

# Federal Reserve Banks' Certification Authority (FR-CA) Certification Practice Statement

## 1.0 INTRODUCTION

### 1.1 OVERVIEW

The Federal Reserve Banks ("FRBs"), utilizing Public Key Infrastructure ("PKI") technology and operating as a Certification Authority ("FR-CA"), will issue a public key certificate to an external FRB business customer for use in accessing certain FRB business applications. This Certification Practice Statement ("CPS") describes the policies and practices of the FR-CA, and sets forth the obligations of an external user of an FR-CA certificate. An external user ("Participant") is a depository institution or other authorized entity that is subject to the provisions set forth in Federal Reserve Operating Circular 5, Electronic Access ("OC 5"). A subscriber ("Subscriber") is a named individual employee or agent of a Participant who is issued a certificate to access an FRB business application. By accessing certain FRB business applications by means of a certificate the Participant and Subscriber agree to the provisions of this CPS.

### 1.2 IDENTIFICATION

This CPS is called the Federal Reserve Banks' Certification Authority Certification Practice Statement. The current issue is version 1.7, dated December 4, 2006.

### 1.3 COMMUNITY AND APPLICABILITY

The following are roles relevant to the administration and operation of the FR-CA.

#### 1.3.1 CERTIFICATION AUTHORITY

The FRBs, located in twelve Federal Reserve Districts in the United States of America, jointly operate the FR-CA.

The FR-CA will issue a certificate, which links a public and private key pair, to a Subscriber. In general, only an authorized employee or agent of a Participant may be a Subscriber, although the FR-CA may issue server certificates ("server-based certificates") and object code-signing certificates. Certificates may be issued in several ways. Some certificates will be issued after the Subscriber follows the appropriate steps to generate the certificate from the certificate retrieval web site ("browser-based certificates"). Other certificates will be generated by the FR-CA and sent to the Subscriber on a token-based media ("token-based certificates"). Unless otherwise noted, the obligations set forth in this CPS apply to server-based, browser-based and token-based certificates.

#### 1.3.2 REGISTRATION AUTHORITIES

A Registration Authority ("RA") is an FRB that collects and processes Subscriber requests from the Participant's authorized contacts, containing

information about the Subscriber's identity, authorization, roles, and other information, which will be used by the FRBs.

### **1.3.3 REPOSITORIES**

The FR-CA uses directory services for publishing and distributing the certificates issued to its Subscribers. The FR-CA maintains a certificate revocation list ("CRL"), a list of all certificates revoked and made non-operational, which is accessible only by the FRBs, except as otherwise provided.

The FR-CA also maintains a repository for its CPS and the certification policies it supports. This repository is located at the FR-CA's URL at <<https://profile.federalreserve.org>>.

### **1.3.4 PARTICIPANTS/SUBSCRIBERS**

A Participant is a depository institution or other authorized entity subject to the provisions set forth in OC 5 which seeks access to an FRB business application. A Subscriber is a named individual employee or agent of a Participant who is issued a certificate to access an FRB business application. An FRB business application may have other security requirements for access in addition to the use of a certificate.

In some instances, a Participant may seek to access an FRB business application that has special connectivity requirements, such as file transfer and messaging utilities. In this case, the Participant must request and retrieve a certificate issued by the FR-CA in accordance with the procedures identified in the applicable guide or another designated document related to the application. Such certificates will be issued directly to a designated technical contact ("Technical Contact") for the Participant, who will be a Subscriber and therefore subject to all obligations of a Subscriber as set forth in this CPS, as well as certain additional obligations specified for Technical Contacts in the applicable Federal Reserve user guides.

In other instances, where a browser-based certificate is issued to a Participant subscribing to FedImage<sup>®</sup> Gateway Retrieval, the Participant must similarly request and retrieve a browser-based certificate issued by the FR-CA in accordance with the procedures identified in the applicable FedImage Gateway Retrieval documentation, and further agrees that its designated Technical Contact will create an electronic agent<sup>1</sup> for the Participant that accesses FedImage Gateway Retrieval to retrieve image files in response to requests originated by the Participant. Although the FRB will provide an Application Programming Interface ("API") packet, the Participant is solely responsible for the development and maintenance of such electronic agent.

