Certification Practice Statement for the Board of Governors of the Federal Reserve System

1. Introduction

1.1 Overview

The Federal Reserve Banks ("FRBs"), with oversight from the Board of Governors of the Federal Reserve System ("Board"), utilizing Public Key Infrastructure ("PKI") technology and operating as a Certification Authority ("FR-CA"), will issue a public key certificate to Federal, state, foreign financial supervisory agencies or filing organizations or individuals ("Filer") for use in accessing a Board system, including a Board application that permits Filers to submit regulatory and other filings to the Board through electronic means. 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, otherwise known as a "Participant," is a Federal, state, foreign financial supervisory agency or Filer. A subscriber ("Subscriber") is a named individual employee or agent of a Participant who is issued a certificate to access a Board application. By accessing a Board application by means of a certificate, the Participant and Subscriber agree to the provisions of this CPS.

1.2 Identification

This CPS is called the Certification Practice Statement for the Board of Governors of the Federal Reserve System. The current issue is version 1.3, dated September 18, 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 and object code-signing certificates.

1.3.2 Registration Authorities

The Registration Authority ("RA") shall be a Division of the Board which shall collect and validate, through the Participant's authorized contacts, a Subscriber's identity, authorization, roles, and other information, which will be used by the FRBs and the Board. The Board may delegate RA functions to individual 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"), which is a list of all certificates revoked and made non-operational, which will be accessible only by the FRBs and the Board.

The FR-CA also maintains a repository for its CPS and the certification policies it supports that relate to the Board. This repository is located at: http://www.federalreserve.gov/PKICertificates.

1.3.4 Participants/Subscribers

A Participant is a Federal financial supervisory agency, including, but not limited to, the Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, the Office of Thrift Supervision, a state financial supervisory agency, or a foreign financial supervisory agency which shall be granted access to specified data and information owned by the Board pursuant to a statute, regulation, or agreement. A Participant may also be a Filer that is authorized to submit regulatory and other filings to the Board through electronic means pursuant to a statute, regulation, or agreement. The Subscriber is a named individual employee or agent of a Participant who is issued a certificate to access a Board application.

1.3.5 Relying Parties

For purposes of the certificate issued under this CPS, except as otherwise provided in this CPS, the "Relying Parties" are the FRBs and the Board, which rely on the certificate to permit Subscribers to access a Board application.

1.3.6 Applicability

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

1.4 Contact Details

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

2. 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 and the Board certain specific 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 CRL.

6. Maintaining this CPS.

7. 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 the End User Authorization Contact and certificate request.

2. Verifying that the Participant's access to confidential data and information owned by the Board extends only to that data which the Participant has been duly authorized to access by the Board.

3. Forwarding a validated certificate request to the FR-CA.

4. Sending authorization codes to the End User Authorization Contact after receiving a properly completed and verified request from a Participant.

5. Sending reference codes to the Subscriber after receiving a properly completed and verified request from a Participant.

6. Confirming certificate revocation requests with the Participant.

7. Confirming and initiating validated certificate renewal requests.

8. Creating and maintaining an accurate audit trail.

The responsibilities of the FR-CA or any RA are illustrative and not exclusive; in addition, any one or more of these responsibilities may be automated by the FRBs and the Board.

The FR-CA will issue a certificate to a Subscriber within a reasonable time after a properly formatted certificate request is received and verified by the FR-CA. After presenting the correct reference number and authorization code to the appropriate URL, a Subscriber will be notified that the certificate has been issued.

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. Subscribers will not be notified directly of certificate revocation, but will be denied electronic access to Board systems. Revoked certificates are published in a CRL, which is issued by the FR-CA and posted to a directory for FRB and Board use only.

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. Participant must identify the names and contact information for at least two (2) Participant End User Authorization Contacts ("End User Authorization Contacts"). The identification must be provided to the RA in paper form, signed and dated by an authorized representative of the Participant. If the contact information changes (employee retirement, reassignment, termination, etc.), consistent with the RA's standard procedures, the Participant must provide the RA with the updated information as soon as practicable.

2. A Participant's End User Authorization Contacts are responsible for the identification of Subscribers and the notification processes between the Participant and the RA. The Participant's End User Authorization Contact is

responsible for keeping confidential any authorization codes supplied to the End User Authentication Contact. The End User Authorization Contact shall provide the authorization code 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 a Board application. The End User Authorization Contact must notify the RA immediately if a certificate should not be issued to the proposed Subscriber.

