bank business application, along with a certificate issued by the FRBS-CA. If the Participant's browser verifies the signature and accepts the certificate, the browser will load the object code. If the browser cannot verify the signature, the browser will post a message stating that the signature has come from a web site that cannot be identified. If such a message is posted, the Participant should not execute the object code and should contact the RA immediately. Additionally, the Participants may be Relying Parties with respect to mutual authentication of Federal Reserve Bank and Participant servers in order to meet certain special connectivity requirements with the Federal Reserve Banks.

In no event will entities other than the Federal Reserve Banks or Participants be recognized as Relying Parties.

The Federal Reserve Banks will not issue certificates for purposes of authentication to third-party applications or in support of third-party services except where specifically authorized by the Federal Reserve Banks and as stated in this CPS.

Where certificate status services are provided by the FRBS-CA, Relying Parties are expected to consider revocation status information during certificate validation and prior to relying on certificates issued by the FRBS-CA or any information contained within those certificates, as well as other specific obligations described in this CPS.

#### **1.3.5 Other participants**

No stipulation.

### **1.4 Certificate usage**

Certificates issued by the FRBS-CA are to be used solely for access to business applications of the Federal Reserve Banks and are not for use by, nor with, any entity other than those established by the FRBS-CA as Relying Parties. This includes authentication and other assurances of identification.

Subscriber certificate use is specifically restricted through key usage certificate extensions and extended key usage certificate extensions. Any use of the certificates that is inconsistent with those extensions, whether by Subscribers or Relying Parties, is not permitted.

## 1.5 Policy administration

This CPS, along with other documented policies and standards supporting operations of the FRBS-CA, is administered by the Federal Reserve Banks.

## 1.6 Definitions and Acronyms

### 1.6.1 Definitions

Activation Data	Data, other than keys, that is required to access or operate cryptographic modules (e.g., a "PIN")
Authentication	A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and verifying such relationship
Authority Revocation List (ARL)	A list of revoked CA certificates.
Certificate	The public key of a subject and the associated information, digitally signed with the private key of the issuer
Certificate Revocation List	A list maintained by the certificate issuer of all certificates that have been revoked prior to their expiration
Certification (Certificate) Authority	An entity that is trusted to associate a public key to the information on the subject, as contained in a certificate.
Certification Practice Statement	A document summarizing the processes, procedures, and other prevailing conditions used in the management of certificates throughout their life cycle
Certificate Policy	A set of rules governing the operation and practices of a CA and establishing the conditions of issuance, revocation, etc, of certificates issued by that CA; also used by Relying Parties to establish the trustworthiness of a PKI

Digital Signature	The data produced by transforming an electronic record or document using public key cryptography and the private key of the signer, allowing a recipient to accurately determine whether the data produced by the transformation was generated using the signer's private key that corresponds to a specific public key and whether the original electronic record or document has been altered since that transformation.
Directory	Database of certificate status information
Distinguished Name	A name used in certificates, and comprised of one or more attributes, to uniquely identifies the Subject
Object Identifier	A unique alphanumeric value representing a specific object or object class
Online Certificate Status Protocol	An online protocol that allows Relying Parties to determine the status of an identified certificate via a responder that interacts directly with the CA's repository.
Participant	See section 1.3.3
PKCS#10	A Public Key Cryptography Standard published by RSA Laboratories and establishing the syntax for certification requests consisting of certification request information (distinguished name, public key, and other necessary attributes), a signature algorithm identifier, and a digital signature. This standard is also republished by the IETF as RFC 2986.
PKCS#12	A Public Key Cryptography Standard published by RSA Laboratories and establishing a transfer syntax for personal identity information, including private keys, certificates, miscellaneous secrets, and extensions. This syntax allows users to import, export, and store personal identity information under one or more of several privacy and integrity modes.
Private Key Compromise Event	Any set of circumstances in which the Subscriber's private key or the password protecting the Subscriber's private key is known or thought to be known by any person or entity other than the Subscriber.

Public Key Infrastructure	A set of hardware, software, people, procedures, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of certificates and their associated keys based on public key cryptography.
Registration Authority	A role that administers the registration process under delegated authority from the CA, and that processes requests for certificate issuance, reissuance, suspension, reinstatement, and revocation.
Relying Party	An organization that has received information that includes a certificate and digital signature verifiable with reference to a public key in the certificate and is in a position to make decisions based on assurances received through their trust in the certificate issuer.
Root CA	In a hierarchical PKI, the top-level CA and trust anchor for certificate validation.
Subject	The individual, device, or entity named in the Common Name (CN) section of a certificate's Subject field.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is signed by a root CA and whose activities are governed or constrained by that root CA.
Subscriber	The individual, device, or entity named in the Distinguished Name (DN) section of a certificate's Subject field.
Technical Contact	An individual who, although not named in a certificate, is authorized to receive that certificate and is subject to all obligations of a Subscriber
Token	A hardware device (e.g., smart card) or software component used to securely store a certificate and its associated private key for the purposes of performing cryptographic functions.

## 1.6.2 Acronyms

CA	Certification Authority
CN	Common Name
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
EUAC	End User Authorization Contact
FIPS	Federal Information Processing Standard
FRBS-CA	Federal Reserve Banks' Services CA
IETF	Internet Engineering Task Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organization Unit
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment

## 2.0 REPOSITORIES

The FRBS-CA maintains repositories to support Federal Reserve PKI operation, and will at a minimum ensure that those repositories contain all certificates issued by the FRBS-CA and all Certificate Revocation Lists (CRLs) it publishes.

The Federal Reserve Banks will publish other information concerning the FRBS-CA or the PKI services it delivers where deemed necessary to support its continued use and operations, or as needed to meet its obligations to Relying Parties. This repository will be maintained at the FRBS-CA's URL at <<https://profile.federalreserve.org>>.

All information maintained in the repositories but not intended for public dissemination will be protected by logical and physical access controls sufficient for restricting access and preventing unauthorized additions, deletions, duplication or modification. Information maintained in the repositories and made publicly available will also be sufficiently protected from unauthorized additions, deletions, or modification.

