Federal Reserve Certification Authority (FR-CA)
Certification Practice Statement
for United States Treasury Auctions

1.0 INTRODUCTION

1.1 OVERVIEW

The Federal Reserve Bank of New York ("FRBNY") acts as fiscal agent of the United States Department of the Treasury ("Treasury"), including the Treasury's Bureau of the Public Debt ("BPD"). In this capacity, FRBNY operates and maintains the Treasury Automated Auction Processing System ("TAAPS") business application in support of U.S. Treasury auctions. 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 for use in accessing the TAAPS business application by the TAAPS application's users, including the FRBNY and other Treasury authorized employees and agents, primary dealers and other Treasury auction bidders, certain clearing banks who receive Treasury securities at original issue, and other authorized entities. 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 the Treasury, a primary dealer, depository institution or other entity that is bidding in a Treasury auction, is the agent of an entity bidding in a Treasury auction, or is otherwise authorized to access the TAAPS application by the FRBNY. A subscriber ("Subscriber") is a named individual employee or agent of a Participant who is issued a certificate to access the TAAPS business application. By accessing the TAAPS business application by means of a certificate, the Participant and Subscriber agree to the provisions of this CPS and applicable Treasury regulations and agreements.

1.2 IDENTIFICATION

This CPS is called the Certification Authority (FR-CA) Certification Practice Statement for United States Treasury Auctions. The current issue is version 1.0, dated June 26, 2007.

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. In most cases, certificates will be generated by the FR-CA and sent to the Subscriber on a token-based media ("token-based certificates"). In other limited instances, a certificate may be issued after the Subscriber follows the appropriate steps to generate the certificate from the certificate retrieval web site ("browser-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

The Registration Authority ("RA") is one or more FRBs that collect and process Subscriber requests from the Local Registration Group, containing information about the Subscriber's identity, authorization, roles, and other information.

1.3.2.1 LOCAL REGISTRATION GROUP

The Local Registration Group ("LRG") shall be within the Markets Group at the FRBNY, and serving in a capacity delegated from the RA and with approval of the FR-CA, shall collect and validate the Participant's authorized contacts, along with a Subscriber's identity, authorization, roles, and other information.

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.   To obtain the location of this repository, contact the LRG.

1.3.4 PARTICIPANTS/SUBSCRIBERS

A Participant is the Treasury, or a primary dealer, a depository institution or other entity that is bidding in a Treasury auction, or is the agent of an entity bidding in a Treasury auction, or is otherwise authorized to access the TAAPS application by the FRBNY. A Subscriber is a named individual employee or agent of a Participant who is issued a certificate to access the TAAPS application.

In some instances, a Participant may seek to access the TAAPS 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.

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, which rely on the certificate to permit Subscribers to access the TAAPS 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 LRG 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 LRG concerning the request form used to designate a TAAPS End User Authorization Contact ("TAAPS-EUAC") and if applicable, a certificate request form.

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

3. Sending, for a token-based certificate, a token passphrase to a Subscriber.

4. Sending, for a token-based certificate, a related token to the TAAPS-EUAC.

5. Sending, for a server or browser-based certificate, authorization codes to the Participant after receiving a properly completed and verified request from a Participant.

6. Sending, for a server or browser-based certificate, reference codes to the Subscriber after receiving a properly completed and verified request from a Participant.

7. Creating and maintaining an accurate audit trail.

The LRG is responsible for the following:

1. Validating information submitted to the LRG by the Participant concerning the request used to designate a TAAPS-EUAC and if applicable a certificate request.

2. Confirming certificate revocation requests with the Participant.

3. Confirming and initiating validated certificate renewal requests.

4. Notifying the RA without delay of confirmed requests for certificate revocation received from the Participant, TAAPS-EUAC, or Subscriber.

5. Creating and maintaining an accurate audit trail.

These responsibilities of the FR-CA, the RA and the LRG 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 a description of the certificate issuance process.

A certificate will be revoked as soon as practicable following receipt of a revocation request and its confirmation by the LRG, 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 the TAAPS application. 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 TAAPS-EUACs. The identification must be signed and dated by an authorized representative of the Participant. The Participant also is responsible for informing the LRG, in accordance with the LRG's then-standard procedures, of all updates and substitutions made for the TAAPS-EUACs, as events warrant (due to employee retirement, reassignment, termination, etc.). A TAAPS-EUAC is not permitted to request or approve a Subscriber certificate for himself or herself.

