The trust behind your digital identity
ORC
Operational Research Consultants, Inc.

Certification Practices Statement Summary
For the
Operational Research Consultants, Inc. (ORC)
Non-Federal Issuer (NFI)
Public Key Infrastructure (PKI)

Version 1.2

February 24, 2012

11250 Waples Mill Road
South Tower, Suite 210
Fairfax, VA 22030

Revision History

Document Version	Revision Date	Revision Details
0.1	11 March 2011	Initial version established to support cross-certification with FBCA as an NFI
	2 May 2011	Edits to comply with ORC NFI CP.
	5 May 2011	Edits to comply with ORC NFI CP.
1.0	10 June 2011	Edits resulting from Triennial Phase 1 audit.
1.1	17 Nov 2011	Updates resulting from operational updates and completion of Triennial Phase 1 audit.
1.2	24 Feb 2012	Updates for Public Release

1 Introduction

Operational Research Consultants, Inc. (ORC), as a Non-Federal Issuer supporting the Personal Identity Verification (PIV) initiative, has elected to establish a certificate authority designed and maintained in accordance with established guidance for the purpose of issuing identity cards that are "(a) technically interoperable with Federal government PIV systems, and are (b) issued in a manner that allows Federal government relying parties to trust the cards."[1] The ORC NFI PKI will operate in accordance with the Operational Research Consultants, Inc. Non Federal Issuer Certificate Policy (CP), v1.0.1, dated March 8, 2011.

- The goal of the ORC NFI PKI is to issue identity cards that can be "trusted by the Federal government" through cross-certification with the Federal Bridge Certification Authority (FBCA), accepted as a valid physical and logical form of identity within and outside of the Federal government, and provide a commensurate level of assurance to complement the Federal PKI community. At a minimum, the ORC NFI PKI will provide the following security management services:
- Key generation/storage
- Certificate generation, modification, renewal, rekey, and distribution
- Certificate revocation list (CRL) generation and distribution
- Directory management of certificate related items
- Certificate token initialization/programming/management
- System management functions (e.g., security audit, configuration management, archive.)

[1] "Personal Identity Verification Interoperability for Non-Federal Issuers", May 2009 {www.idmanagment.gov}

In accordance with the ORC NFI CP, subscribers are required to use FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys. Furthermore, the use of ORC NFI certificates with devices requires use of FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys.

ORC NFI public key certificates may be utilized for non-Federal government and non-government individual identity and device authentications by Federal, state, local, and non-government entities (Relying Parties). Any use of or reference to the ORC NFI CP or this CPS outside of the purview of the ORC NFI PKI is specifically prohibited. It is intended that the ORC NFI PKI support only interoperability with the Federal PKI.

This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) request for comments (RFC) 3647, CP and Certification Practice Statement Framework.

The terms and provisions of this ORC NFI CPS are to be interpreted under and governed by applicable Federal law and the laws of the Commonwealth of Virginia.

1.1 Overview

This ORC NFI Certification Practices Statement (CPS) is the implementation document for Operational Research Consultant's (ORC's) NFI PKI (also known as the ORC Non-Federal Issuer (NFI) Public Key Infrastructure, "ORC NFI PKI").

Operation of the ORC NFI PKI is established with cross-certification with the FBCA. Successful cross certification asserts that the ORC NFI operates in accordance with the standards, guidelines and practices of the Federal PKI Policy Authority (FPKIPA), acting on the authority of the Identity, Credential and Access Management Subcommittee (ICAMSC) of the Federal Chief Information Officer (CIO) Council's Information Security and Identity Management Committee (ISIMC).This CPS is applicable to individuals, business representatives, State and Local Government employees, relying parties, and organization applications who [that] directly use these certificates, and who are responsible for applications or servers that use certificates. Certificate users include, but are not limited to, Certificate Management Authorities (CMAs), Registration Authorities (RAs), Issuing Authorities (IAs), Local Registration Authorities (LRAs), subscribers, and relying parties.

In accordance with the stipulations of this CPS, the ORC NFI CAs issue certificates asserting PIV-I OIDs in accordance with the current ORC NFI CP and this CPS. This CPS describes the operations of the ORC NFI PKI and the services that the ORC NFI PKI provides. These services include:

- Subscriber Registration: A subscriber or certificate applicant must appear in person before an ORC Registration Authority (RA), an approved Local

Registration Authority (LRA) or a registered Notary Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions), as stipulated by the Policy Authority, present valid identification (driver's license, passport, etc.), sign the subscriber's obligation and mail the forms to ORC.

- Subscriber Enrollment: The ORC NFI system provides Federal Information Processing Standards (FIPS) 140-2 Level 3 Secure Socket Layer (SSL) connections to the certification authority. The subscriber must use a FIPS 140-2 Level 1 or 2 client for connection for enrollment.
- Enrollment Validation: The ORC registration process validates the subscriber enrollment information (see above).
- Certificate Issuance: When notified by an RA of a valid enrollment request, an ORC IA issues the requested certificate for delivery to a FIPS 140-2 Level 1 or 2 client. A FIPS 140-2 Level 1 issuance does not require a hardware token. ORC then notifies the subscriber of the issuance and provide instructions for receiving the certificate.
- Certificate Publishing: When a certificate is issued, the ORC publishes it to a Lightweight Directory Access Protocol (LDAP) directory. The directory may be accessed via Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) gateway or via the LDAP protocol.
- Certificate Status information: In the form of Certificate Revocation Lists (CRLs) distribution (via LDAP and HTTP) and Online Certificate Status Protocol (OCSP) responses.

To assist in providing these services and in meeting the reporting requirements outlined in this CPS, ORC maintains a website, which contains instructions, online forms, a summary of this CPS, compliance audit results, and copies of certificates and CRLs. The majority of the information on the website is publicly accessible, although it incorporates SSL to promote data integrity and to allow users to validate the source of the information. Portions of the website are access controlled and require certificate authentication for access to authorized individuals.

ORC is periodically audited by its independent IT auditor against this CPS and operates primary and secondary secure data centers in conformance with the U.S. General Services Administration (GSA), National Security Agency (NSA), and commercial best practices.

1.1.1 Certificate Policy

The ORC NFI PKI operates in accordance with the policies established in the ORC NFI Certificate Policy (CP). The ORC NFI CP is mapped to the Federal

Bridge Certification Authority Certificate Policy by an independent third party, to ensure compliance with the FBCA CP and that the ORC NFI CP defines a commensurate level of assurance with the requirements of the FBCA. ORC NFI certificates contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to the specific type and specific level of assurance for all ORC NFI certificates issued under this CPS, which are available to all Relying Parties. Each ORC NFI certificate issued asserts the appropriate level of assurance in the *certificatePolicies* extension.

1.1.2 Relationship between the CP and the CPS

This CPS applies to X.509 version 3 certificates with assurance levels as defined in the ORCNFI CP as used to protect information up to and including Sensitive But Unclassified (SBU). The policies and procedures in this CPS are applicable to individuals who manage the certificates, who directly use these certificates, and individuals who are responsible for applications or servers that rely on these certificates.

1.1.3 Relationship between the NFI CP and the Federal Bridge Certification Authority (FBCA) CP

ORC NFI is a participant in a Memorandum of Agreement (MOA) with the Federal PKI Policy Authority (FPKIPA), which sets forth the respective responsibilities and obligations of both parties and the mappings between the certificate levels of assurance contained in the NFI CP and those in the FBCA CP.

1.1.4 Scope

The ORC NFI PKI exists to facilitate trusted electronic business transactions for State and Local Governments, and non-Federal organizations and individuals. This ORC NFI CPS describes the following:

- Roles, responsibilities, and relationships among the CAs, Registration Authorities (RAs), Certificate Manufacturing Authorities (CMAs), Repositories, Subscribers, Relying Parties, and the Policy Authority (PA) (referred to collectively herein as “Program Participants”) authorized to participate in the PKI described by this ORC NFI CP
- The primary obligations and operational responsibilities of the Program Participants
- The rules and requirements for the issuance, acquisition, management, and use of ORC NFI certificates to verify digital signatures

This CPS is applicable to individuals, business representatives, State and Local Government employees, relying parties, and organization applications who [that] directly use these certificates, and who are responsible for applications or servers that use certificates. Certificate users include, but are not limited to, Certificate Management Authorities (CMAs), Registration Authorities (RAs), Issuing Authorities (IAs), Local Registration Authorities (LRAs), subscribers, and relying parties.

1.1.5 Interaction between ORC NFI and the Federal Government

The ORC NFI CP and ORC NFI CPS collectively ensure interoperability between the FBCA and all Authorized NFI CAs. MOAs with the FPKIPA and other entities ensure interaction and interoperability with authorized Federal Government and non-government CAs.

1.2 Document Name and Identification

The NFI CP is registered with the Computer Security Objects Register (CSOR) at the National Institute of Standards and Technology (NIST). The ORC NFI PKI and each CA complies with the following object identifiers (OIDs) for the NFI Certificates defined in this CPS:

ORC NFI CP Description	Description	Policy OID
ORC NFI Authorized CA	id-orc-nfissp-ca	::= {1.2.840.113549.5.6.1.3}
ORC NFI Medium	id-orc-nfissp -medium	::={ 1.2.840.113549.5.6.1.3.1.3}
ORC NFI Medium Hardware	id-orc-nfissp -mediumhardware	::={ 1.2.840.113549.5.6.1.3.1.12}
ORC NFI PIV-I Hardware	id-orc-nfissp-pivi-hardware	::={ 1.2.840.113549.5.6.1.3.1.18}
ORC NFI PIV-I Card Authentication	id-orc-nfissp-pivi-cardAuth	::={ 1.2.840.113549.5.6.1.3.1.19}
ORC NFI PIV-I Content Signing	id-orc-nfissp-pivi-contentSigning	::={1.2.840.113549.5.6.1.3.1.20}
ORC NFI Device	id-orc-nfissp-devices	::={ 1.2.840.113549.5.6.1.3.1.21}

Table 1, ORC NFI Object Identifiers

ORC NFI certificates issued under this CPS reference the ORC NFI CP in the Certificate Policies field. Additionally, each ORC NFI CA that issues certificates asserting a PIV-I OID will be cross-certified with the FBCA CA or an Authorized CA that holds a certificate signed by the FBCA CA. The foregoing OIDs may not be used except as specifically authorized by the NFI CP. Unless specifically approved by the Federal PKI Policy Authority, ORC CAs do not assert the FBCA CP OIDs in any certificates issued, except in the policyMappings extension establishing an equivalency between an FBCA OID and an OID in the NFI CP. Only the OIDs identified above are used within ORC certificates with the exception of the policyMappings extension, which may assert other PKI Policy OIDs for purposes of cross certification of the ORC NFI PKI to another PKI. CSOR information is available from 1) http://csrc.nist.gov/groups/ST/crypto_apps_infra/csor/index.html, and 2) csor@nist.gov.

The ORC NFI PKI and this CPS support medium assurance and medium-hardware assurance levels as defined in Section 1.4.1.

The requirements associated with PIV-I Hardware and PIV-I Content Signing are identical to Medium Hardware except where specifically noted in the text and further described in Appendix A.

In addition, the PIV-I Content Signing policy is reserved for certificates used by the ORC Card Management System (CMS) to sign the PIV-I card security objects.

These Object Identifiers are specifically mapped to the requirement for Personal Identification Verification – Interoperable (PIV-I). The requirements associated with the Medium Hardware certificates are identical to those defined for the Medium Assurance certificates, with the exception of subscriber cryptographic module requirements.

id-orc-nfissp-medium::={ 1.2.840.113549.5.6.1.3.1.3}

Maps to FBCA Medium Assurance. For users with software cryptographic modules. Uses: digital signature, client authentication, encryption.

id-orc-nfissp-medium ::= {1.2.840.113549.5.6.1.3.1.3}

Maps to FBCA mediumAssurance. For users with software cryptographic modules. Uses: digital signature, client authentication, encryption. Mutually exclusive of id-orc-nfissp-mediumHardware.

id-orc-nfissp-mediumHardware ::= {1.2.840.113549.5.6.1.3.1.12}

Maps to FBCA mediumHardware. For users with hardware cryptographic modules (e.g., smart card). Uses: digital signature, client authentication, encryption. Mutually exclusive of id-orc-nfissp-medium.

id-orc-nfissp-pivi-hardware ::= {1.2.840.113549.5.6.1.3.1.18}

For user authentication only, no digital signature capability (comparable to PIV authentication with pivFASC-N name type). Uses: client authentication for physical access after private key activation; requires OCSP services. Note: a certificate asserting this policy OID is referred to as PIV-interoperable Authentication certificate, or PIV-I Auth.

id-orc-nfissp-pivi-cardAuth ::= {1.2.840.113549.5.6.1.3.1.19}

For user authentication only, no digital signature capability (comparable to PIV card authentication with pivFASC-N name type). Uses: client authentication for physical access- private key can be used without subscriber activation; requires OCSP services. Note: a certificate asserting this policy OID is referred to as a PIV-interoperable Card Authentication certificate or PIV-I Card Auth.

id-orc-nfissp-pivi-contentSigning ::= {1.2.840.113549.5.6.1.3.1.20}

For signing by the CMS only. Uses: certificates used by the Card Management System (CMS) to sign objects on the PIV-I Card (e.g., CHUID, Security Object).

id-orc-nfissp-devices ::= [1.2.840.113549.5.6.1.3.1.21}

For devices only; requires a human sponsor. Uses: device authentication, encryption.

Certificates issued to a Non-Federal SSP CA may contain any or all of these OIDs. Certificates issued to users to support digitally signed documents or key management may contain the id-orc-nfissp-medium, or id-orc-nfissp-mediumHardware. Certificates issued to devices under this policy shall include the id-orc-nfissp-devices. Certificates issued to users supporting authentication but not digital signature may contain id-orc-nfissp-authentication. Certificates issued to users supporting authentication where the private key can be used without user authentication may contain id-orc-nfissp-cardAuth. These Policy Object Identifiers are populated in accordance with CPS section 7.1.6.

1.3 Community and Applicability

This CPS describes the practices governing the operation of a bounded public key infrastructure. It describes the rights and obligations of persons and entities authorized under the CP and this CPS to fulfill any of the following roles:

Certificate Service Provider

- Certification Authority (CA)
- Registration Authority (RA)
- Certificate Manufacturing Authority (CMA)
- Repository

End Entity

- Medium
- Medium Hardware
- Device
- PIV-I Hardware
- PIV-I Card Authentication
- PIV-I Content Signing

Policy Authority

Requirements for persons and entities authorized to fulfill any of the above roles are defined in this Section.

Additional obligations are set forth in other provisions of the CP; and in the requirements of this CPS, the ORC System Security Plan (SSP), Privacy Practices and Procedures (PPP), any agreements with Relying Parties, and Subscriber Agreements.

The following are roles relevant to the administration and operation of CAs operating under this CPS and the applicable policy:

1.3.1 NFI PKI Authorities

1.3.1.1NFI Policy Authority

The ORC Board serves as the Policy Authority and is responsible for organizing and administering the ORC NFI CP and the ORC NFI MOA(s).

Those ORC Board members are:

ORC Chief Executive Officer
ORC Chief Operating Officer
ORC Executive Director

1.3.1.2NFI Program Manager

The ORC NFI Policy Authority serves as the NFI Program Management Office (PMO) and is responsible for organizing and administering the ORC NFI program and ORC NFI Contracts/MOAs. The ORC NFI Program Manager is:

ORC Executive Director, NFI Program

1.3.1.3NFI Policy Management Authority

The ORC Board serves as the NFI policy management authority to manage the Authorized NFI CAs in accordance with the NFI MOA and the NFI CP and to resolve name space collisions within the NFI program.

1.3.1.4Authorized ORC NFI CAs

ORC is an authorized NFI CA and may issue certificates that reference the ORC NFI CP, having qualified as an Authorized NFI CA by:

1. Having been granted Interim Authority to Operate (IATO) by the ORC NFI Policy Authority;

2. Documenting the specific implemented practices and procedures under which ORC satisfies the requirements of the NFI CP in the ORC NFI CPS;

3. Successfully completing Security Certification and Accreditation (C&A) in accordance with Federal, GSA, and NFI laws, regulations, and guidelines; and

4. Successful completion of cross-certification with the FBCA.

ORC is responsible for all aspects of the issuance and management of ORC NFI Certificates, including:

- The application/enrollment process
- The identification verification and authentication process
- The certificate manufacturing process
- Dissemination and activation of certificates

- Publication of certificates
- Renewal, suspension, revocation, and replacement of certificates
- Verification of certificate status upon request
- Generation and destruction of CA signing keys
- Ensuring that all aspects of the ORC NFI CA services and ORC NFI CA operations and infrastructure related to NFI Certificates issued under the NFI CP and this CPS are performed in accordance with the requirements, representations, and warranties of the NFI CP (the only exception being when the Government, pursuant to agreement between GSA, Relying Parties, and the ORC NFI provides defined portions of the RA role and function) and this CPS

ORC is responsible for ensuring that all work is performed under the supervision of the ORC or responsible employees of the ORC, and provides assurance of the trustworthiness and competence of employees and their satisfactory performance of duties relating to provision of NFI services. Each ORC NFI CA or employee of ORC to whom information may be made available or disclosed is notified in writing by ORC that information so disclosed to ORC or ORC's employees can be used only for the purposes and to the extent authorized herein.