### 3.0 IDENTIFICATION AND AUTHENTICATION

#### 3.1 Naming

##### 3.1.1 Types of Names

The FRBS-CA will only generate and sign certificates that contain a non-null X.501 Distinguished Name (DN) in the Issuer and Subject fields. For that purpose, the certificate subject attribute in certificates issued to external Subscribers will contain the following attributes and values:

Attribute:	Value:
Country Name	US
Organizational Name	Federal Reserve Banks
Organizational Unit	Routing Transit Number (RTN) of Institution
Common Name	Subscriber name, as specified in 3.1.2

Certificates may be issued by the FRBS-CA using alternative name forms, including those issued to employees or agents of the Federal Reserve Banks. No other restrictions are placed on the types of names that can be used.

##### 3.1.2 Need Names to be Meaningful

Names used will identify the natural person, legal person, or object to which they are assigned in a meaningful way and in a manner permitting the determination of the identity of the certificate Subscriber. The name assigned to the common name attribute will generally be composed of the Subscriber's first name, followed by a space, followed by the Subscriber's middle initial, followed by a space, followed by the Subscriber's surname.

##### 3.1.3 Anonymity or Pseudonymity of Subscribers

Pseudonymous certificates may be issued to Technical Contacts under this CPS where it supports internal operations of the Federal Reserve Banks or other approved special connectivity requirements of the Federal Reserve. Where a certificate is issued to a Technical Contact, the Common Name value will contain unique attributes related to the intended use of the certificate. DNs in pseudonymous certificates must satisfy name space uniqueness requirements, as specified in section 3.1.5, and must provide assurance for the accountability of actions performed on the basis of the pseudonymous certificates.

#### **3.1.4 Rules for Interpreting Various Name Forms**

Other terms, numbers, characters and letters may be appended to existing names to ensure the uniqueness of each name.

#### **3.1.5 Uniqueness of Names**

The FRBS-CA ensures that DNs are unique through automated components of the Subscriber enrollment process. The Organizational Unit (OU) and Common Name (CN) together generally form the basis for the uniqueness of each assigned name. The FRBS-CA reserves the right to assign in the certificate subject attribute a combination of the Participant's name, the Subscriber's name, surname, and other terms, numbers, characters or letters to ensure the uniqueness of each name.

#### **3.1.6 Recognition, Authentication, and Role of Trademarks**

No stipulation.

### **3.2 Initial Identity Validation**

#### **3.2.1 Method to Prove Possession of Private Key**

In cases where the Subscriber generates his or her own keys, the FRBS-CA will have proof that the Subscriber possesses the private key by validating the Subscriber's digital signature which is included as part of the certificate request. In cases where the private key is generated by the FRBS-CA or RA either directly on a hardware or software token or via a key generator that transfers the key to a token, proof of possession is not required.

#### **3.2.2 Authentication of Organization Identity**

The RA, using its internal procedures, will verify information submitted by a Participant in requesting recognition of an EUAC and the authorization of that individual to act in the name of the Participant. The EUAC will then represent and make all decisions for the Participant regarding certificate requests.

#### **3.2.3 Authentication of Individual Identity**

The Participant, through actions of the EUAC, must provide to the RA the necessary Subscriber information to request a certificate. A Participant's EUACs are solely responsible for the identification, authentication and notification processes between the Participant and the RA with respect to Subscribers.

### **3.2.4 Non-verified Subscriber Information**

Information that is not verified must not be included in the certificates issued by the FRBS-CA.

### **3.2.5 Validation of Authority**

See section 3.2.2.

### **3.2.6 Criteria for Interoperation**

No stipulation.

## **3.3 Identification and Authentication for Re-key Requests**

### **3.3.1 Identification and Authentication for Routine Re-key**

Subscribers will identify themselves for purposes of routine re-keying through use of the current signature key. Routine automated re-issuance of expiring certificates may exist for Subscribers and RAs, who, as part of the re-key process, may then be able to request new certificates based upon the validity of their existing, non-revoked certificates.

### **3.3.2 Identification and Authentication for Re-key after Revocation**

Requests for a certificate after revocation, other than that which might occur during routine rekey or certificate modification, must be processed in accordance with certificate issuance requests.

## **3.4 Identification and Authentication for Revocation Requests**

All revocation requests for Subscriber certificates must be submitted in writing or electronically by a Participant's EUAC and confirmed by the RA in order to be validated and processed. Requests to revoke a certificate issued to a named individual employee or contractor of a Federal Reserve Bank may be authenticated by digital signature using that certificate's public key, regardless of whether the associated private key is known or suspected to be compromised. Otherwise, requests to revoke a certificate issued a named individual employee or contractor of a Federal Reserve Bank must be submitted by the Subscriber's management and confirmed by the RA in order to be validated and processed.

## **4.0 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**

### **4.1 Certificate Application**

#### **4.1.1 Who Can Submit a Certificate Application**

For any Subscriber that is not also an EUAC, the certificate application must be submitted to the RA by an authorized EUAC for the corresponding Participant.

Certificate applications for EUACs must be submitted to the RA by another EUAC or another authorized representative of the Participant.

For any Subscriber that is a named individual employee or contractor of a Federal Reserve Bank, the certificate application must be submitted to the RA by that Subscriber's management.

#### **4.1.2 Enrollment Process and Responsibilities**

All requests to the FRBS-CA for certificates must include complete and accurate information. Each certificate produced by the FRBS-CA will be checked to verify that each field and extension is properly populated with correct information prior to delivery of the certificate to the Subscriber.

### **4.2 Certificate Application Processing**

A Participant's EUAC is solely responsible for the identification and authentication of external Subscribers for whom they submit certificate requests to the FRBS-CA. Likewise, for Subscribers that are named individual employees or contractors of a Federal Reserve Bank, the Subscribers' management is solely responsible for the identification and authentication of the Subscribers for whom they submit certificate requests.

The RA is solely responsible for validating certificate requests it receives as being complete and in proper format prior to submitting the request to the FRBS-CA.

The FRBS-CA will issue certificates within a reasonable time after receiving a properly formatted and validated certificate request from the RA.

### **4.3 Certificate Issuance**

The submission of a completed and properly formatted Subscriber certificate request by the Participant is a representation that its EUAC has validated the identity, authority and roles of the Subscriber to the RA. If submitted in error or if there is other reason to

believe the named individual should not be issued a certificate, the EUAC must immediately notify the RA.

Using the information provided by the EUAC, the RA will forward the validated request to the FRBS-CA for certification, which will then issue the certificate in a timely manner.

#### **4.3.1 CA Actions during Certificate Issuance**

##### **4.3.1.1 Issuance of Browser-based (Soft Token) Certificates**

Browser-based certificates will include the correct policy OID as specified in section 1.2. For all browser-based certificates issued to employees or agents of the Federal Reserve Banks, the activities required of the EUAC will be performed by the Subscriber's management.