3. The Participant's End User Authorization Contact(s) must notify the RA, by telephone and in writing, prior to (or depending on the event, immediately after) the occurrence of any of the following:

   (a) a Subscriber's employment with the Participant is terminated;

   (b) a Subscriber no longer requires or is authorized to have access to a Board system;

   (c) if applicable; a Subscriber is unable to recall the PIN for the token device that protects the Subscriber's private key; or

   (d) the Subscriber knows or suspects that his or her private key or the PIN used to protect the private key has been disclosed to, or is known by, any other person or entity or the Subscriber loses the token device storing the certificate("Private Key Compromise Event").

   Any such notice automatically constitutes a Participant's request that the Subscriber's certificate be revoked. No new certificate will be issued to that Subscriber unless requested by an End User Authorization Contact.

4. The Participant's End User Authorization Contact must notify the RA by telephone immediately following the occurrence of any of the following events:

   (a) The End User Authorization Contact has not received the authorization code within four (4) business days of submitting the Subscriber Request form;

   (b) The Subscriber has not received the reference number within seven (7) business days of the End User Authorization Contact submitting the Subscriber Request form;

   (c) The End User Authorization Contact or the Subscriber receives an authorization code or reference number by a physical means that displays evidence of tampering; or

(d) A Subscriber attempts to use the authorization code and reference number, but is unable to generate a certificate.

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

5. 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 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 number are for the exclusive use of the Subscriber to generate the digital certificate.

(b) 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, any other data of the private key, or the PIN protecting the private key, to any person or entity.

(c) Specifying and always using a PIN of at least eight alphanumeric characters to protect any and all private keys associated with the FR-CA certificate. PINs should contain no words from a dictionary, and include a combination of upper and lower case characters, numbers and special characters. The Subscriber must conform to any security procedures, operating instructions, guidelines, and specifications for interconnection that the Board specifies from time to time.

(d) Notifying the End User Authorization Contact immediately if the Subscriber is unable to recall the PIN for the token devices (if applicable) that protects the Subscriber's private key, or knows or suspects that a Private Key Compromise Event has occurred.

(e) If a Private Key Compromise Event occurs, discontinuing use of a compromised private key and destroying the private key and any related certificate.

(f) Notifying the End User Authorization Contact if the Subscriber has not received the reference number within seven (7) days of the End User Authorization Contact submitting the Subscriber Request form.

(g) Notifying the End User Authorization Contact immediately if the reference number is received by a physical means that displays evidence of tampering.

(h) 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 certificate.

(i) 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.

(j) UTILIZE CERTIFICATES AND PRIVATE KEYS SOLELY IN THE MANNER FOR WHICH THEY ARE INTENDED, I.E., TO ACCESS A BOARD SYSTEM FOR OFFICIAL BUSINESS ONLY.

Once the FR-CA has issued a certificate to the Subscriber, thereby granting the Subscriber access to a Board 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 of the Participant's authorized Subscribers, except to the extent that an act or omission is caused by the negligence of the FR-CA or any RA.

2.1.3 Relying Party Obligations

1. Except as stated in paragraph 2 below, the FRBs and the Board are the Relying Parties with respect to an FR-CA issued certificate which permits Subscribers authorized access to a Board system and thus Subscribers and Participants may not rely upon an FR-CA issued certificate.

   Once the FRB's web server has received and has recognized a certificate issued by the FR-CA, it shall permit authorized access to a Board system. If a certificate is recognized but has been revoked, access will be denied.

2. The Participant acts as Relying Party only to the extent that the Participant's browser connects to the FRB server and the Subscriber is sent digitally signed executable object code related to a Board 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 must 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.

2.2 Liability

Authority to access a Board system is pursuant to a statute, regulation, or agreement and not pursuant to this CPS. Nothing in this CPS grants such authority or in any way alters, modifies, replaces, voids, or supersedes any such statute, regulation or agreement. The Federal Reserve System shall not be liable to any party who uses a FR-CA issued certificate to access a Board application for any loss or damage incurred by such party. The Federal Reserve System takes reasonable measures to ensure the quality of the data and other information accessible by use of a certificate. However, the Federal Reserve System makes no warranty, express or implied, nor assumes any legal liability or responsibility for the accuracy, correctness, or completeness of any information accessible by use of a certificate.

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

The terms of this CPS are governed by the Federal laws of the United States.