ORC complies with all applicable Federal and GSA requirements, including those for the prevention and reporting of waste, fraud, and abuse set forth in the NFI MOA.

1.3.1.4.1 Cross-Certification with the FBCA

ORC has designated specific CAs within the ORC NFI CA to cross certify directly with the FBCA (e.g., through the exchange of cross-certificates). The designated ORC NFI CAs issue either end-entity certificates or CA certificates to other ORC NFI CAs, or both. Where the ORC NFI CA operates a hierarchical PKI, the designated CA serves as the Root CA. Where the ORC NFI CA operates a mesh PKI, the designated ORC CA for cross-certification with the FBCA may be any CA within their PKI.

ORC NFI CAs may request that the FBCA cross certify with more than one CA within our PKI, whether or not the ORC NFI CA employs a hierarchical or other PKI architecture.

1.3.1.5Certificate Status Servers

ORC operates a CSA using an OCSP responder that provides revocation status and/or certificate validation responses. The ORC CSA practices conform to the stipulations of the NFI CP and this CPS. All ORC CSA practice updates, as well as any subsequent changes are updated in this CPS and submitted to the Policy Authority for conformance assessment. The CSA practices include:

- Conformance to the stipulations of the NFI CP and this CPS.
- Ensuring that certificate and revocation information is accepted only from valid CAs.
- Providing only valid and appropriate responses.
- Maintaining evidence of due diligence being exercised in validating certificate status.

1.3.2 Registration Authorities

RAs are designated directly by an ORC CAA and are issued RA certificates for the purpose of submitting digitally signed verification of applicant identities and information to be entered into public key certificates. ORC RAs use hardware tokens for their RA certificates. RAs appear in person to either a CAA or an IA for identity verification with official identification, in accordance with the requirements of Section 3.1.9. RAs are provided training in identity proofing and in the policies and processes of this CPS prior to being issued their RA certificates. RA certificates are not valid for performing administrative tasks on the CA or IA equipment, including issuing or revoking certificates.

Upon designation by an ORC CAA, the designated RA(s) receive training covering:

General Training on the certificate policy

certificate assurance levels

key-pair life cycle and timing constraints

Certificate registration procedures

certificate security requirements

certificate naming conventions

identity verification requirements

Training on Identity Verification procedures and requirements

Verification of individual identity and affiliation

supporting identity document requirements

Privacy Act of 1974

At the completion of training, the designated RA(s) signs an Appointment Letter attesting to the responsibilities incumbent upon the role of RA. The Appointment

Letter is then signed by either the ORC Chief Operating Officer or the ORC Chief Executive Officer.

Following completion of the Appointment process, the RA(s) is issued Medium Hardware certificates on a Hardware token to be used for RA functions. The RA(s) may then proceed with performing the duties of an RA.

The RA is responsible for applicant registration, certificate application, and authentication of identity functions for State and Local Government Representatives, Organizational Representatives (individual subscribers), Servers, and Relying Parties. An RA may also be responsible for handling suspension and revocation requests, and for aspects of Subscriber education.

1.3.3 Card Management System (CMS)

The Card Management System is responsible for managing ORC NFI smart card token content. In the context of this CPS, the CMS requirements are associated with the Medium Hardware and PIV-I policies only. ORC NFI CAs issuing Medium Hardware or PIV-I certificates are responsible for ensuring that all CMSs meet the requirements described in this document, including all requirements specified in Appendix B. In addition, the CMS shall not be issued any certificates that express the PIV-I Hardware or PIV-I Card Authentication policy OID.

The Card Management Master Key is maintained in a FIPS 140-2 Level 2 Cryptographic Module that conforms to [NIST SP 800-78] requirements. Diversification operations are used for the operation of the Hardware Security Module (HSM). The diversification setting is an inherent feature within the HSM, and is verified as enabled during initial HSM configuration. Use of these keys requires PIV-I Hardware or commensurate.

Activation of the Card Management Master Key requires strong authentication of Trusted Roles. The Master Key is generated and maintained on the Hardware Security Module (HSM). The process requires two-person controls for physical access to the HSM and a “k of m” quorum to perform the requisite operation on the HSM.

Card management is configured such that only the authorized ORC NFI CMS can manage issued cards.

All personnel who perform duties with respect to the operation of the CMS receive comprehensive training. Any significant change to CMS operations results in a training (awareness) session, which is subsequently documented. The documentation of training is maintained in a Security Training binder.

Incident handing procedures for the CMS are part of ORC overall contingency planning procedures. A test of the contingency plan is performed at least annually to ensure proper execution of the procedures in place. If the CMS were compromised, all certificates issued to the CMS will be revoked, if applicable.

The damage caused by the CMS compromise will be assessed as stated in the contingency plan and all Subscriber certificates that may have been compromised will be revoked, and Subscribers will be notified of such revocation via either email notification or by an alert posted to the ORC NFI website. The CMS will then be re-established.

All Trusted Roles who operate an ORC NFI CMS are allowed access only when authenticated using a method commensurate with PIV-I Hardware or equivalent Medium-Hardware or higher assurance level.

1.3.4 Subscribers

A subscriber is the EE whose name appears as the subject in a certificate, and who asserts that it uses its key and certificate in accordance with this CPS. Subscribers are limited to the following categories of entities:

- Unaffiliated Individuals, including citizens of the United States conducting personal business with a U.S. Government agency at local, state or Federal level
- Employees of businesses acting in the capacity of an employee and conducting business with a U.S. Government agency at local, state or Federal level
- Employees of state and local governments conducting business on behalf of their organization
- Qualified Relying Parties, including: workstations, guards and firewalls, routers, trusted servers (e.g., database, File Transfer Protocol (FTP), and World Wide Web (WWW)), and other infrastructure components communicating securely with, or for, a U.S. Government agency at local, state or Federal level. These components must be under the cognizance of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key.

The ORC CAs are technically a subscriber to the PKI; however, the term subscriber as used in this CPS refers only to those EEs who request certificates for uses other than signing and issuing certificates. Additionally, the ORC Card Management System is technically a subscriber and is responsible for managing smart card token content. The ORC Card Management System is only issued the PIV-I Content Signing certificate and a Connector Certificate and is not issued any certificates that express the PIV-I Hardware or PIV-I Card Authentication policy OID. Review of the certificate profile information contained within this CPS verifies that only the Content Signing Certificate and a Connector Certificate are issued to the ORC Card Management System.

Testing of cards generated by the Card Management System is performed using the PIV Data Model Tester (SP 800-85B Tool). The subsequent report is then reviewed to ensure compliance. If any item(s) results in a “failed” result, updates and configuration changes are made accordingly and a follow-up test is performed. This process is continued until all items return with a “passed” result. A test card for the sponsoring agency/organization is then generated and provided to the agency/organization for submittal to GSA for testing. The facial image capture process is tested using “facial mage test tool v1.0.1.” All equipment used for PIV card issuance adhere to FIPS 201 and are products from the Approved Products List (APL).

1.3.5 Affiliated Organizations

Subscriber certificates may be issued in conjunction with an organization that has a relationship with the subscriber; this is termed affiliation. The organizational affiliation will be indicated in the certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

For Affiliated certificates, the subscriber must show Proof of Organizational Affiliation. A photo ID badge issued by the Affiliated Organization that shows the subscriber’s company affiliation is an acceptable means of Proof of Organizational Affiliation. If the subscriber does not have a badge that demonstrates company affiliation, then the subscriber will need to submit a letter on the Affiliated Organization’s company letterhead, signed by a Duly Authorized Company Representative, stating that the subscriber is either an employee of that organization or an authorized contractor affiliated with the Affiliated Organization.

The Proof of Organizational Affiliation Letter does not take the place of a second photo ID, which is required at the time of in-person validation. The subscriber must still submit 2 photo IDs if they are using the Proof of Organizational Affiliation Letter. The Organizational Affiliation letter is retained by the Registration Authority at the time of registration.

1.3.6 Relying Parties

Relying parties are those persons and entities authorized to accept and rely upon ORC NFI Certificates for purposes of verifying digital signatures. A Relying Party is an individual or organization that, by using another’s certificate can:

- Verify the integrity of a digitally signed message.
- Identify the creator of a message, or establish confidential communications with the holder of the certificate.

- Rely on the validity of the binding of the subscriber's name to a public key.

Under the NFI program relying parties are those eligible organizations and entities that enter into an agreement with ORC and/or GSA to accept NFI Certificates and agree to be bound by the terms of the ORC NFI CP and this CPS.

Other eligible federal agencies and entities under the FPCPF include all Federal agencies, authorized federal contractors, agency-sponsored universities and laboratories, other organizations, and, if authorized by law, state, local, and tribal governments.

At one's own risk, a Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.7 Other Participants

1.3.7.1Certificate Management Authority (CMA)

ORC is responsible for the functions of manufacturing, issuance, suspension, and revocation of ORC NFI certificates.

The ORC NFI CA, RAs and LRAs are considered "Certificate Management Authorities" (CMAs). The term CMA refers to a function assigned to either CAs or RAs, or to both CAs and RAs.

Certificate Status Authorities (CSAs) such as Online Certificate State Protocol (OCSP) Responders operated by ORC are also considered CMAs. ORC will operate an OCSP Responder is support of ORC NFI.

ORC is responsible for ensuring that all ORC NFI CMAs (i.e., the CA, CSAs, RAs, and LRAs) are in compliance with this CPS and the NFI CP.

ORC may subcontract CMA functions to third party CMAs who agrees to be bound by the NFI CP and this CPS, provided that ORC approves such subcontractor in advance. However, ORC remains responsible for the performance of those services in accordance with the NFI CP, this CPS and any applicable NFI MOA.

1.3.7.2Repositories

ORC performs the role and functions of the repository under the ORC NFI Program.

ORC maintains a publicly accessible repository that is available to subscribers and relying parties that contains:

- A listing of all current signature and encryption certificates signed by the ORC NFI CAs
- Current, complete, and accurate CRLs
- ORC NFI certificates for signing keys
- ORC NFI certificates for CRL signing keys
- A copy or link to the current NFI CP
- A summary of this approved CPS
- Any additional policy, waiver, or practice information that is supplemental to the NFI CP or this CPS

The repository is located at http://www.orc.com/NFI.

ORC maintains a master directory accessible through an LDAP interface. This directory is protected by a firewall and is accessible through the Internet. Information in NFI repositories is protected in accordance with the Privacy Act of 1974 as set forth in ORC's Privacy Policy and Procedures documents.

Updating the repository is restricted only to authorized individuals using certificate authenticated access control over SSL. The directory is configured by the CAA to recognize ORC IAs and CAAs as authorized to make changes. ORC protects any and all repository information not intended for public dissemination or modification.

The directory is located at:

ldap://orc-ds.orc.com.

The CRLs are located at:

ldap://orc-ds.orc.com/ cn=<CA Name>, o=ORC PKI, c=US?certificateRevocationList;binary
http://crl-server.orc.com/CRLs/<CA Name>.crl

The ORC CA signing certificates are located at:

ldap://orc-ds.orc.com/ cn=<CA Name>, o= ORC PKI, c=US?cACertificate;binary,crossCertificatePair;binary

http://crl-server.orc.com/caCerts/<CA Name>.p7c

The ORC Root Certificates are located at:

ldap://orc-ds.orc.com/ cn=<ORC Root2>, o= ORC PKI, c=US?cACertificate;binary,crossCertificatePair;binary

http://crl-server.orc.com/caCerts/<ORC Root2>.p7c

A link to the FPCPF Trust Anchor is located at:

http://www.orc.com/FICC

1.3.7.3Organization Applications

ORC is authorized to issue NFI certificates to Applications running servers for various purposes as described below.

1.3.7.3.1 Organization Application Secure Sockets Layer (SSL) Server Certificates

Authorized ORC NFI CAs may issue Application SSL Server Certificates for use on Servers to allow mutual authentication and/or trusted SSL communications with customers. These certificates are issued to the Server where the common name is the registered Domain Name of the Web server. Certificates will allow for both server and client authentication through the extended KeyUsage extension.

1.3.7.3.2 Organization Application (Signing)

Authorized ORC NFI CAs may issue signing-only certificates to Applications for the purpose of providing customers with signed return receipt notifications acknowledging that the Application received the customer’s transaction. Additionally, an Application may utilize a signing certificates to sign internal data (customer transactions, application log files, or agency archive data) where required by specific agency policies.

1.3.7.3.3 Organization Application (Encryption)

Authorized ORC NFI CAs may issue a data encryption certificate to an Application for the purposes of encrypting Application sensitive data where required by specific agency policies.

1.3.7.3.4 Organization Application (Other)

. Authorized ORC NFI CAs may issue other certificate types as needed by an application, which include, but are not limited to, the following:

- Virtual Private Network (VPN) IPSec certificates
- Device certificates
- Code signing certificates
- Validation/ OCSP responder certificates

If new OIDs are required, the Policy Authority assigns new OIDs to certificates as needed, and maintains control over the numbering sequence of OIDs. Authorized ORC NFI CAs requiring new OIDs will submit a request to the Policy Authority.

1.3.7.4 Issuing Authority (IA)

An Issuing Authority (IA) is a role specific to ORC’s operations. However, in some cases such a role is referred to as an Officer. IAs, at the discretion of the

CAA, can assume the responsibility of issuing and revoking certificates. IA responsibilities include:

- Issuing certificates that have been properly validated (including CAA approval as applicable)
- Revoking certificates with properly validated revocation requests
- Validating the credentials of RAs
- RA Training
- Posting certificates

IA's are provided training in the policies and processes of this CPS prior to being issued their IA certificates. IA certificates are valid for performing administrative tasks on the CA and IA equipment, including issuing or revoking certificates.

Upon designation by an ORC CAA, the designated RA(s) receive training covering:

Obligations of being an Issuing Authority
Roles
Management of issuing from the CA
Implementation of CPS guidelines
Issuance of certificates
Coordination with Trusted Agents
Duties as part of compliance audits
Technical & Help Desk support
Components
Certificate Authority
Issuing Authority
Registration Authority
Trusted Agent
Training
Help Desk
Functional Tasks
Workstation set-up
Password Requirements
Issuance Procedures
Revocation Procedures
Cancellation Procedures
Certificate Issuance Notification
Certificate Renewal Notification
Certificate Re-issuance Procedures
Security Awareness

At the completion of training, the designated IA(s) signs an Appointment Letter attesting to the responsibilities incumbent upon the role of IA. The Appointment Letter is then signed by either the ORC Chief Operating Officer or the ORC Chief Executive Officer.

Following completion of the Appointment process, the IA(s) is issued Medium Hardware certificates on a Hardware token to be used for IA functions. The IA(s) may then proceed with performing the duties of an IA.

1.3.7.5Local Registration Authorities (LRAs)

ORC RAs may delegate the identity proofing tasks to LRAs. LRAs can be ORC employees on location at a subscriber's organization or employees of a subscriber's organization. LRAs perform duties identical to RAs, but have their identity validated by RAs instead of a CAA or IA. Upon performing their duties, LRAs provide verification to RAs via mail (for non-FPCPF certificates only) or signed email (using a medium hardware assurance certificate). If an RA delegates duties to one or more LRAs, the RA informs the CAAs. LRAs may not designate other LRAs. RA certificates are not valid for performing administrative tasks on the CA or IA equipment, including issuing or revoking certificates.

ORC uses the term "Local Registration Authority" synonymously with the term "trusted agent". LRAs are obligated to accurately represent the information prepared for the RA. LRAs may not designate other LRAs under this CPS. LRAs under this CPS are not authorized to assume any other CA administration functions.

Notaries Public, as a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions, are also considered a trusted agent under this CPS.

When validating subscriber requests for certificates issued under this CPS, an LRA accepts the following obligations:

- To validate that the named subscriber actually requested the certificate
- To use the LRA certificate only for purposes associated with the LRA function
- To request revocation and verify reissue requirements of a subscriber's certificate upon notification of changes to information contained in the certificate
- To request revocation of the certificates of subscribers found to have acted in a manner counter to subscriber obligations
- To inform subscribers and an RA of any changes in LRA status
- To protect the LRA certificate private keys from unauthorized access

- To immediately request revocation of the LRA certificate and report to the RA if private key compromise is suspected
- To ensure that obligations are imposed on subscribers in accordance with Section 2.1.5
- To inform subscribers of the consequences of not complying with those obligations

An LRA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of LRA responsibilities.