For all browser-based certificates issued to employees or agents of a Participant, the submission of a complete and properly formatted certificate request by a Participant is a representation that the Participant's EUAC has successfully validated the identity, authority, and role of the Subscriber. Using the information provided by the EUAC, the RA will forward the validated request to the FRBS-CA for certification in a timely manner.

During the registration process, the RA will send the EUAC an authorization code, and through separate communications will send a reference number to the Subscriber.

Upon receipt of the reference number from the RA, the EUAC will provide that information to the Subscriber. The EUAC is solely responsible for communicating the authorization code to the Subscriber in a timely manner.

Upon receipt of the authorization code from the EUAC and the reference number from the RA, the Subscriber must access the appropriate interface to the FRBS-CA in order to submit a certificate request. Through this interface, presenting the reference number in combination with the authorization code uniquely identifies the Subscriber to the FRBS-CA.

Upon successfully presenting the correct combination of reference number and authorization code, the Subscriber will use his or her browser to interact with the FRBS-CA in the following manner:

- The Subscriber's browser, via a cryptographic security module, will generate an asymmetric key pair consisting of a public key component and a private key component.

- The public key component of the asymmetric key pair will be passed to the CA in the form of a cryptographically secure PKCS#10 certificate signing request.

Upon establishing proof of possession of the private key, as specified in section 3.2.1 of this Certification Practice Statement, the CA will sign the certificate, publish the certificate in the appropriate repositories, and will distribute the certificate to the Subscriber.

#### **4.3.1.2 Issuance of Hardware Token-based Certificates**

Hardware token-based certificates will include the correct policy OID as specified in section 1.2. For all hardware token-based certificates issued to employees or contractors of the Federal Reserve Banks, the activities required of the EUAC will be performed by the Subscriber's management.

For hardware token-based certificates issued to employees or agents of a Participant, the submission of a complete and properly formatted certificate request by a Participant is a representation that the Participant's EUAC has successfully validated the identity, authority, and role of the Subscriber. Using the information provided by the EUAC, the RA will forward the validated request to the FRBS-CA for certification, which will then issue the certificate in a timely manner.

During certificate issuance by the FRBS-CA, the RA will generate an asymmetric key pair using the capabilities of the hardware token and will interface with the FRBS-CA in order to submit the public key component of that asymmetric key pair for purposes of certificate signing by the FRBS-CA.

Upon the successful signing of the certificate by the FRBS-CA using information provided by the Participant, the RA will send the hardware token to the EUAC, who assumes responsibility for providing that token to the intended Subscriber. The EUAC is solely responsible for distributing the token to the Subscriber in a secure and timely manner.

The RA, through separate communication, will provide the Subscriber with the passphrase necessary for activating the private key component secured on the hardware token.

#### **4.3.1.3 Issuance of Browser-based (Soft Token) Certificates in Support of Automated Testing**

Browser-based certificates issued in support of automated testing will include the correct policy OID as specified in section 1.2.

For browser-based certificates issued in support of automated testing, the submission of a complete and properly formatted certificate request from appropriate Federal Reserve Bank management is a representation that they have successfully validated the identity, authority, and role of a Technical Contact assuming responsibilities of a Subscriber. Using the information provided by Federal Reserve Bank management, the RA will forward the validated request to the FRBS-CA for certification, which will then issue the certificate in a timely manner.

Upon certificate issuance by the FRBS-CA, the RA will send the representative of Federal Reserve Bank management an authorization code, and through separate communications, will send a reference number to the Subscriber.

Upon receipt of the authorization code from the RA, the representative of Federal Reserve Bank management will provide that information to the Subscriber. The representative of Federal Reserve Bank management is responsible for communicating the authorization code to the Subscriber in a secure manner.

Upon receipt of the authorization code from the representative of Federal Reserve Bank management and the reference number from the RA, the Subscriber must access the appropriate interface to the FRBS-CA in order to submit a certificate request. Through this interface, presenting the reference number in combination with the authorization code uniquely identifies the Subscriber to the FRBS-CA.

Upon successfully presenting the correct combination of reference number and authorization code, the Subscriber will interact with the FRBS-CA in the following manner:

- The Subscriber's browser, via a cryptographic security module, will generate an asymmetric key pair consisting of a public key component and a private key component.
- The public key component of the asymmetric key pair will be passed to the CA in the form of a cryptographically secure PKCS#10 certificate signing request.

Upon establishing proof of possession of the private key, as specified in section 3.2.1 of this Certification Practice Statement, the FRBS-CA will sign the certificate, publish the certificate in the appropriate repositories, and will distribute the certificate to the Subscriber.

The Subscriber, upon receiving the certificate from the FRBS-CA and as required to support use of the certificate for automated testing, may export the certificate and private key using the transfer syntax specified for personal identity information in the password privacy mode of PKCS#12.

#### **4.3.2 Notification of Subscriber by the CA of Issuance of Certificate**

No stipulation.

#### **4.4 Certificate Acceptance**

Prior to a Subscriber using her or his certificate or the corresponding private key, the Participant shall convey to the Subscriber her or his responsibilities as described in this CPS.

Failure of a Subscriber to object to a certificate issued by the FRBS-CA or its content constitutes acceptance of the certificate. When a certificate issued to a Subscriber is used to access a Federal Reserve Bank business application for the first time, the Subscriber and Participant are thereby deemed to have accepted the certificate and all relevant duties, responsibilities, and liabilities defined in this CPS.

#### **4.5 Key and Certificate Usage**

##### **4.5.1 Subscriber Private Key and Certificate Usage**

For all certificates issued under this CPS, the Subscriber must protect his or her certificate and the associated private keys from access by other parties. The Subscriber must not divulge the contents or any other data of the private key, or the applicable password or token-pass phrase protecting the private key, to any other person or entity.

Subscribers may use certificates issued by the FRBS-CA solely in the manner for which they are intended. Restrictions on the intended use for a private key will be specified through appropriate certificate extensions in the associated certificate, including key usage extension, the extended key usage extension, and private extensions where deemed necessary.