---

<sup>1</sup> An electronic agent is the automated software agent that resides at the financial institution and which exchanges data, using standard XML data-type definitions and SSL encryption, with the FedImage Services archive maintained by the Federal Reserve Banks. See the FedImage<sup>®</sup> Gateway Retrieval Interface Guide or another designated document for further information.

There may be other instances where a browser-based certificate is issued to a Technical Contact and a Participant may store the certificate on a server in accordance with applicable Federal Reserve user guides.

### **1.3.5 RELYING PARTIES**

Parties relying on a certificate (“Relying Parties”) will be the FRBs in order to permit Subscribers to access an FRB business application, except in the instances of: (1) server certificates and object code-signing certificates; and (2) Participants requiring mutual authentication of servers with the FRBs with respect to special connectivity requirements. In no event should relying parties be an entity other than the FRBs or a Participant.

### **1.3.6 APPLICABILITY**

Certificates issued by the FR-CA are to be used solely for official electronic business communications with the FRBs and are not for use by, nor with, any unapproved party. Use of FR-CA- issued certificates for other than official business communications with the FRBs is expressly prohibited.

## **1.4 CONTACT DETAILS**

This CPS is administered by the FR-CA. The RA will provide Subscribers with contact information, which may be revised from time to time.

## **2.0 GENERAL PROVISIONS**

### **2.1 OBLIGATIONS**

#### **2.1.1 Certification Authority and Registration Authority Obligations**

The FR-CA is responsible for the following:

1. Acting in accordance with policies and procedures designed to safeguard the certificate management process (including certificate issuance, certificate revocation, and audit trails) and to protect the FR-CA private key.
2. Validating information submitted by a Federal Reserve Information Security Officer that gives appropriate officials of the FRBs certain RA responsibilities.
3. Ensuring that there is no duplication of a Subscriber’s name (as defined in the distinguished name on the Subscriber’s certificate).
4. Issuing a certificate to a Subscriber after a properly formatted and verified certificate request is received by the FR-CA.
5. Creating and maintaining an accurate Certificate Revocation List (“CRL”).

6. Notifying the Participant of a revoked FRB server certificate used for special connectivity purposes.
7. Maintaining this CPS.
8. Creating and maintaining an accurate audit trail.

An RA is responsible for the following:

1. Validating information submitted to the RA by the Participant concerning the form used to designate an End User Authorization Contact and if applicable, a certificate request.
2. Forwarding a validated certificate request to the FR-CA.
3. Sending, for a server-based or a browser-based certificate, authorization codes to the Participant after receiving a properly completed and verified request from a Participant.
4. Sending, for a server-based or a browser-based certificate, reference codes to the Subscriber after receiving a properly completed and verified request from a Participant.
5. Sending, for a token-based certificate, a token-pass phrase to a Subscriber.
6. Sending, for a token-based certificate, a related token to the End User Authorization Contact.
7. Confirming certificate revocation requests with the Participant.
8. Confirming and initiating validated certificate renewal requests.
9. Creating and maintaining an accurate audit trail.

These responsibilities of the FR-CA and each RA are illustrative and not exclusive. Any one or more of these responsibilities may be automated by the FRBs.

The FR-CA will issue certificates to a Subscriber within a reasonable time after a properly formatted certificate request is received and verified by the FR-CA. See Section 4.2 for the certificate issuance process.

A certificate will be revoked as soon as practicable following receipt of a revocation request 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. Except as otherwise provided, Subscribers will not be notified directly of certificate revocation, but will be denied access to FRB business applications. Revoked certificates are published in a CRL, which is issued by the FR-CA and posted to a directory for FRB use only, except as otherwise provided.