In certain instances, ORC may identify one of the above officials to act in the role of compliance auditor and/or attribute authority. An official performing registration functions cannot audit the registration process and vice versa. The subscriber is required to submit the notarized form and copies of the information used to establish identity via certified mail to an IA.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

This section contains definitions for two levels of assurance, and guidance for certificate usage in their application. Emphasis is placed on two types of activity: integrity and access control to information considered sensitive, and information related to electronic financial transactions and other e-commerce. The final selection of the security mechanisms, and level of strength and assurance, requires a risk management process that addresses the specific mission and environment. Each Relying Party is responsible for carrying out this risk analysis.

1.4.1.1Medium Assurance (Software Certificate)

This level is intended for applications handling sensitive medium value information based on the relying party’s assessment, which may include:

- Non-repudiation for small and medium value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications
- Authorization of payment for small and medium value financial transactions
- Authorization of payment for small and medium value travel claims
- Authorization of payment for small and medium value payroll
- Acceptance of payment for small and medium value financial transactions

1.4.1.2Medium Hardware Assurance:

Medium Hardware Assurance certificate are issued to subscribers on hardware tokens (e.g. PIV-interoperable).

This level is intended for all applications operating in environments appropriate for medium assurance but which require a higher degree of assurance and technical non-repudiation based on the relying party’s assessment.

- All applications appropriate for medium assurance certificates
- Mobile code signing
- Applications performing contracting and contract modifications

1.4.1.3PIV-I Hardware Assurance:

PIV-I Hardware Assurance certificate are issued to subscribers on hardware tokens.

This level is intended for all applications operating in environments appropriate for medium assurance but which require a higher degree of assurance and technical non-repudiation based on the relying party’s assessment.

- All applications appropriate for PIV-I assurance certificates
- Mobile code signing
- Applications performing contracting and contract modifications

1.4.1.4PIV-I Card Authentication Assurance:

PIV-I Card Authentication certificates are issued to subscribers on hardware tokens.

This level is intended for authentication to physical access systems only and is not exportable. Private/secret key operations may be performed using this key with or without explicit user action (e.g., a PIN is not required to be supplied). PIV-I Card Authentication certificate must specify the policy id-CommonAuth.

1.4.1.5PIV-I Content Signing Assurance:

PIV-I Content Signing certificates are used to verify signatures on PIV CHUIDs and PIV biometrics.

1.4.1.6NFI Device Assurance:

NFI Device Assurance is used for authentication between computing and communications components (web servers, routers, firewalls, etc.). In such cases, the component must have a human PKI Sponsor.

1.4.2 Prohibited Certificate Uses

This CPS prohibits the use of any application that does not follow approved standards for the storage and transmittal of cryptographic information. Applicable standards include:

- FIPS 140-2, Security Requirements for Cryptographic Modules;
- FIPS 180-12, Secure Hash Algorithm;
- FIPS 186-21, Digital Signature Standard
- PKCS #11 Hardware Format; and
- PKCS #12 Software Format.
- X.509 v23 Information Technology – ASN.1 Encoding Rules 1994
- ANSI X9.31 American National Standard for Digital Signature using Reversible Public Key Cryptography for the Financial Service Industry

Certificates that assert PIV-I-cardAuth are only to be used to authenticate the hardware token containing the associated private key and are not to be interpreted as authenticating the presenter or holder of the token.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Board of Directors of Operational Research Consultants, Inc., administers ORC PKI organization. The ORC PKI Project Director is responsible for registration, maintenance, and interpretation of this CPS. PKI Project Director, 11250 Waples Mill, South Tower, Ste 210, Fairfax, VA 22030.

1.5.2 Contact Person

Questions regarding this CPS are directed to the contact ORC using the ORC NFI Help Desk request from, found at:

http://www.orc.com/NFI/help.html

1.5.3 Person Determining CPS Suitability for the NFI Policy

The ORC Board has determined the suitability of this CPS as part of the evaluation process. Any changes to this CPS made after determination of suitability will be transmitted to the ORC Board for approval prior to incorporation.

The ORC Board is responsible for ensuring that this CPS conforms to the NFI CP and NFI MOAs.

The ORC Board approves the CPS for each CA that issues certificates under the ORC NFI CP.

1.5.4 CPS Approval Procedures

ORC NFI CAs issuing certificates under the ORC NFI CP are required to meet all facets of the policy. Waivers will not be issued.

The ORC Board makes the determination that this CPS complies with the policy. The CA and RA must meet all requirements of an approved CPS before commencing operations. In some cases, the ORC Board may require the additional approval of an authorized organization or agency. The ORC Board will make this determination based on the nature of the system function, the type of communications, or the operating environment.

In each case, the determination of suitability will be based on an independent compliance auditor’s results and recommendations.

1.6 Definitions and Acronyms

See sections 11 and 12.

2 Publication and Repository Responsibilities

ORC maintains a master directory accessible through an LDAP interface. This directory is protected by a firewall and is accessible through the Internet. Information in NFI repositories is protected in accordance with the Privacy Act of 1974 as set forth in ORC’s Privacy Policy and Procedures documents. See Section 2.8.1.1.

Updating the repository is restricted only to authorized individuals using certificate authenticated access control over SSL. The directory is configured by the CAA to recognize ORC IAs and CAAs as authorized to make changes. ORC protects any and all repository information not intended for public dissemination or modification.

The directory is located at:

ldap://orc-ds.orc.com.

The CRLs are located at:

ldap://orc-ds.orc.com/ cn=<CA Name>, o=ORC PKI, c=US?certificateRevocationList;binary

http://crl-server.orc.com/CRLs/<CA Name>.crl

The ORC CA signing certificates are located at:

ldap://orc-ds.orc.com/ cn=<CA Name>, o= ORC PKI,
c=US?cACertificate;binary,crossCertificatePair;binary

http://crl-server.orc.com/caCerts/<CA Name>.p7c

The ORC Root Certificate is located at:

ldap://orc-ds.orc.com/ cn=<ORC Root2>, o= ORC PKI,
c=US?cACertificate;binary,crossCertificatePair;binary

http://crl-server.orc.com/caCerts/<ORC Root2>.p7c

A link to the FPCPF Trust Anchor is located at:

http://orc.com/FICC

2.1 Repositories

The ORC Repository is responsible for:

- Maintaining a secure system for storing and retrieving Certificates.
- Maintaining a current copy of this CPS.
- Maintaining other information relevant to Certificates.
- Providing information regarding the status of Certificates as valid or invalid that can be determined by a Qualified Relying Party.

ORC posts certificates and CRL information in an LDAP enabled directory established by the ORC NFI PKI. Only information contained in the certificate(s) is posted in this directory to ensure compliance with the Privacy Act. Access is available via an interoperable implementation of an LDAP directory, providing anonymous read/bind access, with certificate storage accomplished for sub-trees identified by organization, "o=". Access to the directory is also available via HTTPS, via a directory gateway interface. The ORC directory sub-trees identify the organization of the EE. The ORC directory gateway is located at:

https://orc.com/NFI/dsgw/bin/csearch?context=dsgw

ORC also posts CRLs at the following locations, accessible via HTTP:

http://crl-server.orc.com/CRLs/<CA Name>.crl

LDAP and HTTP access is defined in the CRL Distribution Point field of end entity certificates.

The certificate repository meets the following obligations:

To list all un-expired certificates for the ORC CAs to relying parties

- To contain an accurate and current CRL for the respective CAs for use by relying parties
- To be publicly accessible
- To be physically accessible, via certificate-authenticated access control over SSL, for authorized requests coordinated with the ORCs Point of Contact (PoC) during normal business hours for the operating organization
- To be maintained in accordance with the practices specified in this CPS
- To meet or exceed the requirement of 99% availability for all components within the control of the operating organization

Communication failures as a result of Internet problems external to the operating organization will not count against this availability requirement.

ORC maintains a copy of at least all certificates and CRLs ORC issues and provides this information for archiving. ORC provides this information on a certificate accessed web server posted no later than 10 days after the end of the collection of the data.

2.1.1 Repository Obligations

ORC maintains a repository for the ORC NFI PKI, which affords secure access for retrieving currently valid ORC NFI certificates, a copy of the ORC NFI CP, and other relevant ORC NFI information. Access is controlled through digital certificate authentication, and firewall protection.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

ORC maintains a publicly accessible repository that is available to subscribers and relying parties that contains:

- A listing of all current signature and encryption certificates signed by the ORC NFI CAs
- Current, complete, and accurate CRLs
- ORC NFI certificates for signing keys
- ORC NFI certificates for CRL signing keys
- A copy or link to the current NFI CP
- A summary of this approved CPS

- Any additional policy, waiver, or practice information that is supplemental to the NFI CP or this CPS

The repository is located at http://www.orc.com/NFI

All information published in the Repository is published immediately after such information is available to the Authorized ORC NFI CA. The Authorized ORC NFI CA will publish certificates immediately upon acceptance of such certificates. At a minimum, the ORC NFI repositories contain all CA certificates issued by or to the ORC NFI PKI and CRLs issued by the ORC NFI PKI.

Authorized ORC NFI CA certificates, CRLs, and online certificate status information are available for retrieval 24 hours a day, seven days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually, excluding network outages.

2.2.2 Publication of CA Information

The ORC NFI Certificate Policy document is publicly available on the ORC NFI website (see http://www.orc.com/NFI). The ORC NFI CPS for the ORC NFI CA will not be published; a redacted version of this CPS will be publicly available from the ORC NFI website (see http://www.orc.com/NFI/policies.html). Additional information related to Authorized ORC NFI CAs is also available at the respective Authorized ORC NFI website.

2.2.3 Interoperability

Certificates and CRLs issued under this CPS are published in directories, using standards-based schemas for directory objects and attributes, as specified and in compliance with the Shared Service Provider Repository Service Requirements [SSP-REP]. ORC ensures that all Authorized ORC NFI CAs are interoperable with each other, and with the FBCA repository.

2.3 Frequency of Publication

Certificates are published to a repository at the time of issuance and remain accessible from the repository following subscriber acceptance. CRL publication is in accordance with Section 4.9. Frequency of CRL publication is in accordance with Section 4.9.7.

2.4 Access Controls on Repositories

There are no access controls on the reading of the CPS summary, any supplemental policy information, or any supplemental practice information published by ORC. Certificate and CRL information are publicly available.

Access to NFI Certificates and NFI Certificate status information is in accordance with provisions of the ORC NFI MOA. Access controls include:

- Access to ORC Electronic Resources are be controlled by job requirements and authentication, as stipulated in this CPS.
- ORC employees are only able to access those resources that they require to accomplish the tasks they are assigned, as stipulated in this CPS (access rights are assigned by resource (server, computer, share, volume, printer, etc.)).
- User authentication is via certificate authentication (or UserID and password when appropriate) and data encryption is used, as stipulated in this CPS.
- ORC employees are assigned access rights before accessing any electronic resources.
- The ORC Corporate Security Auditor determines and periodically reviews user access rights.

The CAA and SA are notified of any changes that affect employee access rights.

These policies are elaborated upon in the ORC Systems Security Plan (SSP).

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

All certificates issued by the ORC under this CPS use the Distinguished Name (DN) format for subject and issuer name fields. In the case of individual certificates, ORC assigns an X.501 distinguished name specifying a geo-political name. In the case of component/ device certificates, ORC assigns a geo-political name.

DNs consist of a combination of a Common Name (CN) and a Relative Distinguished Name (RDN). CNs are either full names for individuals, Uniform Resource Locators (URLs) or Internet Protocol (IP) addresses for servers or name of the code signer’s organization for code signing certificates.

All CA and RA certificates cross-certified with the Federal Bridge will include a non-NULL subject DN. All certificates issued to end entities, except those issued at the Rudimentary level of assurance, will include a non-NULL subject DN. The ORC IA will ensure by visual inspection on the CA server that the certificates will be issued with a non-null subject DN prior to issuance.

The table below summarizes the naming requirements that apply to each applicable level of assurance.

Basic	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
Medium	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
PIV-I Card Authentication	Non-Null Subject Name, and Subject Alternative Name For PIV-I Card Authentication subscriber certificates, use of the subscriber common name is prohibited. PIV-I Card Authentication certificates shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms: For certificates with an Affiliated Organization: serialNumber=UUID, ou=Affiliated Organization Name,{Base DN} For certificates with no Affiliated Organization: serialNumber=UUID, ou=Unaffiliated, ou=Entity CA's Name,{Base DN} The UUID shall be encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

ORC NFI Medium Hardware and PIV-I Hardware certificates indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

cn=Subscriber's full name, ou=Affiliated Organization Name,{Base DN}

For certificates with no Affiliated Organization:

cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name,{Base DN}

PIV-I Content Signing certificates clearly indicate the organization administering the CMS.

For PIV-I Card Authentication subscriber certificates, use of the subscriber common name is prohibited.

PIV-I Card Authentication certificates indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

serialNumber=UUID, ou=Affiliated Organization Name,{Base DN}

For certificates with no Affiliated Organization:

serialNumber=UUID, ou=Unaffiliated, ou=Entity CA's Name,{Base DN}

The UUID shall be encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

{Base DN} is defined as: 'o=ORC PKI, c=US'.

3.1.2 Need for Names to be Meaningful

Names used in the certificates issued by an Authorized ORC NFI CA identify the person or object to which they are assigned in a meaningful way, as provided in the table below.

Certificate Description	Name Meanings
Authorized ORC NFI CA Digital Signature Certificates	Authorized ORC NFI CAs shall implement the name constraint extension of the X.509 version 3, certificate profile in issuing CA certificates.
Digital Signature and Encryption Certificates	The authenticated common name should be the combination of first name, middle name and/or initial, and surname and reflect the legal name of the organization and/or unit.
Device Certificates	The common name should be the authenticated registered domain name of the Application server.
Validation Signing Certificates	The authenticated common name should be the combination of the name of the device and reflect the legal name of the organization and/or unit.
FBCA Cross-Certificates	Authorized ORC NFI CAs shall implement the name constraint extension of the X.509 version 3 certificate profile in issuing cross certificates.

Common Names are meaningful as individual names, as actual server Uniform Resource Locators (URLs) or Internet Protocol (IP) addresses or as code signing organizational names. Names identify the person or object to which they are assigned. ORC ensures that an affiliation exists between the subscriber and any organization that is identified by any component of any name in its certificate.

The common name used represents the subscriber in a way that is easily understandable for humans. For people, this is typically a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

ORC CAs asserting this policy only sign certificates with subject names from within a name-space approved by the GSA NFI Program Manager.

In the case of all Digital Signature and Encryption Certificates asserting FPCPF OIDs issued to federal employees:

CN = Nickname Smith; or
CN = John J Smith; or
CN = John Jay Smith

In the case of all Digital Signature and Encryption Certificates asserting FPCPF OIDs issued to federal contractors and other affiliates designated by a sponsoring agency:

CN = Nickname Smith (affiliate); or
CN = John J Smith (affiliate); or
CN = John Jay Smith (affiliate)

3.1.3 Anonymity or Pseudonymity of Subscribers

ORC NFI does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable certificate profile (see Section 7.1.4), The ORC NFI certificate profiles are established by the ORC NFI Policy Authority and conform to the CCP-PROF. The ORC NFI PIV-I certificate profiles are established by the ORC NFI Policy Authority and conform to the PIV-I-PROF. The NFI Program Management Office is responsible for CA name space control.

Rules for interpreting the pivFASC-N name type are specified in [SP 800-73].

3.1.5 Uniqueness of Names

ORC complies with uniqueness of names; including X.500 DNs. ORC enforces name uniqueness, as described in Sections 3.1.1 and 3.1.2.

ORC ensures the following for subscriber names:

The name contains the subscriber identity and organization affiliation (if applicable) that is meaningful to humans

The naming convention is described in this CPS (Section 3.1.1)

ORC complies with the Policy Authority for the naming convention.

This does not prevent devices from sharing a Fully Qualified Domain Name (FQDN) as CN.

3.1.6 Recognition, Authentication, and Role of Trademarks

A corporate entity is not guaranteed that its Common Name will contain a trademark if requested. ORC will not issue that name to the rightful owner if it has already issued one sufficient for identification.

The use of trademarks in a name form or as any part of a name form is discouraged. Trademarks will not be used as a name form or as a part of the name form for certificates issued to government employees unless U.S. Government personnel hold them or devices have a legitimate right to their use. The holder of the trademark will only use trademarks in certificates issued to contractors, contractor-owned servers, foreign nationals, or organizations with specific permission.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the subscriber generates key pairs, the subscriber is required to prove, to an ORC NFI CA, possession of the private key that corresponds to the public key in the certificate request. Subscribers are required to use a FIPS 140-2 validated cryptographic module for generation of keys. In the case of a Level 1 cryptographic module, the ORC NFI CAs perform a browser check prior to registration to ensure compliance against a list of FIPS 140-2 Level 1 browsers and upon submitting a registration request. ORC NFI CAs only allows compliant key pair generation. In the case of Level 2 tokens, required for medium hardware assurance certificates, key pair generation is accomplished with a Level 2-compliant token in the presence of an ORC RA or LRA, or other specifically assigned authority.