##### **4.5.2 Relying Party Public Key and Certificate Usage**

Relying parties may use certificates issued by the FRBS-CA solely in the manner for which they are intended. Restrictions on the intended usage by Relying Parties will be specified through appropriate critical certificate extensions in the associated certificate, including basic constraints and key usage extensions. Furthermore, the FRBS-CA will issue CRLs specifying the status of all unexpired certificates it has issued. Relying

parties are expected to process and comply with this information when placing reliance on certificates issued by the FRBS-CA.

## **4.6 Certificate Renewal**

### **4.6.1 Circumstances for Certificate Renewal**

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, the Subscriber attributes are unchanged, and renewal is authorized by the Participant.

For any Subscriber that is a named individual employee or contractor of a Federal Reserve Bank, certificate renewal requests must be authorized by that Subscriber's management.

### **4.6.2 Who May Request Renewal**

For certificates issued to external Subscribers, certificate renewal requests must be submitted to the RA by an authorized EUAC for the corresponding Participant. Submission of a completed and properly formatted certificate renewal request by the Participant is a representation that its EUAC has validated the identity, authority and roles of the Subscriber to the RA.

For any Subscriber that is a named individual employee or contractor of a Federal Reserve Bank, certificate renewal requests must be submitted by that Subscriber's management.

### **4.6.3 Processing Certificate Renewal Requests**

Only renewal requests received from the RA will be accepted by the FRBS-CA, and only after the RA has completed all required validation procedures. Renewal procedures must ensure that the person or entity seeking renewal is the Subject identified in the certificate's CN.

### **4.6.4 Notification of New Certificate Issuance to Subscriber**

No stipulation.

### **4.6.5 Conduct Constituting Acceptance of a Renewal Certificate**

Failure of a Subscriber to object to a renewed certificate issued by the FRBS-CA or its content constitutes acceptance of the certificate. When a renewed certificate issued to a Subscriber is used to access a Federal Reserve Bank business application for the first

time, the Subscriber and Participant are thereby deemed to have accepted the certificate.

#### **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**

Certificate rekey is the application for the issuance of a new certificate that certifies a new public key, and may be supported by the FRBS-CA for all certificate types and classes.

#### **4.7.1 Circumstances for Certificate Re-key**

Prior to the expiration of an existing Subscriber's certificate, it may be necessary for a Subscriber to request rekey of his or her certificate to maintain continuity of usage. Certificates may not be rekeyed after expiration.

For any Subscriber that is a named individual employee or contractor of a Federal Reserve Bank, certificate re-key requests must be authorized by that Subscriber's management.

#### **4.7.2 Who May Request Certification of a New Public Key**

Only re-key requests received from the Participant's EUAC, and validated by the RA, will be accepted by the FRBS-CA. Subscribers requesting re-keying must successfully identify themselves as specified in section 3.3.1 of this CPS.

For any Subscriber that is a named individual employee or contractor of a Federal Reserve Bank, certificate re-key requests must be submitted by that Subscriber's management.

#### **4.7.3 Processing Certificate Re-keying Requests**

Only rekey requests received from the RA will be accepted by the FRBS-CA, and only after the RA has completed all required validation procedures. Rekey procedures must ensure that the person or entity seeking renewal is the Subject identified in the certificate's CN.

#### **4.7.4 Notification of Re-keyed Certificate Issuance to Subscriber**

No stipulation.

#### **4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate**

Failure of a Subscriber to object to a rekeyed certificate issued by the FRBS-CA or its content constitutes acceptance of the certificate. When a rekeyed certificate issued to a Subscriber is used to access a Federal Reserve Bank business application for the first time, the Subscriber and Participant are thereby deemed to have accepted the certificate.

#### **4.7.6 Publication of the Re-keyed Certificate by the CA**

No stipulation.

#### **4.7.7 Notification of Certificate Re-Key by the CA to Other Entities**

No stipulation.

### **4.8 Certificate Modification**

#### **4.8.1 Circumstances for Certificate Modification**

Certificate modification is supported under this CPS prior to the expiration of the Subscriber certificate where necessary due to changes in the information in an existing certificate (other than the Subscriber's public key) in order to maintain continuity of certificate usage.

#### **4.8.2. Who May Request Certificate Modification**

See section 4.1 of this CPS.

#### **4.8.3. Processing Certificate Modification Requests**

Only certificate modification requests received from the RA will be accepted by the FRBS-CA, and only after the RA has completed all required validation procedures. After certificate modification, the old certificate may be revoked.

#### **4.8.4. Notification of Modified Certificate Issuance to Subscriber**

No stipulation.

#### **4.8.5. Conduct Constituting Acceptance of Modified Certificate**

Failure of a Subscriber to object to a modified certificate issued by the FRBS-CA or its content constitutes acceptance of the certificate. When a modified certificate issued to a Subscriber is used to access a Federal Reserve Bank business application for the first time, the Subscriber and Participant are thereby deemed to have accepted the certificate.

#### **4.8.6. Publication of the Modified Certificate by the CA**

No stipulation.

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

No stipulation.

### **4.9 Certificate Revocation**

#### **4.9.1 Circumstances for Revocation**

Any certificate issued to a named individual must be revoked by the FRBS-CA if it or the RA determines that any of the following events have occurred:

- (1) the Subscriber's private key or the password protecting the Subscriber's private key is compromised (i.e., known or thought to be known by any person or entity other than the Subscriber);
- (2) the Subscriber no longer requires access to any Federal Reserve Bank business application;
- (3) the Subscriber's employment or affiliation with the Participant is terminated;
- (4) the Subscriber's employment or affiliation with a Federal Reserve Bank is terminated in circumstances where Subscribers are a named individual employee or contractor of a Federal Reserve Bank;
- (5) the Subscriber loses the token on which a token-based certificate resides, or some other Private Key Compromise event occurs, to the certificate or the token;
- (6) the FRBS-CA or RA, in its sole discretion, believes revocation of a certificate is warranted; or
- (7) the private key of the FRBS-CA is compromised.

For certificates issued to Technical Contacts, the Participant must notify the RA prior to (or if impossible, immediately after) the occurrence of any of the following events:

- (1) the Participant no longer requires access to any Federal Reserve Bank business application; or
- (2) the security procedures instituted by the Participant are compromised and the Participant seeks to have the certificate revoked.

Any such notice automatically constitutes a Participant's request that the Technical Contact's certificate be revoked. No new certificate will be issued to a Subscriber serving as the Technical Contact unless requested by an EUAC.

The FRBS-CA also reserves the right to revoke any certificate if the FRBS-CA or RA, in its sole discretion, believes revocation of a certificate is warranted or if the private key of the FRBS-CA is compromised.