## 2.1.2 Participant and Subscriber Obligations

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:

1. The Participant must identify the names and contact information for at least two (2) Participant End User Authorization Contacts. The identification must be provided to the RA in a writing signed and dated by an authorized Participant representative. The Participant also is responsible for informing the RA, in accordance with that RA's then-standard procedures, of all updates and substitutions made for the End User Authorization Contacts, as events warrant (due to employee retirement, reassignment, termination, etc.).
2. The Participant must provide to the RA the necessary Subscriber information to request a certificate for a Subscriber. A request for a Subscriber that is not also an End User Authorization Contact may be submitted in paper form or electronically.
3. A Participant's End User Authorization Contacts are solely responsible for the identification, authentication, and notification processes between the Participant and the RA with respect to Subscribers. The Participant's End User Authorization Contact is responsible for keeping confidential any authorization codes supplied to the End User Authorization Contact. The End User Authorization Contact shall provide any applicable authorization code or token to the Subscriber only if the End User Authorization Contact has first validated the identity of the Subscriber and has authorized the Subscriber to access an FRB business application. The End User Authorization Contact must notify the RA immediately if a certificate should not be issued to the proposed Subscriber. The FR-CA has no responsibility for, and may rely entirely upon, the End User Authorization Contacts to validate the identity and authority of that Participant's Subscribers, and the Subscribers' roles within the FRB business applications.
4. At least one of the Participant's End User Authorization Contacts 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 FRB business application;
  - (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; or

- (d) 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 (“Private Key Compromise Event”).

Any such notice automatically constitutes a Participant’s request that the Subscriber’s certificate be revoked. In addition, for token-based certificates, a Subscriber’s certificate may be revoked if the token becomes locked out.

The above requirements set forth in this Section 2.1.2 (4) do not apply in the instance where a certificate is issued to a Participant’s Technical Contact. Instead, the Participant must notify the RA if the Technical Contact no longer has 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 of the new Technical Contact.

5. The Participant’s End User Authorization Contact must notify the RA immediately following the occurrence of any of the following events:

- (a) The End User Authorization Contact 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 the 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 End User Authorization Contact submitting the Subscriber request;
- (c) The End User Authorization Contact 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 a server-based or a browser-based certificate; or
- (e) A Subscriber attempts to use the token-based certificate but is unable to access an authorized FRB business application.

6. The Participant is solely responsible for 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 Participant's Subscribers 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 End User Authorization Contact 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 a browser-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 FR-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 FR-CA certificate. It is suggested that passwords contain no words from a dictionary, and include a combination of upper and lower case characters, numbers and special characters. Software that does not allow the use of passwords to protect the private key may be used by the Participant and Subscriber, but the use of such software by the Participant and Subscriber creates a greater risk of the occurrence of a Private Key Compromise Event. The Participant shall be wholly responsible and liable for all Private Key Compromise Events.
- (e) Notifying the End User Authorization Contact 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 End User Authorization Contact 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 days of the End User Authorization Contact submitting the Subscriber request.
- (h) Notifying the End User Authorization Contact immediately if the reference number for a server-based or a browser-based certificate, or the token or token-pass phrase for a token-based certificate, is received by a physical means that displays evidence of tampering.
- (i) Notifying the End User Authorization Contact immediately if a Subscriber attempts to use the reference number and authorization code provided to the Subscriber, but is unable to generate 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 FRB business application.
- (j) Acting in accordance with all other FR-CA procedures and instructions distributed by the RA or the FR-CA, or posted on the FR-CA certificate retrieval web site, related to requesting certificates and sending messages to the RAs and FR-CA.
- (k) **UTILIZING CERTIFICATES AND PRIVATE KEYS SOLELY IN THE MANNER FOR WHICH THEY ARE INTENDED, I.E., ONLY TO ACCESS AN FRB BUSINESS APPLICATION.**

Once the FR-CA has issued a certificate to the Subscriber, thereby granting the Subscriber access to an FRB 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 and assumes all liability concerning the use or misuse of any certificate issued by the FR-CA to any Subscriber authorized by the Participant, except for a claim or loss arising exclusively from the FR-CA or RA's failure to exercise ordinary care or act in good faith.