FPCPF PIV certificates are issued on a PIV card via a FIPS-201 approved Card Management System (CMS), refer to FIPS 201 Evaluation Program Approved Product List (http://fips201ep.cio.gov/apl.php).

The subscriber is in possession and control of the private key from time of generation or benign transfer. The ORC NFI CAs authenticate the subscriber with a Proof of Possession (POP) test when requesting and retrieving a certificate by requiring the subscriber to perform a private key operation and verifying that the public key presented by the subscriber matches the private key. ORC supports multiple enrollment protocols which support POP including:

- KEYGEN/SPAC, CRMF/CMMF, PKCS #10 and CMC.

To affect POP the CA supplies a random challenge string to the browser as part of the KEYGEN tag. The public key generated by the browser and the challenge string supplied by the CA are DER (Distinguished Encoding Rules) encoded together, and the resulting PublicKeyAndChallenge value is then digitally signed with the private key to produce a SignedPublicKeyAndChallenge value. This signed value is then base 64 encoded and sent to the CA as part of the certificate request; the CA verifies the signature using the included public key, thus proving possession by the browser of the private key corresponding to that public key.

The public key and challenge strings are DER encoded as PublicKeyAndChallenge and then digitally signed with the private key to produce a SignedPublicKeyAndChallenge. The SignedPublicKeyAndChallenge is base64 encoded, and the ASCII data is finally submitted to the server as the value of a name-value pair, where the name is specified by the NAME attribute of the KEYGEN tag. When retrieving the completed certificate the browser also checks before importing the certificate into its database, to verify that the public key in the certificate being installed matches the private key it originally generated.

An additional out-of-band check is performed by requiring the requestor to print the base 64 of the DER encoded certificate request and present it in person during the validation process. The RA validates both the person’s identity and their possession of a certificate request corresponding to their private key.

In all cases, IAs may request additional information or verification from an RA or LRA if deemed necessary by the IA to confirm the requestor’s identity.

3.2.2 Authentication of Sponsoring Organization Identity

If the applicant is requesting a Business Representative, Federal Employee or State Employee NFI Certificate, in addition to verifying the applicant’s authorization to represent the Sponsoring Organization, ORC verifies the Sponsoring Organization's current operating status and that said organization conducts business at the address listed in the NFI Certificate application. ORC provides validation of information concerning the Sponsoring Organization, such as legal company name, type of entity, year of formation, names of directors and officers, address (number and street, city, ZIP code), and telephone number. All applicants are notified, on the website application process, that the process is secure. ORC will verify the operating status of the organization through publicly available database/websites, such as the Central Contractor Registry (CCR), Dunn and Bradstreet, corporate and government websites.

Users will provide proof of their relationship to the company/organization they work for. This proof can be accomplished by:

Applicant requesting a certificate accompanied by a U.S. Government sponsor

Applicant presenting a government-issued photo ID badge including the applicants company affiliation

Applicant providing a signed letter on company or agency letterhead from an authorized organization official attesting to the relationship (this is the only method approved for server certificate requests and code signing certificate requests)

Applicant presenting an un-expired photo ID badge issued by the organization

In all cases, in order to issue a certificate asserting a FPCPF OID, the applicant will obtain, from an authorized organization official, approval to hold a FPCPF certificate, as stipulated in Section 3.1.9.7, below.

3.2.3 Authentication of Individual Identity

ORC allows a certificate to be issued only to a single entity. Certificates are not issued that contain a public key whose associated private key is shared.

3.2.3.1Authentication of Human Subscribers

Verification of an applicant’s identity will be performed prior to certificate issuance. All applicants for medium assurance and medium hardware assurance certificates are required to appear in person before an RA, an LRA, for identity authentication. Applicants for medium assurance and medium hardware assurance certificates are required to present either one Federal Government-issued Picture I.D., or two ID’s, one of which shall be a non-Federal Government photo ID (e.g., a Drivers License), and the second of which shall be Government issued ID or a verifiable membership-type ID and the applicant form generated during the certificate request process containing the public key.

Minors and others not competent to perform face-to-face registration alone are not supported under this CPS.

The RA or LRA will archive a copy of all information used in the verification process. In all cases, the RA or LRA will submit a digitally signed e-mail message to an ORC IA, including the public key, attesting that the identity of the individual has been authenticated.

In all cases, ORC records the following information:

- The Identity of the person performing the validation process
- Applicant's name as it appears in the certificate Common Name field
- A signed declaration by the identity-verifying agent that they verified the identity of the applicant
- Method of application (i.e., online, in-person)
- The method used to authenticate the applicant's identity, including identification type and unique number or alphanumeric identifier on the ID
- The date of verification
- A handwritten signature by the applicant in the presence of the person performing the identity verification
- For each data element accepted for proofing, including electronic forms:
- Name of document presented for identity proofing
- For PIV-I certificates the identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification.
- Issuing authority
- Date of issuance
- Date of expiration

All fields verified

- Source of verification (i.e., which databases used for cross-checks)
- Method of verification (i.e., online, in-person)
- Date/time of verification
- The ORC NFI name, including subcontractors, if any
- All associated error messages and codes
- Date/time of process completion
- Names (IDs) of ORC PKI processes, including subcontractors' processes, if any.

Alternately, certificate requests may be validated and authenticated on the basis of electronically authenticated subscriber requests using a current, valid PKI signature certificate issued by an ORC NFI CA and associated private key. The following restrictions apply:

- The assurance level of the new certificate will be the same or lower than the certificate used as the authentication credential.
- The DN of the new certificate will be identical to the DN of the certificate used as the authentication credential.
- Information in the new certificate that could be used for authorization will be identical to that of the certificate used as the authentication credential.
- The expiration date of the new certificate will be no later than the next required in-person authentication date associated with the certificate used as the authentication credential.
- The validity period of the new certificate will not be greater than the maximum validity period requirements of the NFI CP for that particular type of certificate.
- The in-person authentication date associated with the new certificate will be no later than the in-person authentication date associated with the certificate used for authentication.

In all cases, ORC may request additional information or verification if deemed necessary to confirm the requestor's identity.

3.2.3.1.1 Authentication of Unaffiliated Individual NFI Digital Signature and Encryption Certificates

Unaffiliated Individuals are required to appear in person before an ORC RA, an LRA, or a Notary Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions) for identity authentication. ORC verifies all of the following identification information supplied by the applicant: first name, middle initial, and last name, date of birth, current address (number and street, city, ZIP code), and telephone number.

An exception to the above is provided to the Government when the Government provides identity proofing. Any exception is the subject of an approved Registration Practice Statement.

3.2.3.1.2 Authentication of NFI Business Representative Digital Signature and Encryption Certificates

Verification of an applicant's identity for an NFI Business Representative Digital Signature or Encryption Certificate is performed prior to certificate issuance.

Applicants are required to appear in person before an RA, an LRA, or a Notary Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions) for identity authentication.

The ORC NFI RA, LRA or Trusted Agent verify:

- That the applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association, in good standing.
- The Sponsoring Organization’s identity as specified in Section 3.1.8.
- The process documentation and authentication requirements will include the following:
- Identity of the person performing the identification
- A signed declaration by that person that he or she verified the identity of the subscriber as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy
- A unique identifying number from the ID of the verifier and from the ID of the applicant
- The date and time of the verification
- A declaration of identity signed by the applicant, using a handwritten signature, performed in the presence of the person performing the identity authentication.

3.2.3.1.3 Authentication of NFI Organization (Relying Party Applications) Digital Signature and Encryption Certificates

If the applicant is requesting an ORC NFI Organization (Relying Party Applications) Digital Signature or Encryption Certificate, ORC verifies:

- that the applicant is authorized to act on behalf of the Relying Party
- the affiliation of the NFI Certificate applicant with the Relying Party that the applicant’s organization has completed a Relying Party Agreement with ORC

3.2.3.1.4 Authentication of Component Identity Certificates (e.g. Agency/Organization Application SSL Server or VPN IPSec Certificates)

Some computing and communications components (web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor as described in Section 5.2.1.2.4.

The PKI Sponsor is responsible for providing the ORC NFI approved IA's, through an application form, correct information regarding:

- Registered domain name or IP address
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)

Contact information to enable the CA or RA to communicate with the sponsor when required. An ORC NFI IA will authenticate the validity of any authorizations to be asserted in the certificate, and will verify source and integrity of the data collected to an assurance level commensurate with the certificate level being requested. Authentication and integrity checking is accomplished by one of the following methods:

- Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested). Only ORC Issued NFI certificates may be used in digitally signed messages requesting certificate issuance. The ORC IA will examine the certificate that signed the message and verify the issuer and subscriber in the certificate and that the certificate has not been revoked.
- In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.1.9.

3.2.3.1.5 Qualified Relying Party NFI Certificates

If the applicant is requesting a Qualified Relying Party NFI Certificate, ORC verifies:

- That the applicant is authorized to act on behalf of the Qualified Relying Party.
- The affiliation of the NFI Certificate applicant with the Qualified Relying Party, or an Organization Application.

3.2.3.2Authentication of Devices

3.2.3.2.1 Code-signer Authentication

Code signing certificates are issued to individuals on behalf of the CSAA sponsoring organization. Each sponsoring organization is required to send a signed letter on organizational/agency letterhead to ORC authorizing CSAA(s). The CAA maintains a log of these letters, which is available to all RAs for verification purposes. The CSAA is required to send a signed memorandum on organizational/agency letterhead to the RA authorizing the code signer to receive a code-signing certificate. The memorandum could be either a hard copy with ink signature or an electronic copy that is digitally signed. The memorandum specifies, at a minimum, the subject DN to be asserted including the office symbol and an optional number (in order to make the code signing certificate's subject DN unique). The memorandum also contains the DN of the person authorized as the code signer. If digitally signed, the public key certificate used to verify the digital signature is an ORC medium hardware assurance certificate.

After generating a key-pair and submitting a certificate request to an ORC NFI CA, the Code Signer is required to send a digitally signed e-mail to the RA. The e-mail will contain the following information:

- Request number
- Subject DN in the certificate request
- DN of the code signer as it appears in the subject alternate name field

The e-mail will be digitally signed using an approved ORC medium hardware assurance certificate. If the person authorized to become a code signer does not possess the required certificate, the person obtains the credential using the process defined in this CPS, prior to making the code signer request.

The RA performs the following steps:

- Verify that it has received a signed memorandum from the valid attribute authority (i.e., the attribute authority identified in this CPS) for the code signer. This verification includes the verification of digital signature if it received an electronic copy of the memorandum
- Verify the digital signature on the e-mail from the code signer.
- Verify that the e-mail was signed using the acceptable PKI credentials.
- Verify that the subject alternate name DN in the e-mail is same as the DN of the e-mail signer

In all cases, the public key certificate used to verify the digital signature will be an ORC medium hardware assurance certificate. In no cases will the ORC NFI PKI issue a code-signing certificate that asserts any FPCPF OID.

3.2.3.2.2 Authentication of Component Identities

Some computing and communications components (web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor as described in Section 5.2.1.2.4. The PKI Sponsor is responsible for providing the CAA, or approved IAs, through an application form, correct information regarding:

- Equipment identification

- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable ORC to communicate with the PKI sponsor when required

An ORC IA authenticates the validity of any authorizations to be asserted in the certificate, and verifies source and integrity of the data collected to an assurance level commensurate with the certificate level being requested. Authentication and integrity checking is accomplished by one of the following methods:

- Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested)
- In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.1.9

3.2.4 Non-verified Subscriber Information

ORC does not included information in certificates that has not been verified.

3.2.5 Validation of Authority

Before issuing certificates that assert organizational authority, ORC validates the individual's authority to act in the name of the organization. This validation is performed by having the applicant complete and submit an "Proof of Organizational Affiliation" letter, made available to applicants on the ORC NFI website. ORC uses Proof of Organizational Affiliation letters for applicants attempting to obtain:

- Component/ Server certificates
- VPN IPsec Component Certificates
- Code Signing Certificates

A specific Proof of Organizational Affiliation letter is provided for each particular type of certificate request.

ORC additionally requires a Proof of Organizational Affiliation for certificate requests from individuals who either do not possess a company issued photo ID badge or organizations which do not issue company photo ID badges, signed by a Duly Authorized Company Representative, stating that they are an employee of that organization.

3.2.6 Criteria for Interoperation

The FPKIPA determines the interoperability criteria for CAs operating under the X.509 U.S. Federal PKI Common Policy Framework (FPCPF) policy. MOA(s) with the FPKIPA and other entities ensure interaction and interoperability with Authorized ORC NFI CAs, authorized State and Local Government agencies, and non-government CAs.

3.3 Identification and Authentication for Re-key and Renewal

3.3.1 Identification and Authentication for Routine Re-key

NFI Certificate re-keying (signing and encryption) is accomplished through the limitation on certificate renewal, as described in Section 3.2. The minimum requirement for all NFI certificate re-keying, with the exception of CA certificates, is once every 9 years from the time of initial registration (i.e., after two 3-year renewals). ORC NFI subscribers must identify themselves for the purpose of re-keying through use of their current signature key, except that identity will be established through initial registration process described in Section 3.2.

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature, Authentication and Encryption Certificates
PIV-I Card Authentication	Identity may be established through use of the current signature key certificate, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.

Subscribers' signature private keys and certificates have a maximum lifetime of three years. Subscriber encryption certificates have a maximum lifetime of three years; use of subscriber decryption private keys is unrestricted.

CA certificate re-key follows the same procedure as is performed for initial CA certificate generation.

3.3.2 Identification and Authentication for Renewal

ORC accepts NFI Certificate renewal requests from their subscribers within 90 days from the scheduled end of the operational period (expiration date) of the NFI Certificate, provided the NFI Certificate is not revoked, suspended, or expired. NFI Certificates are renewed in 3-year increments, no more than 2 times before certificate re-key is required.

To renew a certificate, as described in the NFI CP, the subscriber obtains a new certificate based on an existing key pair. ORC authenticates the subscriber's renewal request using the subscriber's current certificate for authentication in the renewal process. The authentication in the renewal process examines the expiration date of the current certificate and will only allow renewal if within 90 days of expiration but currently valid. In the event that subject information has changed (and/or the key pair is required to be changed for any reason), ORC requires the subscriber to request a new NFI Certificate. The old certificate (as a result of an update action) may or may not be revoked, but is not further re-keyed, renewed, or updated. A certificate that is not renewed by the end of the operation period reflects an expired status.

ORC renews NFI Certificates issued to Relying Parties only after completing successful identity proofing verification.

Server subscribers (PKI Sponsors) are required to revalidate their identity and any equipment authorizations and/or attributes (if any are to be included in the certificate). The subscriber is required to present a currently valid certificate to request a new certificate. End-users are required to renew their certificates through a web-based electronic form.

Medium assurance certificate may be renewed or updated on the basis of electronically authenticated subscriber requests three times. Every eight years, in-person authentication is required.

Medium hardware assurance certificates may be renewed or updated on the basis of electronically authenticated subscriber requests only one time. Every four years, in-person authentication is required.

During the renewal process the user must present his or her current identity certificate during an SSL client authentication to the CA. The CA validates the authenticity of the certificate being presented by verifying that the certificate was issued by the CA in question and mapping the subject name in the certificate to its corresponding certificate in the database. This process verifies that the subscriber is eligible for renewal on the basis of the subscriber's existing certificate, as stipulated above. If the subscriber is not eligible for renewal on the basis of the subscriber's existing certificate, ORC redirects the subscriber to the in-person registration process. The forms to accomplish this process are controlled by access control lists on a secure web server that binds to the corresponding users with certificates in an LDAP directory. Access control to the renewal forms is based on comparing the certificate with the Distinguished Name of the subscriber (based on an X.509 certificate-based authentication) against the certificate with DN in the directory.

Provisions for the renewal of Code signing certificates are in accordance with the Medium Hardware Assurance criteria.

In cases where a subscriber’s organization (including PKI Sponsors or CSAAs) has required authorizations to be included in an ORC NFI certificate, the person responsible for that organization ORC NFI agreement shall notify an ORC NFI RA of the withdrawal of authorizations, via digitally signed e-mail using a medium assurance hardware certificate. The RA verifies the signature of the subscriber’s organization.

3.3.3 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked or expired, the applicant is required to go through the initial registration process as described in Section 3.2.

3.4 Identification and Authentication for Revocation Request

Certificate revocation requests may be made using the same practices as certificate issuance requests. In addition, certificate revocation requests may be made electronically using e-mail digitally signed by a certificate of equal or greater level of assurance than that of the certificate for which the request is made. In either case, the request must include the reason for revocation. See Section 4.9 for details on certificate revocation procedures. Subscribers who are in possession of their private keys may also revoke their own certificates at any time via the ORC NFI website (http://NFI.orc.com).