#### **4.9.2 Who can Request Revocation**

Revocations may only be requested by:

- a Participant's EUAC
- Subscriber's management in circumstances where Subscribers are a named individual employee or contractor of a Federal Reserve Bank
- the FRBS-CA
- the Federal Reserve Banks' Services Root CA

#### **4.9.3 Procedure for Revocation Request**

Upon receipt of a revocation request, the RA may, in certain instances, call an EUAC to confirm the revocation request. The RA uses the RA client software to request revocation of the Subscriber's certificate. This request is subsequently transmitted to the FRBS-CA, where the revocation is processed. A revocation request may also be initiated by the RA or FRBS-CA without a request from the Subscriber or Participant.

The FRBS-CA removes the Subscriber's certificate from the certificate directory and updates the CRL to reflect the revocation of the certificate. At this point, the Subscriber's revoked certificate can no longer be used to gain access to a Federal Reserve Bank business application.

#### **4.9.4 Revocation Request Grace Period**

No stipulation.

#### **4.9.5 Time within which CA Must Process Revocation Requests**

A certificate will be revoked within four hours following receipt of a revocation request by the RA and its confirmation, but action on a revocation request made over a weekend or holiday may be delayed until the following business day of the RA.

#### **4.9.6 Revocation Checking Requirement for Relying Parties**

Relying Parties are expected to consider revocation status information provided by the FRBS-CA during certificate validation and prior to relying on certificates issued by the Federal Reserve Banks or any information contained within those certificates.

#### **4.9.7 CRL Issuance Frequency**

CRLs will be published by the FRBS-CA no less frequently than once every 25 hours even if there are no revocation events subsequent to the previous CRL issuance. However, CRL publication will occur more frequently in the event the FRBS-CA receives a valid revocation request.

#### **4.9.8 Maximum Latency for CRLs**

CRLs will be published no later than the time specified in the “nextUpdate” field of the previously issued CRL.

#### **4.9.9 On-line Revocation/Status Checking Availability**

No stipulation.

#### **4.9.10 On-line Revocation Checking Requirements**

No stipulation.

#### **4.9.11 Other Forms of Revocation Advertisements Available**

The FRBS-CA may use other methods than CRLs to publicize the certificates it revokes.

#### **4.9.12 Special Requirements Regarding Key Compromise**

The FRBS-CA will make a reasonable effort to notify Relying Parties if it discovers or has reason to believe that there has been a compromise of its private key or that of its root CA.

#### **4.9.13 Circumstances for Suspension**

The FRBS-CA may elect to suspend a Subscriber certificate if the Subscriber or Participant does not fulfill the obligations defined in this CPS. The FRBS-CA may also elect to suspend a Subscriber certificate if a certificate is under investigation.

Certificates may be suspended for any of the reasons specified in section 4.9.1 of this CPS or where the following circumstances arise:

- There is an unverified suspicion of private key compromise
- The Subscriber or Participant has failed to meet their obligations under any applicable agreement
- The FRBS-CA or RA determines within their sole discretion that continued use of a certificate could jeopardize the Federal Reserve Banks' PKI.

Suspended certificates may be reinstated only by the FRBS-CA or RA, and only after adequate due diligence has been completed to resolve the issue that resulted in suspension.

#### **4.9.14 Who Can Request Suspension**

Only the RA or the FRBS-CA may initiate certificate suspension.

#### **4.9.15 Procedure for Suspension Request**

The procedures used for certificate revocation must also be followed for certificate suspension.

#### **4.9.16 Limits on Suspension Period**

No stipulation.

### **4.10 Certificate Status Services**

#### **4.10.1 Operational Characteristics**

The FRBS-CA maintains a certificate revocation list (CRL) listing those certificates that have been revoked and made non-operational since issuance (the "Certificate Status Services"). The repositories will be maintained as needed to support operations of the Federal Reserve Banks' PKI. Certificate Status Services may not be possible for certificates used for special connectivity purposes.

#### **4.10.2 Service Availability**

Certificate Status Services, where provided by the FRBS-CA, will be available without scheduled interruption.

#### **4.10.3 Optional Features**

No stipulation.

#### **4.11. End of Subscription**

Subscribers may end a subscription for certificates issued by the FRBS-CA by:

- Allowing the certificate to expire without renewal or rekey
- Requesting revocation before expiration without reissuance via authorized approvers identified in section 4.9.2 of this CPS.

#### **4.12. Key Escrow and Recovery**

##### **4.12.1. Key Escrow and Recovery Policy and Practices**

Private key escrow is not allowed.

##### **4.12.2. Session Key Encapsulation and Recovery Policy and Practices**

Session key encapsulation and recovery is not supported by the FRBS-CA.

### **5.0 MANAGEMENT AND OPERATIONAL CONTROLS**

#### **5.1 Physical Controls**

The servers supporting operations of the FRBS-CA are protected by a variety of physical controls, which include card-key access to the computer data center at multiple layered entry points. In addition, access to the FRBS-CA server and FRBS-CA software will be protected by multiple strong passwords.

##### **5.1.1. Site Location and Construction**

The site location for the FRBS-CA, especially when combined with physical security controls and countermeasures, will provide appropriate protection against unauthorized access to the FRBS-CA, its equipment, and supporting records.

### **5.1.2. Physical Access**

Access to all equipment supporting operations of the FRBS-CA, including any workstations used to administer the FRBS-CA, will be protected from unauthorized physical access. Physical security protections will provide for monitoring against unauthorized intrusion, maintenance and review of access logs, and multi-person control over all cryptographic modules supporting FRBS-CA signing operations.

All activation data will remain secret or be recorded and stored separately from the cryptographic module.

Equipment supporting RA operations must also be protected from unauthorized access, as well as unauthorized modification while not activated.

### **5.1.3. Power and Air Conditioning**

The FRBS-CA has sufficient power backup capability to ensure the ability to complete pending actions in the event of power failure, and to ensure the availability of repositories.

### **5.1.4. Water Exposures**

The FRBS-CA is installed in a manner that limits danger of exposure to water, excluding that related to fire prevention or protection measures.

### **5.1.5. Fire Prevention and Protection**

The FRBS-CA is installed in a manner that ensures its systems are protected with appropriate fire suppression controls.

### **5.1.6. Media Storage**

All media used in operations of the FRBS-CA is handled and secured according to the requirements appropriate for its classification, including adequate controls on its storage to prevent unauthorized physical access.