All notices provided by an End User Authorization Contact under this paragraph 2.1.2 must be sent to the RA in accordance with that RA's instructions.

The above requirements set forth in this Section 2.1.2 (6) (c), (d), (e) and (f) may not apply in the instance where a certificate is issued to a Participant for access by a Technical Contact.

With respect to a certificate issued to a Participant's Technical Contact, the Participant is solely responsible for the storage and security related to the certificate used to access an FRB business application. The Participant is solely responsible for and assumes all liability concerning the use or misuse of any certificate issued by the FR-CA to the Technical Contact, except for a claim or loss arising exclusively from the FR-CA or RA's failure to exercise ordinary care or act in good faith.

In addition, with respect to FedImage Gateway Retrieval, the Participant is solely responsible for the development and maintenance of an electronic agent and the Participant is solely responsible for the storage and security related to the browser-based certificate used to access FedImage Gateway Retrieval. The browser-based certificate issued by the FR-CA is used to authenticate the Participant's access to FedImage Gateway Retrieval. All image requests to FedImage Gateway Retrieval are identified as originating from the browser-based certificate issued to the Participant's Technical Contact regardless of whether the Participant allows its customers to make use of the electronic agent. The Participant is solely responsible for and assumes all liability concerning the use or misuse of any certificate issued by the FR-CA to the Technical Contact, except for a claim or loss arising exclusively from the FR-CA or RA's failure to exercise ordinary care or act in good faith. Browser-based certificates issued by the FR-CA for access to FedImage Gateway Retrieval are to be used solely for purposes of retrieving from the FedImage archive images that the Reserve Bank has stored at the Participant's request.

### **2.1.3 Relying Party Obligations**

- A. Except as stated in subparagraph B below, the FRBs are the Relying Parties with respect to certificates that permit Subscribers to access an FRB business application. Reliance upon an FR-CA issued certificate is unwarranted and inappropriate by and for Subscribers, except as stated in Paragraph B below.

Once the FRB's Web server has received and has recognized a certificate issued by the FR-CA, it shall permit authorized FRB transactions to be processed. If a certificate is recognized but has been revoked, FRB transactions will not be processed.

- B. The Relying Party may be the Participant in situations where the Participant's browser connects to the FRB server, and the Subscriber is sent digitally signed executable object code related to an FRB business application, along with an FR-CA issued certificate. 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. Neither the FR-CA nor the RA is liable for damages as a result of the use of code that does not have a valid digital signature produced by an attached FR-CA certificate.

Additionally, the Participant may be called upon to rely on FR-CA certificates with respect to mutual authentication of FRB and Participant servers in order to meet certain special connectivity requirements with the FRBs.

## **2.2 LIABILITY**

OC 5 sets forth applicable liability provisions. Nothing in this CPS limits any rights a Reserve Bank has under any other agreement.

## **2.3 FIDUCIARY RELATIONSHIPS**

Issuance of a certificate does not make the FR-CA an agent, fiduciary, trustee, or other representative of a Subscriber or any other party.

## **2.4 INTERPRETATION AND ENFORCEMENT**

This CPS is incorporated by reference in OC 5.

## **2.5 CONFIDENTIALITY POLICY**

All information collected, generated, transmitted, and maintained by the FR-CA and/or RA is considered confidential, except for information that: (i) is posted to the FR-CA's URL; (ii) is in the possession of a Participant or Subscriber, except information which has been received under an obligation of confidentiality agreed to by the FR-CA and/or RA in a written agreement; or (iii) is or becomes publicly available through no wrongful act.