2. The Participant must complete the necessary Subscriber information to request a certificate for a Subscriber.

3. A Participant's TAAPS-EUACs are responsible for the identification of Subscribers and the notification processes between the Participant and the LRG. The TAAPS-EUAC shall provide the token to the Subscriber only if the TAAPS-EUAC has first validated the identity of the

Subscriber and has authorized the Subscriber to access the TAAPS application. In the case of server-based or browser-based certificates, the Participant's TAAPS-EUAC shall provide an authorization code to the Subscriber only if the TAAPS-EUAC has first validated the identity of the Subscriber and has authorized the Subscriber to access the TAAPS application; the TAAPS End User Authentication Contact shall otherwise keep authorization codes confidential. The EUAC must notify the LRG 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 TAAPS-EUACs to validate the identity and authority of that Participant's Subscribers.

4. At least one of the Participant's TAAPS-EUACs must notify the LRG, 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 TAAPS;

   (c) the Subscriber knows or suspects that his or her private key or any password or token-based passphrase 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. 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 LRG if the Technical Contact no longer has responsibility for the Participant's 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 TAAPS-EUAC must notify the LRG, by telephone and in writing, following the occurrence of any of the following events:

   (a) The TAAPS-EUAC has not received the token in the case of a token-based certificate, or an authorization code for a server or browser based certificate, within four (4) business days of submitting the Subscriber request;

(b) The Subscriber has not received, for a token-based certificate, the token passphrase or, for a server-based or a browser-based certificate, the reference number within four (4) business days of the TAAPS-EUAC submitting the Subscriber request;

(c) The TAAPS-EUAC or the Subscriber receives, for a token-based certificate, the token, and the token displays evidence of tampering.

(d) A Subscriber attempts to use the token-based certificate but is unable to access the TAAPS application.

(e) A Subscriber attempts to use the authorization code and reference number, but is unable to generate a server or browser-based certificate.

All telephone calls and written notices provided by a TAAPS-EUAC under this paragraph 2.1.2 must be to the LRG in accordance with that LRG's instructions.

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 token-based certificates, the security of the token and the confidentiality of the token passphrase, which are for the exclusive use by the Subscriber to access and use the token-based certificate.

(b) Maintaining the confidentiality of the authorization code obtained from the Participant's TAAPS-EUAC 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.

(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, any other data of the private key, or the password or token-based passphrase protecting the private key, to any person or entity.

(d) Specifying and always using a password or token-based passphrase of at least eight alphanumeric characters to protect any and all private keys associated with the FR-CA certificate. Passwords and token-based passphrases 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 that the LRG specifies from time to time. The Participant shall be wholly responsible and liable for all Private Key Compromise Events.

(e) Notifying the TAAPS-EUAC immediately if the Subscriber is unable to recall the passphrase 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.

(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 TAAPS-EUAC if the Subscriber has not received the reference number within four (4) days of the EUAC submitting the Subscriber Request form.

(h) Notifying the TAAPS-EUAC immediately if the token is received by a physical means that displays evidence of tampering.

(i) Notifying the TAAPS-EUAC immediately if a Subscriber attempts to use the reference number and authorization code provided to the Subscriber, but is unable to generate a certificate.

(j) Acting in accordance with all other FR-CA procedures and instructions distributed by the LRG, the RA or the FR-CA, related to requesting certificates and sending messages to the LRG, the RA and FR-CA.

(k) UTILIZE CERTIFICATES AND PRIVATE KEYS SOLELY IN THE MANNER FOR WHICH THEY ARE INTENDED, I.E., TO ACCESS THE TAAPS APPLICATION FOR OFFICIAL BUSINESS ONLY.

Once the FR-CA has issued a certificate to the Subscriber, thereby granting the Subscriber access to the TAAPS 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, RA, or LRG's failure to exercise ordinary care or act in good faith.

The above requirements set forth in this Section 2.1.2 (6) (a), (c), (d), (e), and (h) 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 for special connectivity purposes, 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.

2.1.3 RELYING PARTY OBLIGATIONS

A. Except as stated in Paragraph B below, the FRBs are the Relying Parties with respect to certificates that permit Subscribers to access the TAAPS 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 TAAPS transactions to be processed. If a certificate is recognized but has been revoked, TAAPS 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 LRG immediately. Neither the FR-CA, RA nor the LRG 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

The U.S. Treasury Auctions Submitter Agreement, applicable Treasury offering announcements, and relevant U.S. Treasury regulations regarding the sale and issue of U.S. Treasury securities, electronic transactions, and *TREASURYDIRECT* transactions, sets forth applicable liability provisions. Nothing in this CPS limits any rights a Reserve Bank may have 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 the U.S. Treasury Auctions Submitter Agreement.

2.5 CONFIDENTIALITY POLICY

All information collected, generated, transmitted, and maintained by the FR-CA, RA and/or LRG in the course of issuing a certificate is considered confidential, except for information that: (i) is posted to the TAAPS application 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, RA, and/or LRG 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 or pseudo ABA number
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. 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. 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.