### **5.1.7. Waste Disposal**

Sensitive media no longer required for the ongoing operations of the FRBS-CA is securely destroyed in a manner commensurate with its classification.

### **5.1.8. Off-site Backup**

The latest full backup of the FRBS-CA will be maintained at a location separate from the operational CA, with all physical and procedural control afforded the backup being equivalent to that of the operational CA.

## **5.2 Procedural Controls**

Appropriate policies and procedures have been implemented to ensure that the appropriate personnel have been assigned to perform the duties and functions of the FRBS-CA and the respective RAs.

### **5.2.1. Trusted Roles**

The requirements of this CPS are described in terms of four roles. Those roles, which may be combined, are as follows:

- (1) Administrator – authorized to install, configure, and maintain the CA.  
Administrators do not issue certificates to Subscribers.
- (2) Officer – authorized to request or approve certificates or certificate revocations
- (3) Auditor – authorized to maintain audit logs
- (4) Operator – authorized to perform system backup and recovery

### **5.2.2. Number of Persons Required per Task**

Multi-person controls are required for logical access to the FRBS-CA, with at least one of those persons being assigned to the role of Administrator.

Multi-person controls are required specifically for the following tasks:

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

### **5.2.3. Identification and Authentication for Each Role**

For all assurance levels supported by the FRBS-CA, an individual must identify and successfully authenticate herself or himself prior to being permitted to perform the actions of any role.

### **5.2.4. Roles Requiring Separation of Duties**

Where operationally feasible, no individual should assume both the role of Officer and the role of Administrator. To further ensure adequate separation of duties, no

individual shall have more than one identity assigned to any role specified in section 5.2.1 of this CPS.

### **5.3 Personnel Controls**

#### **5.3.1. Qualifications, Experience, and Clearance Requirements**

The Federal Reserve Banks take appropriate steps to ensure assurance of the trustworthiness and competence of personnel supporting CA operations and of the satisfactory performance of their duties in a manner consistent with this CPS. All individuals filling trusted roles are selected on the basis of trustworthiness and integrity.

#### **5.3.2. Background Check Procedures**

Background checks are conducted for all employees and contractors of the Federal Reserve Banks supporting operations of the FRBS-CA.

#### **5.3.3. Training Requirements**

Individuals performing duties in the operation of the FRBS-CA receive appropriate training.

#### **5.3.4. Retraining Frequency and Requirements**

Retraining will occur at the discretion of Federal Reserve Banks management.

#### **5.3.5. Job Rotation Frequency and Sequence**

No stipulation.

#### **5.3.6. Sanctions for Unauthorized Actions**

The Federal Reserve Banks will impose appropriate sanctions, including termination where warranted, for their personnel acting in trusted roles if they perform unauthorized actions or abuse their authority and the trust placed in them.

#### **5.3.7. Independent Contractor Requirements**

The Federal Reserve Banks may employ independent third party contractors to perform services associated with the operation of the FRBS-CA.

#### **5.3.8. Documentation Supplied to Personnel**

Documentation sufficient to define the duties, procedures, and responsibilities for each trusted role defined in 5.2.1 is provided to the personnel filling those roles.

## 5.4 Audit Logging Procedures

The Federal Reserve Banks shall maintain audit logs, which will be updated in real time. These logs will be backed up to physical media (digital tape, CD, or appropriate other storage media). The audit logs will contain the history of the operational activities of the FRBS-CA and will be kept in accordance with the applicable Federal Reserve Bank record retention policy.

Periodic review of the operating practices, procedures, and policies of the FRBS-CA will be performed by internal Federal Reserve Bank auditors.

### 5.4.1. Types of Events Recorded

Audit logs contain information related to the type of event, the date and time of occurrence, an indication of success or failure, and the identity of the operator or entity triggering the event.

Audit logs must be configured to record the following events:

- Any changes to audit parameters
- Any attempt to delete or modify audit logs
- Successful and unsuccessful attempts to assume a role
- Administrator actions to unlock an account that has been locked due to authentication failures
- Key generation (except for symmetric session or one-time keys)
- The loading of private key components
- Access to the private key component
- Changes to trusted public keys (additions or deletions)
- Export of private keys and shared secret (symmetric) keys
- All certificate requests
- All certificate revocation requests
- Approval or rejection of certificate status change requests
- Changes in CA configuration
- Addition or deletion of roles
- Modification in access control privileges
- All changes to certificate profiles
- All changes to CRL profiles
- Assignments to any trusted role
- Installation of the operating system
- Installation of the CA

- Removal or modification of hardware cryptographic modules
- System startup
- Authentication attempts
- Changes to authentication credentials (set or modify passwords)
- Re-key of the CA
- Configuration changes to the CA (hardware, software, operating system, patches)

#### **5.4.2. Frequency of Processing Logs**

Audit logs are maintained and processed in accordance with policies of the Federal Reserve Banks.

#### **5.4.3. Retention Period for Audit Log**

Audit logs are retained in accordance with policies of the Federal Reserve Banks.

#### **5.4.4. Protection of Audit Log**

Only personnel assigned to trusted roles are allowed access to the logs. Audit logs must be sufficiently protected against unauthorized additions, deletions, duplication, and modification.

#### **5.4.5. Audit Log Backup Procedures**

Audit logs are backed up in accordance with policies of the Federal Reserve Banks.

#### **5.4.6. Audit Collection System**

Audit log collection will adhere to policies of the Federal Reserve Banks.

#### **5.4.7. Notification to Event-causing Subject**

No stipulation.

#### **5.4.8. Vulnerability Assessments**

In keeping with Federal Reserve Bank requirements, periodic assessments must be performed of the FRBS-CA for evidence of malicious activity.

### **5.5 Records Archival**

Records of the FRBS-CA and RA are kept in accordance with the Federal Reserve Banks' Record Retention policies.

### **5.5.1. Types of Records Archived**

At a minimum, the following records will be archived:

- Certification Practice Statements
- Contracts and agreements related to CA operations
- System configurations
- Certificate requests
- Revocation requests
- Certificates issued by the CA
- Records of CA re-key
- CA key generation

### **5.5.2. Retention Period for Archive**

Archived records are retained as required to meet business requirements, or as required by law.

### **5.5.3. Protection of Archive**

Archived media is physically and environmentally protected within a secure facility. No unauthorized person is allowed to create, modify, or delete the archive, and its content will not be released without authority or expressed permission.