## **3.0 IDENTIFICATION AND AUTHENTICATION**

### **3.1 INITIAL REGISTRATION**

The FR-CA certificate subject attribute contains the following values:

Country Name:	US
Organizational Name:	Federal Reserve Banks

The certificate subject attribute in FR-CA certificates issued to Subscribers contains the following values:

Country Name:	US
Organizational Name:	Federal Reserve Banks
Organizational Unit:	Routing Transit Number (RTN) of Institution
Common Name:	The Subscriber's name, which is assigned as per Section 3.1.1.

There are also server and object code signing certificates.

Where a certificate is issued to the Participant's Technical Contact, the Common Name value will contain unique attributes related to the intended use of the certificate.

### **3.1.1 Need for Names to be Meaningful**

Names used shall identify the person or object to which they are assigned in a meaningful way. Except as set forth in Section 3.1 for a certificate issued to the Participant's Technical Contact, the name assigned to the common name attribute is composed of the Subscriber's first name, followed by a space, followed by the Subscriber's surname.

### **3.1.2 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.

### **3.1.3 Uniqueness of Names**

The Organizational Unit and Common Name form the basis for the uniqueness of each assigned name. Except as set forth in Section 3.1 for a certificate issued to the Participant's Technical Contact, the FR-CA or RA assigns in the certificate subject attribute a combination of the Participant's name, the Subscriber's first name, surname, and other terms, numbers, characters or letters to ensure the uniqueness of each name.

### **3.1.4 Name Claim Dispute Resolution Procedure**

The naming convention specified in Section 3.1.1 is strictly enforced. Any dispute is resolved by the FR-CA and RA in accordance with this naming convention.

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

The FR-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 Subscriber's certificate request.

### **3.1.6 Authentication of Participant Identity**

The RAs are responsible for validating the authorization of the End User Authorization Contacts, who shall represent and make all decisions for the Participant.

## **3.2 ROUTINE RE-KEY**

Routine automated re-issuance of expiring certificates will not exist for Subscribers but may exist for the 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 REVOCATION REQUEST**

Revocation requests must be submitted in writing or electronically by a Participant's End User Authorization Contact and confirmed by the RA in order to be validated and processed.

### **3.4 RE-KEY AFTER REVOCATION**

Requests for a certificate after revocation are processed in accordance with certificate issuance requests.

## **4.0 OPERATIONAL REQUIREMENTS**

### **4.1 CERTIFICATE APPLICATION**

The FR-CA and RAs shall enforce the following practice with respect to a Subscriber's application:

As required by Section 2.1.2, the Participant must provide the RA with the names and contact information for at least two (2) End User Authorization Contacts. The RA shall use its own internal policies and procedures to verify that the names of the End User Authorization Contacts are sent by authorized personnel of the Participant.

A request for a Subscriber that is not also an End User Authorization Contact may be submitted in paper form or electronically. This Subscriber request will include information about the individual named by the End User Authorization Contact to receive a certificate. The completed Subscriber request must be provided to the RA. A Participant's End User Authorization Contacts are solely responsible for the identification, authentication, and notification processes between the Participant and the RA. The End User Authorization Contacts will be required to validate the identity, authority, and roles of the Subscriber to the RA.

### **4.2 CERTIFICATE ISSUANCE**

#### **4.2.1 Certificate Issuance for Server-based and Browser-based Certificates**

Server-based and browser-based certificates are issued by the FR-CA in accordance with the following practice:

1. The submission of a Subscriber request by the Participant is a representation that its End User Authorization Contact has validated the identity, authority, and roles of the Subscriber to the RA. The End User Authorization Contact must immediately notify the RA if the Participant believes that the Subscriber should not be issued a certificate. Using the information provided by the Participant, the RA will send the End User Authorization Contact an authorization code that the End User Authorization Contact must provide to the Subscriber.