A subscriber may request revocation of a certificate regardless of whether or not it has been compromised. ORC may revoke a subscriber’s certificate for cause. The RA collects signed documentation stating the reason and circumstances for the revocation. If an RA performs this on behalf of a subscriber, a formal, signed message format known to the ORC IA is employed.

In accordance with the NFI MOA, an NFI Certificate revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the NFI Certificate’s associated key pair. The identity of the person submitting a revocation request in any other manner is authenticated in accordance with Section 4.9 of this CPS. Revocation requests authenticated on the basis of the NFI Certificate’s associated key pair are always accepted as valid. Other revocation request authentication mechanisms for non-FPCPF certificates include a request in writing signed by the subscriber and sent via U.S. Postal Service first-class mail. ORC RAs are verify the authentication mechanism and balances the need to prevent unauthorized revocation requests against the need to quickly revoke certificates. In the case of certificates asserting FPCPF OIDs, ORC will only accept revocation requests from the subscriber or persons authorized by each sponsoring agency to make revocation requests.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

ORC NFI offers the certificate types as described in this CPS. The Certificate application process provides sufficient information to:

- Establish the applicant's authorization (by the employing or sponsoring agency) to obtain a certificate. (per section 3.2.3)
- Establish and record the identity of the applicant. (per section 3.2.3)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required. (per section 3.2.1)
- Verify any role or authorization information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for ORC and the applicant, and that do not defeat security. However, all must be completed before certificate issuance.

4.1.1 Application Initiation

The following parties may initiate the ORC NFI Certificate application process:

Potential Subscriber	Authorized Initiator
Unaffiliated Individual	Potential subscriber only
Business Representative	Sponsoring Organization; or potential subscriber
Qualified Relying Party	Duly authorized representative of the Qualified Relying Party, in good standing
Devices	PKI sponsor responsible for the component receiving the certificate
State/Local Government Employee	Sponsoring Organization; or potential subscriber

The application is available only on the Internet at http://NFI.orc.com. Once the applicant starts the application process, the Internet protocol changes from non-secure to secure using the SSL protocol.

The individual requiring the certificate will make a certificate request. When applicable, the subscriber's organization is required to provide a POC for verification of any roles or authorizations to be included in the subscriber's certificates, via signed letterhead or digitally signed e-mail. The CAAs record all such appointments in a log available to all RAs. This point of contact may be the PKI Sponsor or CSAA. A request is made from a workstation via a web interface. When making the certificate request, the applicant will submit a proposed distinguished name in accordance with local naming conventions, generate the public private key pair using FIPS 140-2 Level 1 approved software or Level 2 hardware tokens, and submit the information and the public key to the CA for disposition.

The applicant will protect the private key with a password. This password will be kept confidential and will not be recorded or given to any other parties except in accordance with locally approved key escrow procedures.

In the case of medium assurance certificates, the applicant will make the request using a web browser incorporating a FIPS 140-2 Level 1 cryptographic module for generating the key pair and submitting the required information through an online form. In the case of medium hardware assurance certificates, the applicant will make the request at the RA workstation using a web browser and a FIPS 140-2 Level 2 token for generating the key pair and submitting the required information through an online form. The following instructions explain the steps necessary for an applicant to apply for a certificate:

- Connect to the ORC NFI web page (http://NFI.orc.com) and follow the directions filling out the electronic and printed forms
- For encryption keys, the application process asks if the subscriber desires to escrow the encryption key and notifies subscriber upon successful completion or failure of key escrow
- Present the printed application and two photo IDs to an RA, LRA, or Notaries Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions)

Upon notification of certificate issuance by e-mail, the certificate is accepted and retrieved.

4.1.1.1Application Form

ORC CAs issues certificates to EEs. ORC CAs do not issue certificates to or cross-certify with external CAs without express permission from the Government.

The individuals requiring certificates may make certificate requests. Requests are made from a workstation via a web interface. When making a certificate request, the applicant completes an NFI Certificate application and provides requested information requested by an online form. The following steps occur during the application process:

- The applicant is presented with the Root CA certificate and requested to trust this CA. The site is be protected by a firewall and incorporates SSL to ensure secure distribution of the certificate and to prevent substitution, as stipulated in Section 5
- The applicant is presented with a screen detailing the subscriber obligations and required to accept these obligations prior to continuing
- The applicant completes the online form which includes his or her name, address, phone number, e-mail address (if available), and identifying information
- The applicant generates a public and private key pair and is required to use a password to protect the private key, as stipulated in the Subscriber Agreement. This password is stored locally and is required to be kept confidential and not be recorded or given to any other parties. An applicant should create passwords in accordance with the relevant passage in Section 6.2.5, “Method of Activating Private Key”
- The applicant submits identifying information and the public key to the CA
- The applicant proves to the CA that the public key forms a functioning key pair with the private key via the proof of possession functionality as described in Section 3.1.7

Upon submission of the completed application form, the applicant is provided with a request number and is required to print the form, and take it, with the appropriate identity credentials, to an authorized RA, LRA, trusted agent or member of the Notary Public to have the identity credentials verified. If the applicant goes in person to an RA, LRA or trusted agent, the application process for the applicant is completed. If the applicant has the forms notarized, the applicant is required to send the notarized form via U.S. postal service to ORC or personally deliver the forms to an ORC facility. This information is provided on the printed form.

In the case of certificates asserting a FPCPF OID, if the sponsoring agency's RPS allows applicants the option to use a notary, the applicant is required to send the notarized form via U.S. postal service Registered Mail in a tamper evident packaging system to a sponsoring agency's designated RA or personally deliver the forms to a sponsoring agency's designated RA, in accordance with the stipulations of the agency RPS.

4.1.1.2CA Certificates

In order to obtain a CA certificate, an authorized representative of the applicant CA must submit the application. The authorized representative must provide ORC with a completed “Proof of Organizational Affiliation” letter, found on the ORC NFI website (NFI.orc.com), in addition to completing all other applicable identification and authentication requirements as stipulated in Section 3.2.

4.1.1.3User Certificates

The individuals requiring certificates will make certificate requests. Requests are made from a workstation via a web interface. When making a certificate request, the applicant will complete an NFI Certificate application and provide requested information requested by an online form. The following steps occur during the application process:

- The applicant is presented with the Root CA certificate and requested to trust this CA. The site is be protected by a firewall and incorporates SSL to ensure secure distribution of the certificate and to prevent substitution, as stipulated in Section 5
- The applicant is presented with a screen detailing the subscriber obligations and required to accept these obligations prior to continuing
- The applicant completes the online form which includes his or her name, address, phone number, e-mail address (if available), and identifying information
- The applicant generates a public and private key pair and is required to use a password to protect the private key, as stipulated in the Subscriber Agreement. This password is stored locally and is required to be kept confidential and not be recorded or given to any other parties. An applicant should create passwords in accordance with the relevant passage in Section 6.2.5, “Method of Activating Private Key”
- The applicant submits identifying information and the public key to the CA
- The applicant proves to the CA that the public key forms a functioning key pair with the private key via the proof of possession functionality as described in Section 3.1.7

Upon submission of the completed application form, the applicant is provided with a request number and is required to print the form, and take it, with the appropriate identity credentials, to an authorized RA, LRA, trusted agent or member of the Notary Public to have the identity credentials verified. If the applicant goes in person to an RA, LRA or trusted agent, the application process for the applicant is completed. If the applicant has the forms notarized, the applicant is required to send the notarized form via U.S. postal service to ORC or personally deliver the forms to an ORC facility. This information is provided on the printed form.

In the case of certificates asserting a FPCPF OID, if the sponsoring agency's RPS allows applicants the option to use a notary, the applicant is required to send the notarized form via U.S. postal service Registered Mail in a tamper evident packaging system to a sponsoring agency's designated RA or personally deliver the forms to a sponsoring agency's designated RA, in accordance with the stipulations of the agency RPS.

In the case of PIV-I Hardware certificates, PIV-I Hardware certificates may only be issued to human subscribers.

4.1.1.4Device Certificates

Some computing and communications components (web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor. The PKI Sponsor is responsible for providing to the CAA, or approved IAs, through an application form, correct information regarding:

- Equipment identification
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable ORC to communicate with the PKI sponsor when required

An ORC IA authenticates the validity of any authorizations to be asserted in the certificate, and verifies source and integrity of the data collected to an assurance level commensurate with the certificate level being requested. Authentication and integrity checking is accomplished by one of the following methods:

- Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested)
- In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.2.3.1

4.1.2 Enrollment Process and Responsibilities

The application is available only on the Internet at http://NFI.orc.com. Once the applicant starts the application process, the Internet protocol changes from non-secure to secure using the SSL protocol.

The individual requiring the certificate must make the certificate request. When applicable, the subscriber’s organization is required to provide a PoC for verification of any roles or authorizations to be included in the subscriber’s certificates, via signed letterhead or digitally signed e-mail. The CAAs record all such appointments in a log available to all RAs. This point of contact may be the PKI Sponsor or CSAA. A request is made from a workstation via a web interface. When making the certificate request, the applicant must submit a proposed distinguished name in accordance with local naming conventions, generate the public private key pair using FIPS 140-2 Level 1 approved software or Level 2 hardware tokens, and submit the information and the public key to the CA for disposition.

The applicant must protect the private key with a password. This password must be kept confidential and is not to be recorded or given to any other parties except in accordance with locally approved key escrow procedures.

In the case of medium assurance certificates, the applicant makes the request using a web browser incorporating a FIPS 140-2 Level 1 cryptographic module for generating the key pair and submitting the required information through an online form. In the case of medium hardware assurance certificates, the applicant must make the request at the RA workstation using a web browser and a FIPS 140-2 Level 2 token for generating the key pair and submitting the required information through an online form. The following instructions explain the steps necessary for an applicant to apply for a certificate:

- Connect to the ORC NFI web page (http://NFI.orc.com) and follow the directions filling out the electronic and printed forms
- For encryption keys, the application process asks if the subscriber desires to escrow the encryption key and notifies subscriber upon successful completion or failure of key escrow
- Present the printed application and two photo IDs to an RA, LRA, or Notaries Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions)

Upon notification of certificate issuance by e-mail, the certificate is accepted and retrieved.

4.1.2.1Application Education and Disclosure

ORC notifies applicants prior to issuance, by way of the ORC NFI website, documentation made available via the ORC NFI website, and the application forms, of the advantages and potential risks associated with using NFI Certificates to access Relying Parties electronically. Through those same means, ORC provides information to Subscribers regarding the use of private keys and digital signatures or encrypted messages created with such keys, and the Subscriber’s obligations.   ORC NFI Certificates are intended for use by subscribers to transact business with the Federal Government. Non-Federal Government participants who would otherwise be involved in such transactions provided that the Federal Government does not incur any additional costs may also use these Certificates. Examples of suitable uses include, but are not limited to:

- Personal or restricted information retrieval
- Updating personal or restricted information
- Filings with government agencies
- Application processes, such as applying for government licenses, student loans, government benefits, etc.

- Financial transactions with government agencies
- Distribution of code

Relying Parties must evaluate the environment and the associated threats and vulnerabilities, as well as determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Agency for each application and is not controlled by this CPS.

4.2 Certificate Application Processing

An applicant for an ORC NFI Certificate must complete a Certificate application and provide requested information in a form prescribed by the Authorized ORC NFI CA, the ORC NFI CP and this CPS. Information in certificate applications is verified as being accurate before certificates are issued. This section describes ORC procedures to verify information in certificate applications.

4.2.1 Performing Identification and Authentication Functions

Verification of an applicant's identity is performed prior to certificate issuance. All applicants for medium assurance certificates are required to appear in person before an RA, an LRA, or Notary Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions) for identity authentication. All applicants for medium hardware assurance certificates are required to appear in person before an RA or LRA. Applicants for medium assurance and medium hardware assurance certificates are required to present two (2) official photo credentials along with other application information, identified below, and the applicant form generated during the certificate request process containing the public key.

Minors and others not competent to perform face-to-face registration alone are not supported under this CPS.

When the applicant's identity is validated by a Notary Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions), the applicant will submit the notarized statement of identity along with copies of the information used to verify the applicant's identity directly to an ORC RA or LRA, as prescribed in the subscriber agreement. Applicants must fill out and sign a form acknowledging understanding and acceptance of the responsibilities associated with accepting a certificate. The Subscriber Agreement may also serve as a testimonial to the accuracy of the information provided in the certificate request.

The RA or LRA will archive a copy of all information used in the verification process. In all cases, the RA or LRA will submit a digitally signed e-mail message to an ORC IA, including the public key, attesting that the identity of the individual has been authenticated.

In all cases, ORC records the following information:

- The Identity of the person performing the validation process
- Applicant’s name as it appears in the certificate Common Name field
- A signed declaration by the identity-verifying agent that they verified the identity of the applicant
- Method of application (i.e., online, in-person)
- The method used to authenticate the applicant’s identity, including identification type and unique number or alphanumeric identifier on the ID
- The date of verification
- A handwritten signature by the applicant in the presence of the person performing the identity verification
- For each data element accepted for proofing, including electronic forms:
- Name of document presented for identity proofing
- Issuing authority
- Date of issuance
- Date of expiration
- All fields verified
- Source of verification (i.e., which databases used for cross-checks)
- Method of verification (i.e., online, in-person)
- Date/time of verification
- The ORC NFI name, including subcontractors, if any
- All associated error messages and codes
- Date/time of process completion
- Names (IDs) of ORC PKI processes, including subcontractors’ processes, if any.

Alternately, certificate requests may be validated and authenticated on the basis of electronically authenticated subscriber requests using a current, valid PKI signature certificate issued by an ORC NFI CA and associated private key. The following restrictions apply:

- The assurance level of the new certificate will be the same or lower than the certificate used as the authentication credential.
- The DN of the new certificate will be identical to the DN of the certificate used as the authentication credential.

- Information in the new certificate that could be used for authorization will be identical to that of the certificate used as the authentication credential.
- The expiration date of the new certificate will be no later than the next required in-person authentication date associated with the certificate used as the authentication credential.
- The validity period of the new certificate will not be greater than the maximum validity period requirements of the NFI CP for that particular type of certificate.
- The in-person authentication date associated with the new certificate will be no later than the in-person authentication date associated with the certificate used for authentication.

In all cases, ORC may request additional information or verification if deemed necessary to confirm the requestor's identity.

4.2.1.1Authentication of Unaffiliated Individual NFI Digital Signature and Encryption Certificates

Unaffiliated Individuals are required to appear in person before an ORC RA, an LRA, or a Notary Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions) for identity authentication. ORC verifies all of the following identification information supplied by the applicant: first name, middle initial, and last name, date of birth, current address (number and street, city, ZIP code), and telephone number.

An exception to the above is provided to the Government when the Government provides identity proofing. Any exception is the subject of an approved Registration Practice Statement.

4.2.1.2Authentication of NFI Business Representative Digital Signature and Encryption Certificates

Verification of an applicant's identity for an NFI Business Representative Digital Signature or Encryption Certificate will be performed prior to certificate issuance. Applicants are required to appear in person before an RA, an LRA, or a Notary Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions) for identity authentication.

The ORC NFI RA, LRA or Trusted Agent will verify:

- That the applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association, in good standing.
- The Sponsoring Organization's identity as specified in Section 3.1.8.

The process documentation and authentication requirements will include the following:

- Identity of the person performing the identification
- A signed declaration by that person that he or she verified the identity of the subscriber as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy
- A unique identifying number from the ID of the verifier and from the ID of the applicant
- The date and time of the verification
- A declaration of identity signed by the applicant, using a handwritten signature, performed in the presence of the person performing the identity authentication.

4.2.1.3Authentication of NFI Organization (Relying Party Applications) Digital Signature and Encryption Certificates

If the applicant is requesting an ORC NFI Organization (Relying Party Applications) Digital Signature or Encryption Certificate, ORC verifies:

- that the applicant is authorized to act on behalf of the Relying Party
- the affiliation of the NFI Certificate applicant with the Relying Party
- that the applicant's organization has completed a Relying Party Agreement with ORC

4.2.1.4Authentication of Component Identity Certificates (e.g. Agency Application SSL Server or VPN IPSec Certificates)

Some computing and communications components (web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor as described in Section 3.2.3.1. The PKI Sponsor is responsible for providing the ORC NFI approved IA's, through an application form, correct information regarding:

- Equipment identification
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the ORC to communicate with the PKI sponsor when required

An ORC NFI IA will authenticate the validity of any authorizations to be asserted in the certificate, and will verify source and integrity of the data collected to an assurance level commensurate with the certificate level being requested.

Authentication and integrity checking is accomplished by one of the following methods:

- Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested).
- In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.1.9.

4.2.1.5Qualified Relying Party NFI Certificates

If the applicant is requesting a Qualified Relying Party NFI Certificate, ORC verifies:

- That the applicant is authorized to act on behalf of the Qualified Relying Party.
- The affiliation of the NFI Certificate applicant with the Qualified Relying Party, ORC, or Agency Application.