### **5.5.4. Archive Backup Procedures**

Backup and recovery procedures will ensure that a complete set of backup copies will be available in the event of the loss or destruction of the primary archives.

### **5.5.5. Requirements for Time-stamping of Records**

FRBS-CA is required to use a synchronized reliable time source to time-stamp all transmissions and records.

### **5.5.6. Archive Collection System (Internal or External)**

No stipulation.

### **5.5.7. Procedures to Obtain and Verify Archive Information**

No stipulation.

## **5.6 Key Changeover**

No stipulation.

## **5.7 Compromise and Disaster Recovery**

The FRBS-CA will provide back-up capability and use its best efforts to restore FRBS-CA functionality at an alternate disaster recovery location in the event of a system failure at the FRBS-CA.

### **5.7.1. Incident and Compromise Handling Procedures**

The FRBS-CA adheres to all incident handling and reporting requirements established by the Federal Reserve Banks.

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

In the event that computing resources supporting FRBS-CA operations are corrupted, the FRBS-CA will take appropriate actions to verify that the system's integrity has been restored prior to returning the FRBS-CA to operation. Where the signing private key of the FRBS-CA has not been destroyed or compromised, FRBS-CA operation will be reestablished in a manner giving priority to the ability to generate certificate status information. Where the signing private key of the FRBS-CA is destroyed or compromised, priority will be given to the generation of a new CA key pair.

### **5.7.3. Entity Private Key Compromise Procedures**

In the event that the signing private key of the FRBS-CA is destroyed or compromised, revocation of the FRBS-CA's certificate must be initiated by the Root CA. A new key pair must be generated by the FRBS-CA when practical, and a new certificate issued by the Root CA.

### **5.7.4. Business Continuity Capabilities after a Disaster**

The FRBS-CA is designed to restore service within eighteen (18) hours of primary system failure. Solely at their own discretion and risk, Relying Parties may elect to continue to use certificates pending reestablishment of service.

## **5.8 CA or RA Termination**

The Federal Reserve Banks reserve the right to terminate the FRBS-CA's or RA's function at any time without prior notice. However, the FRBS-CA will exercise its best efforts to notify Participants of any such termination as soon as practicable.

## **6.0 TECHNICAL SECURITY CONTROLS**

The signature key pair of the FRBS-CA is created during the initial installation of the FRBS-CA application is 2048 bits long and is generated on and protected by a hardware cryptographic device certified to FIPS 140-1 Level 3.

Subscribers are required to use private key/public key pairs that are 2048 bits long. Subscriber certificates issued by the FRBS-CA are valid for three years from the date of issuance and may be automatically rolled-over if the credential is still valid or if the capability exists for the specific type of certificate. The certificate of the Federal Reserve Banks Root CA is valid for twenty (20) years from the date of issuance; the certificate of the FRBS-CA is valid for ten (10) years from the date of issuance.

### **6.1. Key Pair Generation and Installation**

#### **6.1.1. Key Pair Generation**

Cryptographic keying material used to sign certificates and certificate status information will be generated in FIPS 140 validated cryptographic modules or modules that have been validated under equivalent standards. Those cryptographic modules must meet or exceed FIPS 140 Security Level 2 (or the equivalent).

Subscriber key pair generation may be performed by the Subscriber, as described in section 4.3.1.1 or by the CA or RA as described in sections 4.3.1.2 and 4.3.1.3.

#### **6.1.2. Private Key Delivery to Subscriber**

Where the FRBS-CA or RA generates keys on behalf of the Subscriber, the private key will be delivered securely on a hardware cryptographic module. The FRBS-CA or RA generating the private key will not retain any copy.

#### **6.1.3. Public Key Delivery to Certificate Issuer**

Where key pairs are generated by Subscribers or RA, the public key will be delivered securely to the FRBS-CA for signing and certificate issuance. The delivery mechanism must bind the verified identity to the public key.

#### **6.1.4. CA Public Key Delivery to Relying Parties**

The FRBS-CA may make its public key available to Relying Parties through its established repository.

### **6.1.5. Key Sizes**

All valid certificates and certificate status information is signed with keys of at least 2048 bits for RSA using SHA-256. Subscriber certificates contain public keys that are at least 2048-bits for RSA.

### **6.1.6. Public Key Parameters Generation and Quality Checking**

Parameter quality checking will be performed in accordance with FIPS 186.

### **6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)**

Subscriber certificates assert key usages based on the intended application of the key pair. Where certificates are to be used for digital signatures (including authentication), the bits for “digitalSignature” and “nonRepudiation” will be set. Where certificates are to be used for key or data encryption, the bits for “keyEncipherment” or “dataEncipherment” will be set. Where certificates are to be used for key agreement, the bits for “keyAgreement” will be set.

## **6.2. Private Key Protection and Cryptographic Module Engineering Controls**

### **6.2.1. Cryptographic Module Standards and Controls**

See section 6.1.1.

### **6.2.2. Private Key (n out of m) Multi-person Control**

Use of the FRBS-CA private signing key requires action by multiple persons. At a minimum, the multi-person control must be set for 2 of 5.

### **6.2.3. Private Key Escrow**

Under no circumstances will private keys be escrowed.

### **6.2.4. Private Key Backup**

The FRBS-CA private signing key is backed up under multi-person control, as specified in section 6.2.2.

Subscriber private signing keys may be backed up where technically feasible, but must in all circumstances be held in the Subscriber’s control. Browser-based (software token) certificates and the associated private keys may be stored in the file format specified by the password privacy mode of PKCS#12. Under no circumstances must copies of private

signing keys be stored in plain text or outside of either a cryptographically secure file such as that specified by PKCS#12 or a hardware cryptographic module.

#### **6.2.5. Private Key Archival**

Private signing keys will not be archived.

#### **6.2.6. Private Key Transfer into or from a Cryptographic Module**

Private keys of the FRBS-CA may be exported from a cryptographic module only to perform FRBS-CA key backup procedures.

#### **6.2.7. Private Key Storage on Cryptographic Module**

No stipulation.

#### **6.2.8. Method of Activating Private Key**

Activation of the FRBS-CA private signing key requires multi-person control as specified in section 6.2.2.

#### **6.2.9. Method of Deactivating Private Key**

Cryptographic modules that have been activated must not be available to those without authorization. After required use is completed, the cryptographic module must be deactivated and securely stored.