2. A separate communication containing a reference number will be sent to the Subscriber by the RA.
3. Upon receipt of the authorization code from the End User Authorization Contact and the reference number from the RA, the Subscriber can access the FR-CA's URL at <<https://profile.federalreserve.org>> in order to submit a certificate request. The reference number combined with the authorization code uniquely identifies the Subscriber to the FR-CA. Additional information is required to generate a server-based certificate to be used for special connectivity purposes.
4. The following set of actions are performed by the Subscriber's browser software, working in conjunction with programs on the FRB certificate web site and the FR-CA system:
  - (a) The Subscriber's browser generates a public key/private key pair. The Subscriber is asked to apply a password to protect the private key, unless the browser used does not have this function. The public key is submitted to the FRB certificate web site as a certificate request.
  - (b) The FRB certificate web site passes the certificate request to the FR-CA using a Secure Sockets Layer connection. The FR-CA creates the certificate, publishes the certificate in the directory associated with the FR-CA, and distributes both the Subscriber's certificate and the FRB CA's certificate to the FRB certificate web site.
  - (c) The FRB certificate web site subsequently distributes the Subscriber's certificate and the FR-CA's certificate directly to the Subscriber's browser. The certificates are stored on the Subscriber's hard drive.

Upon completion of these steps, the Subscriber has a certificate issued by the FR-CA; this certificate is located in the Subscriber's browser's certificate-store feature along with the FR-CA public key certificate. The Subscriber is also granted the appropriate permissions for specific web services and applications, and is now able to access and use these services.

See the FedImage Gateway Retrieval Interface Guide for any applicable differences associated with the issuance and storage of a certificate used to allow the Participant access to FedImage Gateway Retrieval. See also the applicable Federal Reserve user documentation for any differences associated with the issuance and storage of a certificate used to allow special connectivity by the Participant to the FRBs.

#### **4.2.2 Certificate Issuance for Token-based Certificates**

Token-based certificates are issued by the FR-CA in accordance with the following practice:

1. The submission of a completed request by the Participant is a representation that its End User Authorization Contact has validated the identity, authority, and roles of the Subscriber to the RA. The End User Authorization Contact must immediately notify the RA if the Participant believes that the Subscriber should not be issued a certificate. Using the information provided by the Participant, the RA will then provide the End User Authorization Contact with a token which the End User Authorization Contact must provide to the Subscriber.
2. A communication containing a token-pass phrase will be sent to the Subscriber by the RA.
3. Upon receipt of the token from the End User Authorization Contact, the Subscriber can then access the certificate by applying the token-pass phrase.

#### **4.3 CERTIFICATE ACCEPTANCE**

When a certificate issued to a Subscriber is used to access an FRB 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 as described in this CPS.

#### **4.4 CERTIFICATE REVOCATION**

See Section 2.1.2 for the Participant's obligation to notify the RA with a request to revoke a Subscriber's certificate. A certificate issued to a Participant's Technical Contact is subject to revocation as outlined in Section 4.4.1 of this CPS. Upon receipt of a revocation request, the RA may, in certain instances, call an End User Authorization Contact 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 FR-CA, where the revocation is processed. A revocation request may also be initiated by the RA or FR-CA without a request from the Subscriber or Participant.

The FR-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 an FRB business application. Certificates relied upon by the Participant for special connectivity with the FRBs may be subject to different certificate directory, revocation and CRL requirements. For example, checking the CRL may not be possible for certificates used for special connectivity purposes. See the appropriate user guide or other designated document related to a specific application for details.

Participant agrees to remove and delete the certificates issued to Participant by the FR-CA for special connectivity purposes under the following circumstances:

1. If the Participant requests that the FR-CA revoke the certificate issued to the Institution for special connectivity purposes;
2. If the FR-CA determines it is necessary to revoke the certificate issued to the Participant for special connectivity purposes; or

Participant agrees to remove and delete the FRB server certificate if the FR-CA determines it is necessary to revoke the FRB server certificate for special connectivity purposes.

Participant is responsible for any transactions sent to an FRB using a revoked certificate if Participant has not complied with the removal and deletion requirements set forth above.