3.1.3 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, RA or LRG 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, RA and LRG 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 LRG is responsible for validating the authorization of the TAAPS-EUACs, 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 LRG, 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 TAAPS-EUAC and confirmed by the LRG 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, RA and LRG shall enforce the following practice with respect to a Subscriber's application:

As required by Section 2.1.2, the Participant must provide the LRG with the names and contact information for at least two (2) TAAPS-EUACs. The LRG shall use internal policies and procedures of the RA to verify that the names of the TAAPS-EUACs are sent by authorized personnel of the Participant.

The Participant may contact the LRG to receive instructions to designate a Subscriber and request a certificate. The completed Subscriber request must be sent to the LRG. A Participant's TAAPS-EUACs are solely responsible for the identification, authentication, and notification processes between the Participant and the LRG. The TAAPS-EUACs will be required to validate the identity, and authority of the Subscriber to the LRG.

4.2 CERTIFICATE ISSUANCE

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

1. After a Participant submits to the LRG a new Subscriber request, the LRG will contact the Participant's TAAPS-EUAC, who will be asked to validate the request, including the identity, and authority requested for the Subscriber to the LRG. The Participant's TAAPS-EUAC must immediately notify the LRG if the Subscriber should not be issued a certificate.

2. The LRG will send all requisite information to the RA necessary to create a Subscriber credential. In the case of a token-based certificate, the RA

will be responsible for coordinating the distribution of the Subscriber token and its associated passphrase. The token will be shipped to the TAAPS-EUAC and the passphrase will be sent directly to the Subscriber. The RA will notify the LRG when the passphrase has been sent to the Subscriber.

In the case of a server or browser-based certificate, the RA will be responsible for distributing: (i) reference number to the Subscriber; and (ii) authorization code to the TAAPS-EUAC, both of which shall be necessary in order to download the certificate directly from the FR-CA.

3. Upon receipt of the token, the TAAPS-EUAC must provide the token to the Subscriber. Separately, the Subscriber will have received the token's unique, associated passphrase from the RA.

   In the case of a server or browser-based certificate, the TAAPS-EUAC must provide the Subscriber with the authorization code sent by the RA. The Subscriber will have received a specific reference number directly from the RA. With the authorization code and the reference number, 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. The Subscriber's browser software will then perform actions necessary to generate a certificate. The Subscriber must install the certificate on a browser or secure web server. The certificate must be protected using a password and other security mechanisms as appropriate.

4. Upon completion of these steps, the TAAPS Subscriber will have a validated certificate issued by the FR-CA. The Subscriber is thereby granted the appropriate permissions to access and use the TAAPS application.

4.3 CERTIFICATE ACCEPTANCE

When a certificate issued to a Subscriber is used to access the TAAPS 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 LRG with a request to revoke a Subscriber's certificate. A certificate will be revoked as soon as practicable following receipt of a revocation request (and if possible 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 or LRG. Except as otherwise provided, Subscribers will not be notified directly of certificate revocation, but will be denied access to the TAAPS application.

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.

Upon receipt of a revocation request, the LRG may, in certain instances, call a TAAPS-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 FR-CA, where the revocation is processed. A revocation request may also be initiated by the LRG, 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 the TAAPS application. Server or browser-based certificates relied upon by the Participant for special connectivity with the FRBs may be subject to different certificate directory, revocation and CRL requirements.

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; or

2. If the FR-CA determines it is necessary to revoke the certificate issued to the Participant for special connectivity purposes.

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.

4.4.1 CIRCUMSTANCES FOR REVOCATION

A certificate will be revoked by the FR-CA if the FR-CA, RA or LRG determines that any of the following events have occurred:

(1) the Subscriber's private key or the password or token-based passphrase 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 the TAAPS 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, RA or LRG, in their sole discretion, believe 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 TAAPS End User Authorization Contact notifies the LRG 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, a TAAPS-EUAC must notify the LRG 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 LRG.

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 LRG prior to (or if impossible, immediately after) the occurrence of any of the following events:

(1) the Participant no longer requires access to the TAAPS 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 entity.

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 a TAAPS-EUAC. The FR-CA reserves the right to revoke any certificate if the FR-CA, RA or LRG, in their sole discretion, believes revocation of a certificate is warranted or if the private key of the FR-CA is compromised.

4.4.2 WHO CAN REQUEST REVOCATION

Revocations may be requested by:

- Participant's TAAPS-EUAC
- LRG
- RA
- FR-CA

4.4.3 PROCEDURE FOR REVOCATION

See Section 4.4. When the request is initiated by the LRG, RA or FR-CA without a request from the 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 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, RA and LRG 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 twenty 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 TAAPS-EUACs 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.