#### **6.2.10. Method of Destroying Private Key**

Individuals in trusted roles must destroy all private signing keys when they are no longer required. For private keys stored in software cryptographic modules, this may be achieved by overwriting the data. For private keys stored in hardware cryptographic modules, this may be achieved through functions that zeroize the data. Physical destruction of the hardware cryptographic module is not required under this CPS.

#### **6.2.11. Cryptographic Module Rating**

See section 6.1.1.

### **6.3. Other Aspects of Key Pair Management**

#### **6.3.1. Public Key Archival**

The public key will be archived only through certificate archival.

### **6.3.2. Certificate Operational Periods and Key Pair Usage Periods**

The private keys of the Federal Reserve Banks Root CA have a maximum lifetime of twenty (20) years; the private keys of the FRBS-CA have a maximum lifetime of ten (10) years. Subscriber private keys have a maximum lifetime of three years.

## **6.4. Activation Data**

### **6.4.1. Activation Data Generation and Installation**

Activation data used to unlock private keys must have an appropriate strength for the keys or data that is being protected. If that activation data must be transmitted, that transmission is to occur via a protected channel. Activation data is expected to be changed upon re-key.

### **6.4.2. Activation Data Protection**

Data used to unlock private keys must be protected from unauthorized disclosure via a combination of cryptographic (logical) and physical access controls. Activation data should be further protected by locking the account or terminating an application after a predetermined number of failed login attempts.

### **6.4.3. Other Aspects of Activation Data**

No stipulation.

## **6.5. Computer Security Controls**

### **6.5.1. Specific Computer Security Technical Requirements**

For the FRBS-CA, technical security requirements for systems supporting its operations must include the following minimum capabilities:

- Authentication of user identities prior to permitting access
- Management of user privileges and limiting users to their assigned roles
- Audit logging
- Enforcement of domain boundaries for critical processes
- Recovery from system failure

### **6.5.2. Computer Security Rating**

No stipulation.

## **6.6. Life Cycle Technical Controls**

### **6.6.1. System Development Controls**

For the FRBS-CA, system development follows a formal, documented methodology.

### **6.6.2. Security Management Controls**

For the FRBS-CA, system modifications and upgrades are documented and applied in a controlled manner. A formal configuration management methodology is followed for ongoing maintenance.

### **6.6.3. Life Cycle Security Controls**

No stipulation.

## **6.7. Network Security Controls**

Networked equipment supporting FRBS-CA operations has all unused ports and services disabled. Any network software installed on systems of the FRBS-CA must be necessary to the functioning of the FRBS-CA. All remote workstations used to administer the FRBS-CA will be allowed a connection only after successful authentication of the device.

## **6.8. Time-stamping**

Automated procedures are in place to synchronize and maintain system time.

## **7.0 CERTIFICATE AND CRL PROFILES**

### **7.1 Certificate Profile**

#### **7.1.1. Version Number(s)**

The FRBS-CA issues X.509 version 3 certificates.

#### **7.1.2. Certificate Extensions**

Use of standard certificate extensions conforms to RFC 3280. Private extension may be used but must not be marked as critical

#### **7.1.3. Algorithm Object Identifiers**

Certificates issued by the FRBS-CA will identify the signature algorithm using the following Object Identifier (OID):

Algorithm	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11

#### 7.1.4. Name Forms

The subject and issuer field are populated with an X.500 Distinguished Name (DN), and are comprised of standard attribute types as identified in RFC 3280.

#### 7.1.5. Name Constraints

No stipulation.

#### 7.1.6. Certificate Policy Object Identifier

See section 1.2.

#### 7.1.7. Usage of Policy Constraints Extension

The policy constraints extension may be asserted in FRBS-CA certificates issued by the Federal Reserve Banks.

#### 7.1.8. Policy Qualifiers Syntax and Semantics

Certificates issued by the Federal Reserve Banks may contain policy qualifiers as identified in RFC 3280.

#### 7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

### 7.2 CRL Profile

#### 7.2.1. Version Number(s)

The FRBS-CA issues X.509 version 2 CRLs.

#### 7.2.2. CRL and CRL Entry Extensions

Field	Value
Version	Integer value of "1"
Signature Algorithm	sha256WithRSAEncryption
Issuer	cn=FRB Services Issuing CA1, ou=PKI Services, o=Federal Reserve Banks, c=us

### **7.3. OCSF Profile**

#### **7.3.1. Version Number(s)**

No stipulation.

#### **7.3.2. OCSF Extensions**

No stipulation.

### **8.0 COMPLIANCE AUDITS**

Periodic review of the operating practices, procedures, and policies of the FRBS-CA will be performed by internal Federal Reserve Bank auditors and according to their defined standards

#### **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.

### **9.0 OTHER BUSINESS AND LEGAL MATTERS**

The general business and legal matters covered by this Section 9.0 of the CPS, where applicable, are set forth in the associated legal agreement(s) referenced in the form to designate an EUAC.

## **9.1 Fees**

Fees are addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

## **9.2 Financial Responsibility**

No stipulation.

## **9.3 Confidentiality of Business Information**

Confidentiality is addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

## **9.4 Privacy of Personal Information**

No stipulation.

## **9.5 Intellectual Property Rights**

Intellectual property rights are addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

## **9.6 Representations and Warranties**

Representations and warranties are addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

## **9.7 Disclaimer of Warranties**

Disclaimers of warranties are addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

## **9.8 Limitations of Liability**

Limitations of liability are addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

## **9.9 Indemnities**

Indemnities are addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

#### **9.10 Term and Termination**

Term and termination are addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

#### **9.11 Individual Notices and Communications with Participants**

No stipulation.

#### **9.12 Amendments**

The Federal Reserve Banks may amend this CPS upon five (5) business days prior notice sent to the EUACs designated by the Participants or to other representatives of the Participant (with no confirmation of actual receipt required; the Federal Reserve Banks may also amend this CPS immediately upon the occurrence of any event deemed by the Federal Reserve Banks to be a security breach or force majeure occurrence.

#### **9.13 Dispute Resolutions Procedures**

Dispute resolution procedures are addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

#### **9.14 Governing Law**

Governing law is addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

#### **9.15 Compliance with Applicable Law**

Compliance with applicable law is addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

#### **9.16 Miscellaneous Provisions**

Miscellaneous provisions are addressed in the associated legal agreement(s) referenced in the form to designate an EUAC.

#### **9.17 Other Provisions**

No stipulation.