4.2.2 Approval or Rejection of Certificate Applications

Upon successful completion of the subscriber identification and authentication process in accordance with the GSA NFI MOA, ORC creates the requested NFI Certificate, notifies the applicant thereof, and makes the NFI Certificate available to the applicant. The subscriber identification and authentication process has been completed successfully when the process(es) described in section 3.2 have occurred and the requested name and Organization have been verified by examination of documentation. If the applicant provided an e-mail address, ORC sends the notification message via e-mail. If no e-mail address was provided, ORC sends the notification to the U.S. postal address provided.

If verification is not successful or the application is otherwise rejected, ORC notifies the applicant of the verification failure or rejection via an out-of-band notification process linked to the certificate applicant's physical postal address. This notification includes the steps required by the applicant to resume processing of the certificate request.

The ORC NFI records the following transaction data:

- Applicant's name as it appears in the applicant's request for a certificate
- Method of application (i.e., online, in-person) for each data element accepted for proofing, including electronic forms
- Name of document presented for identity proofing
- Issuing authority
- Date of issuance

- Date of expiration
- All fields verified
- Source of verification (i.e., which databases used for cross-checks)
- Method of verification (i.e., in-person)
- Date/time of verification
- Names of the individual completing the identity verification
- Fields that failed verification
- Status of current registration process (suspended, ended, etc.)
- All identity verification data
- All associated error messages and codes
- Date/time of process completion or suspension

4.2.3 Time to Process Certificate Applications

The entire process from applicant appearing before one of the required identity verifiers to certificate issuance will take no more than 30 days. ORC RAs will not process certificate requests for issuance if the date of the Identity Verification process is more than 30 days old.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Upon successful completion of the subscriber identification and authentication process in accordance with the ORC NFI CP, ORC creates the requested ORC NFI Certificate, notifies the applicant thereof, and makes the ORC NFI Certificate available to the applicant.

The IA issues certificates upon receipt of the RA digitally signed e-mail only after verifying that the applicant's subject DN (provided in the RAs e-mail) matches the subject DN in the CA database. The IA archives the e-mails signed by RAs when issued certificates are published and issuance transactions automatically logged.

In the case of code signing certificate issuance, the IA verifies that the subject DN and the DN in the subject alternate name field match those provided by the attribute authority and the code signer.

Upon issuance of a Certificate, the Authorized ORC NFI CA warrants to all Program Participants that:

- The Authorized ORC NFI CA will manage the Certificate in accordance with the requirements in the CP and this CPS.
- The Authorized ORC NFI CA has complied with all requirements in this CPS when identifying the Subscriber and issuing the Certificate.
- There are no misrepresentations of fact in the Certificate known to the Authorized ORC NFI CA and the Authorized ORC NFI CA has verified the information in the Certificate. It is the responsibility of the Authorized ORC NFI CA to verify the source of the certificate request, and to ensure that Subscriber information submitted in the application process is correct and accurate. Information will be verified to ensure legitimacy as per Section 3.2, Initial Identity Validation.
- Information provided by the Subscriber for inclusion in the Certificate has been accurately transcribed to the Certificate.
- The Certificate meets the material requirements of the CP and this CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

If the applicant provided an e-mail address, ORC sends the notification message via e-mail. If no e-mail address was provided, ORC sends the notification to the U.S. postal address provided.

The notification informs the applicant of the creation of a certificate, states a URL for use by the applicant for retrieving the certificate, contain a unique serial number, and reaffirms the subscriber’s responsibilities as explained in the application process. The notification also obligates the subscriber to:

- Accurately represent themselves in all communications with the ORC PKI;
- Protect the private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures;
- Notify ORC, in a timely manner, of the suspicion that his or her private key(s) is compromised or lost. Such notification through mechanisms consistent with this CPS; and,
- Abide by all the terms, conditions, and restrictions levied upon the use of his or her private key(s) and certificate(s).

Upon issuance of an NFI Certificate, ORC warrants to all program participants that:

- ORC has issued, and manages, the NFI Certificate in accordance with the requirements in this CPS
- ORC has complied with all requirements in this CPS when identifying the subscriber and issuing the NFI Certificate

- There are no misrepresentations of fact in the NFI Certificate known to ORC and that ORC has verified the information in the NFI Certificate
- Information provided by the subscriber for inclusion in the NFI Certificate has been accurately transcribed to the NFI Certificate
- The NFI Certificate meets the material requirements of this CPS

4.4 Certificate Acceptance

A condition to issuing an NFI Certificate is that the subscriber will indicate acceptance or rejection of the ORC NFI Certificate to ORC and acknowledge the subscriber obligations. By accepting the ORC NFI Certificate, the subscriber is warranting that all information and representations made by the subscriber that are included in the ORC NFI Certificate are true.

ORC notifies the certificate applicant of certificate issuance through e-mail. The notification includes the URL that the applicant uses to receive the approved certificate. ORC verifies possession of the subscriber's private key at the time the applicant accepts the issued certificate.

The notification informs the subscriber of the creation of the certificate, contents of the certificate and reaffirms the subscriber's responsibilities as explained in the application process. The notification informs the subscriber if the private key has been escrowed.

The subscriber agreement includes the following subscriber obligations. The subscriber will:

- Accurately represent themselves in all communications with the ORC.
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures.
- Notify ORC, in a timely manner, of the suspicion that their private keys are compromised or lost. Such notification will be made directly, or indirectly through mechanisms consistent with this CPS.
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.
- Formally accept the certificate at the designated ORC web page during certificate retrieval. (Failure to do so will result in revocation of the certificate.)

The subscriber has already agreed to the obligations during the request phase (as stipulated in the Subscriber Agreement), and the certificate can only be accepted during a PoP of private key test. ORC logs the acceptance of the certificate.

A subscriber who does not provide this verification notice within 30 calendar days of receiving notification that his or her approved certificate is available for downloading, or who is found to have acted in a manner counter to these obligations will have his or her certificate revoked, and will forfeit all claims he or she may have against the ORC NFI PKI in the event of a dispute arising from the failure to fulfill the obligations above.

4.4.1 Conduct Constituting Certificate Acceptance

The subscriber is in possession and control of the private key from time of generation or benign transfer. The ORC NFI CAs authenticate the subscriber with a Proof of Possession (POP) test when requesting and retrieving a certificate by requiring the subscriber to perform a private key operation and verifying that the public key presented by the subscriber matches the private key.

In all cases, IAs may request additional information or verification from an RA or LRA if deemed necessary by the IA to confirm the requestor’s identity.

4.4.2 Publication of the Certificate by the CA

As part of the NFI Certificate application process, the subscriber’s public key is transferred to the ORC NFI CAs in a way that ensures:

- It has not been changed during transit
- The sender possesses the private key that corresponds to the transferred public key
- The sender of the public key is the legitimate user claimed in the certificate application

Public keys are delivered to the certificate issuer in a PKCS#10 or Certificate Request Message Format (CRMF) certificate request

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

ORC will notify Federal PKI Policy Authority any time an ORC NFI CA issues a CA certificate to any entity outside of ORC or upon issuance of a new inter-organization CA cross-certificate.

4.5 Key Pair and Certificate Usage

ORC certifies keys for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension. The key usage extension is included in all certificates and is always marked critical in order to limit the use of a public key certificate for its intended purpose, as stipulated in the X.509 Certificate and CRL Extensions Profile for the FPCPF [CCP-PROF].

4.5.1 Subscriber Private Key and Certificate Usage

Certificates asserting the id-orc-nfissp-pivi-hardware will include a critical keyusage extension, asserting only the digitalSignature value.

4.5.1.1Individual Subscriber

When requesting and using a certificate issued under this CPS, a subscriber accepts the following obligations:

- To accurately represent themselves in all communications with the PKI
- To protect the certificate private key from unauthorized access as stipulated in their certificate acceptance agreements, and local procedures
- To immediately report to the appropriate RA or LRA and request certificate revocation if private key compromise is suspected
- To use the certificate only for authorized applications which have met the requirements of this CPS
- To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension
- To report any changes to information contained in the certificate to the appropriate RA or LRA for certificate reissue
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates
- Subscribers leaving the organizations that sponsored their participation in the PKI will surrender to their organization's PKI PoC (through any accountable mechanism, defined in an agencies Registrations Practice Statement (RPS) in the case of FPFCF) all cryptographic hardware tokens that were issued, under the sponsoring organization, prior to leaving the organization

These obligations are provided to the subscriber during the registration process in the form of a Subscriber Agreement that the subscriber must read and agree to prior to completing registration. Theft, compromise or misuse of the private key may cause the subscriber, Relying Party and their organization legal consequences.

4.5.1.2Server/Component Certificate Subscriber

When requesting, renewing and using a server certificate or VPN IPSec issued under this CPS, the applicant agency or company and their PKI Sponsor accept the following obligations:

- To accurately represent themselves in all communications with the PKI and abide by all the terms, conditions and restrictions levied upon the use of the issued private key(s) and certificate(s).

- To protect the certificate private key from unauthorized access.
- To immediately report to the appropriate RA and request certificate revocation if private key compromise is suspected.
- In the event of a PKI sponsor change, due to the verified individual having left the employ of the subscribing company or no longer being assigned as the PKI sponsor for the certificate, the applicant company must designate a new PKI sponsor and the new PKI sponsor must complete a new identity verification. Additionally, the new PKI Sponsor must sign an acknowledgment of responsibility and accountability for all certificate by DN and serial number that were accountable to the previous PKI Sponsor.
- When renewing the server certificate, the PKI sponsor must complete a new identity verification.
- Confirm that you are a current employee of the applying company and that you are authorized to obtain server certificates for the company by completing and submitting the “Proof of Organizational Affiliation” letter.
- The server designated in the certificate request is the only system on which the certificate is to be installed.
- To use the certificate only for authorized applications that have met the requirements of this CPS.
- To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension.
- To report any changes to information contained in the certificate to the appropriate RA for certificate reissue processing.

4.5.1.3Code Signer Certificate Subscriber

When requesting and using a code-signing certificate issued under this CPS, the organization and the code signer accept the following obligations:

- To accurately represent themselves in all communications with the PKI and abide by all the terms, conditions and restrictions levied upon the use of the issued private key(s) and certificate(s)
- To protect the certificate private key from unauthorized access
- To immediately report to the RA if private key compromise is suspected
- Request that the Code Signing Attribute Authority approve and forward to the RA an authorization on the code signer’s behalf to obtain a code signing certificate
- To apply for (generate a key pair) and download the code signing certificate onto a FIPS 140-2 Level 2 validated smart card

- When not in use, the Code Signer hardware token will be stored in a locked container
- Submit the certificate request to the CA via a secure (SSL protected) web session
- Digitally sign an e-mail, using acceptable PKI credentials, that contains the subject Distinguished Name (DN), code signer DN, and the code signing certificate request number and send it to an ORC RA
- In the event of Code Signer change (due to the verified individual having left the employ of the subscribing organization or no longer being assigned as the code signer for the certificate) the applicant organization must designate and notify ORC of the new Code Signer
- The Code Signer is a current employee of the organization and is authorized to obtain a code signing certificate(s) for the organization
- To use the certificate only for authorized applications which have met the requirements of this CPS
- To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension
- To report any changes to information contained in the certificate to the appropriate RA

4.5.2 Relying Party Public key and Certificate Usage

This CPS is binding on each Qualified Relying Party by virtue of its ORC NFI Agreement, and governs its performance with respect to its application for, use of, and reliance on NFI Certificates.

ORC publicly posts a summary of this CPS on the ORC website (NFI.orc.com) to provide the relying party information regarding the expectation of the ORC systems. When accepting a certificate issued under this CPS, a relying party accepts the following obligations:

- Perform a risk analysis to decide whether the level of assurance provided by the certificate is adequate to protect the Relying Party based upon the intended use
- To ensure that the certificate is being used for an appropriate approved purpose
- To check for certificate revocation prior to reliance
- To use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension)

- To verify the digital signature of the ORC CA that issued the certificate being relied upon as stipulated in the NFI CP
- To establish trust in the ORC NFI PKI by verifying the chain of CA certificates starting from a trust anchor of the relying party in accordance with the guidelines set by the X.509 Version 3 Amendment:
    - ❑ for the ORC NFI PKI, this trust anchor is the ORC NFI Self-signed Root CA with no additional chaining
    - ❑ for ORC certificates asserting a FPCPF OID, this trust anchor is the FPCPF Self-signed CA with no additional chaining
- To acknowledge all warranty and liability limitations
- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data
- To abide by all the terms, conditions and restrictions levied upon the use of the issued private key(s) and certificate(s) as stipulated in the NFI CP

Data format changes associated with application upgrades may invalidate digital signatures and will be avoided.

Relying parties that do not abide by these obligations assume all risks associated with the certificates upon which they are relying.

4.6 Certificate Renewal

ORC accepts NFI Certificate renewal requests from their subscribers within 90 days from the scheduled end of the operational period (expiration date) of the NFI Certificate, provided the NFI Certificate is not revoked, suspended, or expired. NFI Certificates are renewed in 3-year increments, no more than 2 times before certificate re-key is required.

4.6.1 Circumstance for Certificate Renewal

To renew a certificate, as described in the NFI CP, the subscriber obtains a new certificate based on an existing key pair. ORC authenticates the subscriber’s renewal request using the subscriber’s current certificate for authentication in the renewal process. In the event that subject information has changed (and/or the key pair is required to be changed for any reason), ORC requires the subscriber to request a new NFI Certificate. The old certificate (as a result of an update action) may or may not be revoked, but is not further re-keyed, renewed, or updated. A certificate that is not renewed by the end of the operation period reflects an expired status.

ORC renews NFI Certificates issued to Relying Parties only after completing successful identity proofing verification in accordance with the requirements for identity proofing specified in Section 3.2.3.1.

4.6.2 Who May Request Renewal

ORC accepts NFI Certificate renewal requests from their subscribers within 90 days from the scheduled end of the operational period (expiration date) of the NFI Certificate, provided the NFI Certificate is not revoked, suspended, or expired. NFI Certificates are renewed in 3-year increments, no more than 2 times before certificate re-key is required.

4.6.3 Processing Certificate Renewal Requests

To renew a certificate, as described in the NFI CP, the subscriber obtains a new certificate based on an existing key pair. ORC authenticates the subscriber's renewal request using the subscriber's current certificate for authentication in the renewal process. In the event that subject information has changed (and/or the key pair is required to be changed for any reason), ORC requires the subscriber to request a new NFI Certificate. The old certificate (as a result of an update action) may or may not be revoked, but is not further re-keyed, renewed, or updated. A certificate that is not renewed by the end of the operation period reflects an expired status.

ORC renews NFI Certificates issued to Relying Parties only after completing successful identity proofing verification in accordance with the requirements for identity proofing specified in Section 3.2.3.1.

Server subscribers (PKI Sponsors) are required to revalidate their identity and any equipment authorizations and/or attributes (if any are to be included in the certificate). The subscriber is required to present a currently valid certificate to request a new certificate. End-users are required to renew their certificates through a web-based electronic form.

- Medium assurance certificate may be renewed or updated on the basis of electronically authenticated subscriber requests three times. Every eight years, in-person authentication is required.
- Medium hardware assurance certificates may be renewed or updated on the basis of electronically authenticated subscriber requests only one time. Every four years, in-person authentication is required.

Certificates issued by an ORC NFI CA have a validity period of two years. Prior to the expiration of these certificates, identity and encryption certificate subscribers are required to request a new certificate, which may be done by electronically submitting their existing certificates.

During the renewal process the user must present his or her current identity certificate during an SSL client authentication to the CA. The CA validates the authenticity of the certificate being presented by verifying that the certificate was issued by the CA in question and mapping the subject name in the certificate to its corresponding certificate in the database. This process verifies that the subscriber is eligible for renewal on the basis of the subscriber's existing certificate, as stipulated above. If the subscriber is not eligible for renewal on the basis of the subscriber's existing certificate, ORC redirects the subscriber to the in-person registration process. The forms to accomplish this process are controlled by access control lists on a secure web server that binds to the corresponding users with certificates in an LDAP directory. Access control to the renewal forms is based on comparing the certificate with the Distinguished Name of the subscriber (based on an X.509 certificate-based authentication) against the certificate with DN in the directory.

Provisions for the renewal of Code signing certificates are in accordance with the Medium Hardware Assurance criteria below.

In cases where a subscriber's organization (including PKI Sponsors or CSAAs) has required authorizations to be included in an ORC NFI certificate, the person responsible for that organization ORC NFI agreement will notify an ORC NFI RA of the withdrawal of authorizations, via digitally signed e-mail using a medium assurance hardware certificate. The RA verifies the signature of the subscriber's organization.