2.5 Confidentiality Policy

All information collected, generated, transmitted, and maintained by the FR-CA and/or RA in the course of issuing a certificate is considered confidential, except for information that: (i) is posted to the FR-CA's URL, (ii) is in possession of the 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 required by law or regulation, or (iii) is or becomes publicly available. This paragraph does not affect the confidentiality of any Board data that the Subscriber may access.

3. 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:	BOG
Organizational Unit:	Name of Agency or an identifying code for a filing 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.

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. 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. 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 non-ambiguity and 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 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. Operational Requirements

4.1 Certificate Application

The FR-CA and RA 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, and shall designate one such contact as the Primary Contact and the other as the Back-Up Contact. 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 at the Participant.

The Participant may contact the RA to receive the appropriate form to request a certificate. This Subscriber form will include information about the individual named by the End User Authorization Contact to receive a certificate and must be signed by the End User Authorization Contact. The completed Subscriber Request form must be returned to the RA. A Participant's End User Authorization Contacts are responsible for the identification of Subscribers and the notification processes between the Participant and the RA. The End User Authorization Contacts will be required to validate the identity, authority, and, if applicable, roles of the Subscriber to the RA.

4.2 Certificate Issuance

Certificates are issued by the FR-CA in accordance with the following practice:

1. After a Participant submits a completed Subscriber form, the RA will contact the End User Authorization Contact who will validate the identity, authority, and roles of the Subscriber to the RA. The End User Authorization Contact must immediately notify the RA if the Subscriber should not be issued a certificate. The RA will provide the End User Authorization Contact with an authorization code that the End User Authorization Contact must provide to the Subscriber. The RA will enter the request using RA client software to communicate the information to the FR-CA.

2. A communication containing a reference number will be sent to the Subscriber.

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 <http://www.federalreserve.gov/PKICertificates/> in order to submit a certificate request. The reference number combined with the authentication code uniquely identifies the Subscriber to the FR-CA.

4. Except for certificates to access the Board's electronic application filing system, the following set of actions are performed by the Subscriber's browser software, working in conjunction with programs on the FRB and Board certificate web site and the FR-CA system:

   (a) The Subscriber's token device generates a public key/private key pair. The Subscriber is asked to apply a PIN to protect the private key. The public key is submitted to the FRB/Board certificate web site as a certificate request.

   (b) The FRB/Board certificate web site passes the certificate request to the FR-CA using an SSL 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 FR-CA's certificate to the FRB/Board certificate web site.

   (c) The FRB/Board 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 token device.

Upon completion of these steps, the Subscriber has a certificate issued by the FR-CA; this certificate is located on the Subscriber's token device along with the FR-CA public key certificate. The Subscriber is also granted the appropriate permissions for specific web Board systems, and is now able to access and use these systems. In the case of a certificate used to access the Board's electronic application filing system, the Subscriber does not use a token device to generate a public key/private key pair as set forth above in 4(a) and the certificate is not stored on a token device. Instead, upon completion of these steps, the Subscriber has a certificate issued by the FR-CA; this certificate is located on the Subscriber's hard drive along with the FR-CA public key certificate. The Subscriber is also granted appropriate permissions and is now able to access and use the electronic application filing system.

4.3 Certificate Acceptance

When a certificate issued to a Subscriber is used to access a Board system 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. Prior to using the certificate to access a Board system for the first time, the Subscriber must verify that the newly-generated certificate contains the FR-CA certificate fingerprint value as identified in setup materials provided to the Participant.

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. Upon receipt of a revocation request, the RA calls the 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 Certificate Revocation List (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 Board application.

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 PIN protecting the Subscriber's private key is compromised (i.e., thought to be known by any other person or entity other than the Subscriber);

2. the Subscriber no longer requires access to a Board system;

3. the Subscriber's employment or affiliation with the Participant is terminated;

4. the FR-CA or RA, in their sole discretion, believes revocation of a certificate is warranted; or

5. 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, if possible, in advance of the time at which any of the above events occurs. In the case of a known or suspected Private Key Compromise Event, the End User Authorization Contact must notify the RA. 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 by the RA until the following business day.

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 Subscriber or Participant, the request will be documented.

4.5 Audit Procedures

The FR-CA 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 and Board record retention policies.

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. 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 the employment process.

6. 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. Certificate and CRL Profiles

7.1 Certificate Profile

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

8. CPS Administration

8.1 Change Procedures

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

8.2 Approval Procedures

This CPS is approved by the FRBs and Board.