#### **4.4.1 Circumstances for Revocation**

A certificate will be revoked by the FR-CA if the FR-CA or 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., thought to be known by any person or entity other than the Subscriber);
- (2) the Subscriber no longer requires access to any FRB business application;
- (3) the Subscriber's employment or affiliation with the Participant is terminated;
- (4) 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;
- (5) the FR-CA or RA, in its sole discretion, believes revocation of a certificate is warranted; or
- (6) the private key of the FR-CA is compromised.

The Participant has the responsibility to ensure that its End User Authorization Contact notifies the RA in advance (if possible) of the time when any of the above events occurs. In the case of a known or suspected Private Key Compromise Event, an End User Authorization Contact must notify the RA immediately. A certificate will be revoked as soon as practicable following receipt of a revocation request 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.

The provisions above in this Section 4.4.1 do not apply for a certificate issued to a Technical Contact. With respect to such certificates, 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 FRB business application;
- (2) the security procedures instituted by the Participant are compromised and the Participant would like the certificate revoked; or

- (3) the Participant participates in a merger with another financial institution.

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 End User Authorization Contact. The FR-CA reserves the right to revoke any certificate if the FR-CA or RA, in its sole discretion, believes revocation of a certificate is warranted or if the private key of the FR-CA is compromised. A certificate will be revoked as soon as practicable following receipt of a revocation request 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.

#### **4.4.2 Who Can Request Revocation**

Revocations may be requested by:

- Participant's End User Authorization Contact
- RA
- FR-CA

#### **4.4.3 Procedure for Revocation**

See Section 4.4. When the request is initiated by the RA or FR-CA without a request from the Participant, the request will be documented.

### **4.5 AUDIT PROCEDURES**

The FRBs 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 FR-CA and will be kept in accordance with the applicable FRB record retention policy.

Periodic review of the FR-CA's operating practices, procedures, and policies will be performed by internal FRB auditors.

### **4.6 RECORDS ARCHIVAL**

FR-CA and RA records will be kept in accordance with the Federal Reserve's Record Retention policies.

### **4.7 KEY CHANGEOVER**

No stipulation.

### **4.8 COMPROMISE AND DISASTER RECOVERY**

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

#### **4.9 CERTIFICATION AUTHORITY TERMINATION**

The FR-CA reserves the right to terminate its function at any time without prior notice. However, the FR-CA will exercise its best efforts to notify Participants of any such termination as soon as practicable.

### **5.0 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS**

#### **5.1 PHYSICAL CONTROLS**

The FR-CA server will be 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 FR-CA server and FR-CA software will be protected by multiple strong passwords.

#### **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 within the FR-CA and the respective RAs.

#### **5.3 PERSONNEL CONTROLS**

Background checks will be conducted on FR-CA staff, as part of employment at one of the FRBs.

### **6.0 TECHNICAL SECURITY CONTROLS**

The FR-CA's signature key pair is created during the initial installation of the 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 1024 bits long. Subscriber certificates issued by the FR-CA are valid for three years from the date of issuance. The certificate of the FR-CA is valid for ten years from the date of issuance.

### **7.0 CERTIFICATE AND CRL PROFILES**

#### **7.1 CERTIFICATE PROFILE**

The FR-CA issues X.509 Version 3 certificates.

### **8.0 CPS ADMINISTRATION**

#### **8.1 CHANGE PROCEDURES**

The FRBs and the FR-CA may amend this CPS upon five (5) business days prior notice sent to the End User Authorization Contacts designated by the Participants or to other representatives of the Participants (with no confirmation of actual receipt

required); the FRBs and the FR-CA may also amend this CPS immediately upon the occurrence of any event deemed by the FRBs to be a security breach or force majeure occurrence.

## **8.2 APPROVAL PROCEDURES**

This CPS is approved by the FRBs and is incorporated by reference into OC 5.

“FedImage” is a registered service mark of the Federal Reserve Banks. A complete list of marks owned by the Federal Reserve Banks is available at [www.frbervices.org](http://www.frbervices.org).