4.6.4 Notification of New Certificate Issuance to Subscriber

Upon successful completion of the subscriber identification and authentication process in accordance with the GSA NFI MOA, ORC creates the requested NFI Certificate, notifies the applicant thereof, and makes the NFI Certificate available to the applicant. If the applicant provided an e-mail address, ORC sends the notification message via e-mail. If no e-mail address was provided, ORC sends the notification to the U.S. postal address provided.

The notification informs the applicant of the creation of a certificate, states a URL for use by the applicant for retrieving the certificate, contain a unique serial number, and reaffirm the subscriber's responsibilities as explained in the application process. The notification also obligates the subscriber to:

- Accurately represent themselves in all communications with the ORC PKI;
- Protect the private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures;
- Notify ORC, in a timely manner, of the suspicion that his or her private key(s) is compromised or lost. Such notification through mechanisms consistent with this CPS; and,

- Abide by all the terms, conditions, and restrictions levied upon the use of his or her private key(s) and certificate(s).

Upon issuance of an NFI Certificate, ORC warrants to all program participants that:

- ORC has issued, and manages, the NFI Certificate in accordance with the requirements in this CPS
- ORC has complied with all requirements in this CPS when identifying the subscriber and issuing the NFI Certificate
- There are no misrepresentations of fact in the NFI Certificate known to ORC and that ORC has verified the information in the NFI Certificate
- Information provided by the subscriber for inclusion in the NFI Certificate has been accurately transcribed to the NFI Certificate
- The NFI Certificate meets the material requirements of this CPS

The ORC NFI CAs are configured to establish client authenticated SSL sessions and is configured (by the CAA) to recognize IAs as legitimate issuers via certificate authentication. IAs using CA issued medium hardware assurance certificates, and recognized by the CA, are required to initiate the SSL session with the CA to begin the issuance process. Upon successful authentication, the IA searches the CA database for the appropriate certificate request.

The IA issues certificates upon receipt of the RA digitally signed e-mail only after verifying that the applicant’s subject DN (provided in the RAs e-mail) matches the subject DN in the CA database. The IA archives the e-mails signed by RAs when issued certificates are published and issuance transactions automatically logged.

In the case of code signing certificate issuance, the IA verifies that the subject DN and the DN in the subject alternate name field match those provided by the attribute authority and the code signer.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

For certificates issued by the Common Policy Root CA, failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

For all other CAs operating under this policy, failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

The subscriber is in possession and control of the private key from time of generation or benign transfer. The ORC NFI CAs authenticate the subscriber with a Proof of Possession (POP) test when requesting and retrieving a certificate by requiring the subscriber to perform a private key operation and verifying that the public key presented by the subscriber matches the private key.

In all cases, IAs may request additional information or verification from an RA or LRA if deemed necessary by the IA to confirm the requestor's identity.

4.6.6 Publication of the Renewal Certificate by the CA

Publication of the renewed Authorized NFI CA certificate will be in accordance with section 4.4.2, Publication of the Certificate by the Authorized NFI CA.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

ORC NFI CAs will provide notification of certificate issuance to other inter-organizations entities in accordance with the notification processes specified in Section 4.4.3.

4.7 Certificate Re-Key

NFI Certificate re-keying (signing and encryption) is accomplished through the limitation on certificate renewal, see Section 3.2.3. The minimum requirement for all NFI certificate re-keying, with the exception of CA certificates, is once every 9 years from the time of initial registration (i.e., after two 3-year renewals). ORC NFI subscribers will identify themselves for the purpose of re-keying through use of their current signature key, except that identity will be established through initial registration process described in Section 3.1.

After certificate re-key and issuance of new certificate, the old certificate will be revoked and placed on the next CRL. The old certificate will not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-key

A certificate will be re-keyed when it can no longer be renewed. The minimum requirement for all certificate re-keying, with the exception of the Authorized ORC NFI CA certificates, is once every three years, in accordance with Section 6.3.2, Certificate Operational Periods and Key Usage Periods.

A revoked ORC NFI certificate will not be re-keyed.

Requirements for CA re-key are described in Section 5.6.

4.7.2 Who May Request Certification of a New Public Key

For Authorized ORC NFI CAs supporting re-key, such requests are only accepted from the subject of the certificate or PKI Sponsors. Additionally, CAs and RAs may initiate re-key of a subscriber's certificates without a corresponding request.

Subscribers with a currently valid certificate may request certification of a new public key. A successful biometric 1:1 match of the applicant against the biometrics collected, as stipulated in Section 3.2.3.1 is required. This biometric 1:1 match must be conducted in the presence of a trusted agent of the issuer.

4.7.3 Processing Certificate Re-keying Requests

The re-key process will be in accordance with the certificate issuance process described in Section 3.2. Identity validation may be in accordance with Section 3.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

Authorized NFI CAs will notify subscribers of new NFI certificate issuance in accordance with the notification processes specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Conduct constituting acceptance of a re-keyed certificate will be in accordance with the processes specified in Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

When an ORC NFI CA private signature key is updated, and thus generates a new public key, ORC notifies all CAAs, IAs, RAs, LRAs, and subscribers that rely on the CA's certificate that it has been changed.

CA and OCSP responder certificates may be renewed.

Subscriber certificates are published to a repository at the time of issuance, including re-keyed certificates, and remain accessible from the repository following subscriber acceptance.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

When an ORC NFI CA private signature key is updated, and thus generates a new public key, ORC notifies all CAAs, IAs, RAs, LRAs, and subscribers that rely on the CA's certificate that it has been changed.

CA and OCSP responder certificates may be renewed.

For subscriber certificates no stipulation.

4.8 Certificate Modification

Updating a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate. For example, the ORC NFI may choose to update a certificate of a Subscriber who gains an authorization. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

ORC will authenticate the validity of any authorizations using the same means as for the initial authorization or means of equal or greater security and assurance.

When an ORC NFI root CA updates its private signature key and thus generates a new public key, the new trust anchor will be provided to all CAs, RAs, and Subscribers in accordance with the requirements of Section 6.1.4.

When any other CA updates its private signature key and thus generates a new public key, the ORC NFI will obtain a new certificate from the parent CA in accordance with the requirement of Section 4.1.

4.8.1 Circumstance for Certificate Modification

An ORC NFI CA may modify a CA or OCSP responder certificate whose characteristics have changed (e.g. assert new policy OID). The new certificate may have the same or a different subject public key.

An ORC NFI certificate may be modified if some of the information other than the DN, such as the e-mail address or authorizations, has changed.

If the Subscriber’s name has changed, the Subscriber must undergo the initial registration process.

4.8.2 Who May Request Certificate Modification

The Subscriber or RA may request the modification of a Subscriber certificate. The CA or RA will validate any changes in the subscriber authorizations reflected in the certificate.

4.8.3 Processing Certificate Modification Requests

The certificate modification process will be in accordance with the certificate issuance process described in Section 3.2. Identity validation may be in accordance with this CPS. In addition, the CA or RA validates any changes in the subscriber authorizations reflected in the certificate. Proof of all subject information changes must be provided to the RA or other designated agent and verified before the modified certificate is issued. Verification may occur via digitally signed email or written verification from the Subscriber that the information has changed. (Note: that this will probably be limited to the email address.)

4.8.4 Notification of New Certificate Issuance to Subscriber

ORC CAs will notify subscribers of new certificate issuance in accordance with the notification processes specified in Section 4.3.2,

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Conduct constituting acceptance of a certificate shall be in accordance with the processes specified in Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

The individual making the request will either digitally sign requests for certificate revocation, or the individual will present the request in person to an RA.

Code signer certificates may not be revoked when the code signer departs or is no longer with the organization. Code signer's suspected of having signed (intentionally or unintentionally) unapproved code, may have their code signing certificate revoked by the IA.

4.9.1 Circumstances for Revocation

Whenever any of the circumstances below occur, the associated certificate will be revoked and placed on the CRL, except for OCSP Responder certificates that include the id-pkix-ocsp-nocheck extension. In addition, if it is determined, subsequent to issuance of new certificates, that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key will be revoked. Certificates will remain on the CRL until they expire. They will be removed after they expire, but must at least appear in one CRL.

A subscriber, or a Sponsoring Organization (where applicable), is responsible for promptly requesting revocation of an ORC NFI certificate:

- When the private key, or the media holding the private key, associated with the ORC NFI Certificate is, or is suspected of having been, compromised
- When the individual named as a Business Representative no longer represents, or is no longer affiliated with, the Sponsoring Organization
- If ORC learns, or reasonably suspects, that the subscriber's private key has been compromised or the subscriber has failed to meet their responsibilities
- If ORC determines that the ORC NFI Certificate was not properly issued in accordance with this CPS
- If the certificate holder requests that the certificate be revoked
- If the certificate holder can be shown to have violated the subscriber obligations, including payment of any required fees
- If the certificate holder is no longer authorized to hold the certificate (e.g. termination of employment or change in responsibilities)
- If the information in the certificate is no longer accurate so that identifying information needs to be changed (e.g. change of name or privilege attributes asserted in the subscriber's certificate are reduced)
- The subscriber's employer or organization requests revocation
- The certificate was obtained by fraud or mistake
- The certificate was not correctly requested, issued or accepted
- The certificate contains incorrect information, is defective or creates a possibility of incorrect reliance or usage
- Certificate private key compromise is suspected
- The certificate holder fails to make a payment or other contractual obligations related to the certificate

ORC reserves the right to revoke any ORC NFI issued certificate at its discretion.

ORC provides for the revocation of certificates when requested, at any time for any reason. If the Government provided RA functions, or if ORC has delegated revocation functions to subcontractor RAs, all information is transmitted via a network between ORC and/or subcontractors and/or government RAs using mutual authentication.

4.9.2 Who Can Request Revocation

A subscriber may request revocation of his/her/its ORC NFI Certificate at any time for any reason. A Sponsoring Organization may request revocation of an NFI Certificate issued to its Business Representative at any time for any reason. If the Government provided RA functions, or if ORC has delegated revocation functions to subcontractor RAs, all information is transmitted via a network between ORC and/or subcontractors and/or government RAs using mutual authentication.

ORC reserves the right to revoke any ORC NFI issued certificate at its discretion.

4.9.3 Procedure for Revocation Request

An ORC NFI certificate revocation request should be promptly communicated directly to an RA or LRA who are authorized to accept such notices on behalf of the CA.

If the subscriber is making the revocation request for their identity certificate, and is in possession of their private identity key associated with the certificate, the subscriber may access the ORC NFI website to revoke his or her own certificate at any time. Upon accessing the User Certificate Revocation Page the users is presented with a radio button list with the following “Revocation Reason”:

- Unspecified
- Key Compromise
- Cessation of Operation
- Affiliation Changed
- Superseded

A mutually authenticated SSL session is established using the private identity key, which provides proof of possession of the subscriber's private key associated with the identity certificate to be revoked. This revocation is immediate. If a subscriber revokes their private identity key, but continues to hold a key management certificate they must either submit a request for a new identity certificate or a request to revoke their key management certificate(s). If ORC does not receive such a request within 30 days the subscriber's key management certificate(s) will be administratively revoked.

If a subscriber intends to revoke all of their certificates it is recommended that they submit a digitally signed certificate request, as stipulated below, prior then performing the immediate revocation of their identity certificate.

In the case of a subscriber's key management certificate or if the subscriber is no longer in possession of the private key, or an entity other than the subscriber is making the revocation request, this request may be communicated via an online form, electronically via digitally signed e-mail, or in person to an ORC RA, or via U.S. postal mail. In the case of a digitally signed email from the subscriber's the signature will be generated using the subscriber's identity certificate When revoking a subscriber's key management certificate the IA will verify that the subscriber's identity certificate dnQualifier is consistent with the dnQualifier of the subscriber's key management certificate.

All revocation requests are verified prior to certificate revocation. If the subscriber makes the request and has the private key, this proof of possession test is considered adequate and the certificate is revoked immediately.

If the request comes via a digitally signed e-mail message (signed with a certificate at least of the same assurance level as the certificate to be revoked) sent from an ORC CMA or an authorized Sponsoring Organization representative, validation of the e-mail signature is considered adequate and the certificate is revoked.

If the request comes from an in person visit, identity credentials are required (at least to the same assurance level as the certificate to be revoked) from the individual making the request and verified prior to revoking the certificate. If the request is made via online form or unsigned e-mail, ORC contacts the subscriber via the information kept in the database from the request process to verify the request prior to certificate revocation. For these cases, the certificate is suspended pending verification of the revocation request.

In the case of certificates issued under the FPCPF, if the request comes from an agency designated person authorized to request revocation of certificates and signed with identity credentials at least to the same assurance level as the certificate to be revoked, ORC will revoke the certificate immediately.

If an ORC CMA or RA is making the request, the reason for the revocation request is documented. If an LRA is requesting the revocation, the reason will be sent to an RA via a digitally signed e-mail message for revocation, who investigates the request, document the reason for the revocation request and archive. Upon disposition, the CMA or RA sends the reason for revocation and confirm that it was vetted to the IA via a digitally signed e-mail message for revocation.

ORC will revoke or suspend the certificate by placing its serial number and identifying information on a CRL. ORC will also remove the certificate from any repositories containing that certificate.

The subscriber is notified of the revocation request, reason for the request, and status of the request. If appropriate, the subscriber is provided information on obtaining a new certificate and a list of all certificates issued.

If an ORC CMA is choosing to revoke a certificate because of sufficient evidence of noncompliance with this CPS, an ORC IA documents the reason for certificate revocation and notifies the subscriber of the revocation.

Subscribers leaving the organizations that sponsored their participation in the PKI will surrender to their organization's PKI PoC (through any accountable mechanism, defined in the RPS in the case of FPCPF) all cryptographic hardware tokens that were issued, under the sponsoring organization, prior to leaving the organization. The PKI PoC will zero (refer to Section 6.2.7) or destroy the token promptly upon surrender and will protect the token from malicious use from the time of surrender. The procedure(s) used to zero a token will depend on the type of applications and hardware used to access of create the token. If the Subscriber leaves an organization and the hardware tokens cannot be obtained, then all certificates associated with the unretrieved tokens shall be immediately revoked. In all cases, whether software or hardware tokens are involved, the organization will promptly notify an ORC RA to revoke the certificate and attest to the disposition of the token, via a digitally signed e-mail.

4.9.4 Revocation Request Grace Period

Certificates are revoked upon request as soon as the need can be verified. There is no grace period. The subscriber, or sponsoring organization, must request revocation from ORC as soon as the need for revocation has been determined.

4.9.5 Time within which CA must Process the Revocation Request

CAs will revoke certificates within 8 hours of receipt of a proper revocation request. A new CRL will be manually published after any Revocations have been processed.

Certificates are revoked upon request as soon as the need can be verified. There is no grace period. The subscriber, or sponsoring organization, must request revocation from ORC as soon as the need for revocation has been determined.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

The ORC NFI CAs issue CRLs every 12 hours with a validity period of 18 hours. New CRLs are issued twice per day even if there are no changes or updates to be made. When a revocation request is granted for the reason of key compromise, the revocation information will be posted on the next CRL, except that, if the revocation request is made within two hours of the next schedule CRL, the revocation information may be posted on the very next CRL. All superseded CRLs are removed from the repository upon posting of the latest CRL.

When a CA certificate or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL is issued immediately as stipulated in Section 4.9.12.

ORC NFI CRLs may be obtained from:

http://NFI.orc.com/CRLs/<CA Name>.crl

ldap://NFI-ds.orc.com/cn=<CA Name>, o=ORC PKI, c=US?certificaterevocationlist;binary.

4.9.8 Maximum Latency for CRLs

The CRL will be posted upon generation, but within no more than four hours after generation. The system is configured to publish to a public LDAP directory upon issuance of the CRL. In the event of publishing failure, automated monitoring scripts verify the current CRL on the CA versus our publicly available CRLs. If the CRL on the CA is more recently published than the publicly available CRL, the scripts pull the newer CRL and replace the publicly available CRL with the more recent CRL.

4.9.9 On-line Revocation/ Status Checking Availability

ORC validates online and near-real-time the status (Valid, Invalid or Suspended) and signature of the NFI Certificate indicated in an NFI Certificate Validation Request message. The CA returns in the Certificate Status Response message a signed message. This functionality is integrated with the GSA-approved Certificate Arbitrator Module (CAM) using the OCSP.

The ORC WAN OCSP Responder (CSP) is located at: http://NFI2.eva.orc.com. Contact ORC to register for use.

ORC supports online status checking via OCSP [RFC 2560] for end entity certificates issued under all subject certificate policies defined in this CPS. Status information maintained by the OCSP server is updated and available to relying parties within 6 hours.

4.9.10 On-line Revocation Checking Requirements

Each Qualified Relying Party will validate every NFI Certificate it receives in connection with a transaction. Any self-signed OCSP responder used for verifying certificates asserting a policy OID from this CPS are required to meet the certificate profile stipulated in the X.509 Certificate and CRL Extensions Profile for the FPCPF [FPKI-PROF] and ensure that:

- Certificates indicated as being valid have a chain of valid certificates (valid as defined by [X.509]) linking back to a "trusted Root CA"
- Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation, such that the Relying Party need not check more than one responder to validate a subscriber certificate
- Certificate status responses provide authentication and integrity services commensurate with the assurance level of the certificate being verified
- It is made clear in the certificate status response the attributes (other than certificate subject name (e.g., citizenship, clearance authorizations, etc.)) being authenticated by the responder
- Accurate and up-to-date CRLs, from the ORC CAs, are used to provide the revocation status
- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked

ORC disclaims any liability for loss due to use of any validation information relied upon by any party that does not comply with this stipulation, in accordance with this CPS.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related To Key Compromise

If an ORC NFI certificate is revoked because of suspicion of private key compromise, the following additional requirements apply in addition to requirements specified above.

ORC issues new CRLs with date of compromise and notifies, through website posting, any relying parties that download the CRL that a certificate has been revoked because of key compromise, and the date that the suspected compromise occurred.

If the compromised certificate was an RA certificate, the RA revalidates any subscriber certificates validated after the date of the suspected compromise, and revokes any certificates not revalidated.

ORC uses reason codes and has the ability to transition any reason code to compromise.

4.9.13 Circumstances for Suspension

If a certificate revocation request is received in an unverified manner, the certificate is placed in suspended status pending authentication of the request. At no time does ORC suspend a CA certificate.

4.9.14 Who Can Request Suspension

For End-entity certificates, no stipulation.

4.9.15 Procedure for Suspension Request

No stipulation for end-entity certificates.

4.9.16 Limits on Suspension Period

For End-entity certificates, no stipulation.

4.10 Certificate Status Services

The ORC Certificate Status Authority (CSA) operating under this CPS is subject to no stipulations.

4.10.1 Operational Characteristics

The CSA provides OCSP responses to subscribers and is responsible for:

- Providing certificate revocation status and/or complete certification path validation (including revocation checking) to the Relying Parties upon request
- Ensuring that the status and validation responses contain authentication and integrity services commensurate with the assurance level of the certificate being checked

The CAA administers the CSA.

4.10.2 Service Availability

No stipulation

4.10.3 Optional Features

No stipulation

4.11 End of Subscription

No stipulation

4.12 Key Escrow and Recovery

Under no circumstances is a signature key escrowed. ORC does not require private key escrow for confidentiality keys. However, ORC recommends to EEs that they locally escrow a copy of the confidentiality private key.

For some purposes (such as data recovery), some organizations may desire key archival and key retrieval for the private component of the encryption certificate key pair. To facilitate this, ORC offers a key escrow and recovery capability.

CA private keys are never escrowed.

4.12.1 Key Escrow and Recovery Policy and Practices

The method, procedures and controls which apply to the storage, request for, extraction and/or retrieval, delivery, protection and destruction of the requested copy of an escrowed key are described in the ORC KRPS.

Under no circumstances is a subscriber signature key allowed to be held in trust by a third party.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

ORC NFI does not support key escrow and recovery using key encapsulation techniques.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

ORC's CA equipment is dedicated to the CA function. IA workstations and IA hardware tokens are dedicated to the use of issuing certificates. RAs and LRAs use general-purpose workstations and medium hardware assurance certificates dedicated to the NFI certificate application process.

The CA, IA, Certificate Management System, and CSA equipment consists of equipment dedicated to the CA, IA, Certificate Management System, and CSA functions, and do not perform non-related functions. The equipment includes, but is not limited to, the system running the CA, IA, Certificate Management System, and CSA software, hardware cryptographic modules, and databases and directories located on the equipment. In addition, databases and directories located on the equipment are not accessible to the subscribers and Relying Parties.

Unauthorized use of CA, IA, Certificate Management System, and CSA equipment is forbidden. Physical security controls are implemented that protect the hardware and software from unauthorized use. Cryptographic modules are protected against theft, loss, and unauthorized use through multiple party management.

A check is made at least once every 24 hours to ensure that no attempts to defeat the physical security mechanisms have been made (see Section 5.1.2.1 for more details).

5.1.1 Site Location and Construction

From the originating assessment of ORC's NFI offering, which result in an "authorization to operate", through continuous monitoring practices consistent with FISMA requirements ORC maintains physical and logical protections for the ORC NFI systems.

5.1.2 Physical Access

Physical access to hardware is limited to authorized personnel and access to any media is also physically protected and access restricted to authorized personnel.

Access restrictions do not necessarily apply to copies of audit log information or archive information made in response to authorized requests.

All unknown or unidentified persons are accompanied or challenged by personnel to prevent unauthorized access to IT resources and/or disclosure of sensitive data. Only authorized users have access to IT resources. Non-cleared maintenance and cleaning personnel are escorted at all times while in central computer rooms and facilities.

ORC employs five levels of physical access control and separate physical access alarm systems.

All hardware cryptographic modules are stored in the GSA-approved security container when not in use.

5.1.2.1Physical Access for CA Equipment

Only ORC personnel who have successfully completed the required screening process and have met the appropriate “clearance” requirements are granted access to controlled areas.

ORC’s physical and environmental security program addresses access controls, water exposures, fire safety, failure of supporting utilities (power & air conditioning), media storage, waste disposal, off-site backup capabilities, structural collapse, interception of data, and mobile and portable systems, in accordance with Federal regulations, GSA policy, and other supporting GSA security guidelines.

In addition, building security cameras are continually monitored and periodic building perimeter checks are performed by building security personnel.

5.1.3 Power and Air Conditioning

The ORC facilities have adequate power and redundant backup power resources to provide unlimited uptime to the Internet through a central UPS and backup diesel generator power system, which also powers an independent air conditioner during a power disaster.

5.1.4 Water Exposure

The ORC facility is located above ground and off of the floor by two feet to prevent internal flooding.

5.1.5 Fire Prevention and Protection

The ORC facility complies with all applicable national, state, and local fire regulations for a commercial office building.

5.1.6 Media Storage

ORC ensures that media is stored so as to protect it from accidental damage (water, fire, electromagnetic).

5.1.7 Waste Disposal

Any media that contains privacy act or other sensitive information is rendered unrecoverable prior to disposal by one of the following methods:

- crosscut shredded (for paper, discs or hard-drives) or
- overwritten (for tape)

- degaussed (hard-drives, tapes)

When ORC determines the need to have media containing sensitive information rendered unrecoverable by an external third party, ORC contracts with PC Recycler. PC Recycler holds GSA Schedule GS-03F-0068V for shredding services, degaussing services and computer recycling.

PC Recycler's data destruction methods are completely in compliance with:

- Department of Defense (DOD)
- National Security Agency (NSA)
- National Institute of Standards and Technology (NIST) Special Publication Series 800-88
- National Industrial Security Program (NISP) Operating Manual (DOD 5220.22-M)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act of 2002
- Fair and Accurate Credit Transactions Act (FACTA)
- Gramm-Leach-Bliley Act
- Bank Secrecy Act
- Patriot Act of 2002
- Identity Theft and Assumption Deterrence Act
- US Safe Harbor Provisions
- FDA Security Regulations (21 C.F.R. part 11)
- PCI Data Security Standard

5.1.8 Off-Site Backup

Backup media for critical data and programs are stored in a secure, off-site location. Backup media is rotated to ensure that the information contained is no more than one week old.

5.2 Procedural Controls

The NFI system is controlled in accordance with National Institute of Standards and Technology (NIST), DoD, GSA, and National Security Agency (NSA) guidelines for certification authority operations.

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles have proven to be diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. ORC uses two approaches to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the persons filling the roles are trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

ORC maintains lists, including names, organizations, and contact information, of those company individuals who act in trusted roles, and makes them available during compliance audits.

5.2.2 Number of Persons Required Per Task

ORC implements commercially reasonable practices that ensure that one person acting alone cannot circumvent safeguards. To increase the likelihood that these roles can be successfully carried out the functions are distributed among more than one person, so that any malicious activity would require collusion.

Under no circumstances will the incumbent of these roles perform their own auditing function. No individual is assigned more than one trusted role.

At least two parties are necessary to do any key management or log operations.

5.2.3 Identification and Authentication for Each Role

All persons fulfilling one of the CMA roles defined in this CPS must prove capable of identifying and authenticating themselves with two forms of picture identification.

5.2.4 Separation of Roles

ORC implements commercially reasonable practices that ensure that one person acting alone cannot circumvent safeguards. To increase the likelihood that these roles can be successfully carried out the functions are distributed among more than one person, so that any malicious activity would require collusion.

Under no circumstances will the incumbent of these roles perform their own auditing function. No individual is assigned more than one trusted role.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

All personnel performing one of the NFI roles are required to have a personal security investigation that has been favorably adjudicated, to be assigned to sensitive positions.

ORC NFI personnel will:

- Be of unquestionable loyalty, trustworthiness, and integrity
- Have demonstrated security consciousness and awareness in all daily activities
- Have a strong background in information technology resource administration and technical administration in either computer operations, system software, and/or application software totaling 12 months
- Not be assigned other duties that would interfere with their CAA, IA or SA duties and responsibilities
- Not knowingly have been previously relieved of a past assignment for reasons of negligence or non-performance of duties
- Be a U.S. citizens
- Have demonstrated financial stability
- Have valid personal security investigations favorably adjudicated and be assigned to sensitive positions
- Have received proper training in the performance of roles and duties. RAs and LRAs are trained in the verification policies and practices of this CPS and are trained in the performance of RA and LRA duties, respectively

5.3.2 Background Check Procedures

NFI trusted personnel go through a thorough background check performed by a qualified investigator, including, but not limited to:

- Criminal history check that shows no misdemeanor or felony convictions
- Civil lawsuit history checks and a social security number trace to confirm valid number
- Personal, financial, and work/job reference checks which show that the subject of the check is competent, reliable and trustworthy
- Financial status check showing that the subject of the check has not committed any fraud or is otherwise financially trustworthy
- Education verification of highest or most relevant degree (regardless of the date of award)
- DMV records will demonstrate no pattern of violations
- A residence check to demonstrate that the person is a trustworthy neighbor
- Social Security trace will show that the person has a valid social security number

An active secret clearance will be sufficient to meet this requirement. The results of these checks will not be released except as required by Section 9.4.4 of the NFI CP.

A competent adjudication authority (e.g. OPM, DSS) using a process consistent with Executive Order 12968 August 1995 or equivalent will have performed adjudication of the background investigation. Re-screening is performed when required, as determined by the requirements of the initial investigation (e.g. secret, 10 years; confidential, 15 years). The ORC Facility Security Officer is responsible for maintaining and stewardship of clearance data.

5.3.3 Training Requirements

All personnel, and contractors located or working on-site or accessing U.S. Government IT resources, receive information systems security awareness training annually. Additionally, periodic refresher training is provided to all personnel. The training program covers the requirements of the Computer Security Act of 1987, Public Law 100-235, which are adequately detailed in the Office of Personnel Management Computer Security Awareness Training materials. The Security Auditor is responsible for managing this training.

Individuals responsible for administering the ORC NFI system receive training. Reading requirements include the NFI CP, this CPS, and the applicable roles documents. In accordance with ORC's established training plan, training completed by the above personnel is documented. The following training is conducted for all individuals administering the ORC NFI system:

- Training relative to the Privacy Act of 1974, information security, physical security, personnel security, and operations security
- Training relative to the activity's particular information technology resources, including operating systems analysis, PKI software versions in use on the CA system, hardware architecture, computer performance evaluation, and network concepts and operations
- Training relative to the stipulations of the ORC PKI system Guidelines, the CP and this CPS
- National Industrial Security Program Awareness
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Training on administering application software
- Systems security training for the appropriate platforms
- Firewall administration training

- Security awareness and proper protection for cryptographic devices

5.3.4 Retraining Frequency and Requirements

Those involved in filling trusted roles are made aware of changes in an ORC authorized CA operation. Any significant changes to the operation require retraining. Re-training is performed, as required, as new system functionality is deployed, or if there is any substantive change in ORC NFI security or operational procedures. ORC maintains a file of signed and dated documentation for the NFI trusted-role personnel listing their names, roles, re-training received, and date training completed. A binder is maintained holding the documentation of all security training and re-training. The ORC PKI Project Director establishes a training plan and training completed by the above personnel is documented.

5.3.5 Job Rotation Frequency and Sequence

ORC ensures the continuity and integrity of the ORC NFI services by having at least two individuals trained and designated for each trusted role filled, with the exception of ISSO/Corporate Security Auditor.

5.3.6 Sanctions for Unauthorized Actions

Any unauthorized actions resulting in irreparable damage to the NFI system such as compromising the private key will be prosecuted to the fullest extent of the law. The responsible individuals may be prosecuted to the maximum of extent that the law affords, both criminal and civil.

Any unauthorized actions by an IA will result in the immediate revocation of the IA certificate and the removal of that individual from the IA role. Certificates issued by that IA might also be revoked. The IA may be prosecuted for any damages caused to the ORC NFI system.

Any unauthorized actions by an RA or LRA will result in the immediate revocation of the RA/ LRA certificate and the removal of that individual from the RA/ LRA role. Certificates validated by that RA/ LRA might also be revoked. The RA/ LRA may be prosecuted for any damages caused to the ORC NFI system.

5.3.7 Independent Contractor Requirements

Any company subcontracting to provide services for any CMA role with regards to the ORC NFI system is required to establish procedures, which are reviewed and approved by ORC. The subcontractor will require all employees delivering such services to be in accordance with this CPS and the NFI CP, and subject to the compliance audit requirements of this CPS.

5.3.8 Documentation Supplied to Personnel

Operations and maintenance documentation is supplied to authorized individuals performing the roles of CAA and SA. Operations manuals for systems and CA administration are written and managed for each logical instance of the ORC NFI system and each physical instance of an ORC NFI system.

Documentation is provided to personnel as required for fulfilling the requirements of each role.

5.4 Audit Logging Procedures

The ORC NFI system creates, maintains, and protects from modification, unauthorized access, or destruction an audit trail of accesses to the resources it protects in accordance with Federal law, regulations, guidelines, as well as GSA security policy and supporting security guidelines. Activity-auditing capabilities employed by ORC on the NFI system maintain a record of system activity by system, by application processes and by users. The ORC NFI system protects the audit data from destruction and provides alternative audit options when the standard audit mechanism is unable to record events.

5.4.1 Types of Events Recorded

ORC archives data and files that include NFI certificate application information, certificate issuance, and transaction data.

ORC records events attributable to human intervention or automatically invoked by the equipment, listed below in this section. At a minimum, the information recorded includes the type of event and the time the event occurred. Where appropriate, additional information is recorded. Where possible, the security audit data is automatically collected; when this is not possible, a logbook or paper physical mechanism is used. All security audit logs, both electronic and non-electronic, are retained in accordance with the requirements of Section 4.6.3, and made available during compliance audits.

For each auditable event, CMA security audit records include, at a minimum:

- The type of event
- The date and time the event occurred
- Messages from RAs (or other trusted entities) requesting CA actions, the message source, destination and contents
- Attempted CA certificate signature or revocation, a success or failure indication

- Operator initiated actions (including equipment and application access), the identity of the equipment operator who initiated the action
- Events related to the software:
    - Installation - name of installers, date of installation, and build information of any files installed, as well as and EE key generation
    - Software modification - name of modifier, date of modification, build information of any modified files, reason for modification
    - Configuration modification - changes in configuration files, security profiles, certificate and CRL profiles, administrator privileges, changes to audit parameters, and reason for modification
    - Logins and logouts - username, unique identifier number, and time are recorded for failed login attempts
    - Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages
    - Any known or suspected violations of physical security, suspected or known attempts to attack the CMA equipment via network attacks, equipment failures, power outages, network failures, or violations of this certificate policy

The equipment records server installation, access, and modification. Security auditing capabilities of the underlying CMA equipment operating system are enabled during installation. The following operations are recorded:

- Equipment configuration
- Equipment access
- File manipulation and account management
- Posting of any material to a repository
- Access to databases
- Any use of a signing key

Events related to the processing:

- Certificate generation requests – including sender DN, subject DN, and transaction ID
- Certificate revocation requests – including sender DN, issuer DN and serial number of certificate revoked, subject DN of certificate to revoke, revocation reason, transaction ID, and date of suspected compromise
- Responses - transaction ID, subject DN, and status of request

- User confirmation (certificate acceptance) – receipt transaction ID, subject DN, and method of confirmation
- Other actions - designation of IAs and RAs, execution of any IA and RA duties, CSAA authorizations, manual interactions with EEs, disclosure of information, access to databases, and CRL generation
- Publications - certificate and CRL publication to directory, and changes to CPS
- Re-key - new certificate mapped to the list of designated IAs and RAs
- Error conditions - anomalies, software integrity check failures, receipt of improper messages
- Physical access to, loading, zeroing, transferring keys to or from, backing-up, acquiring or destroying cryptographic modules
- Receipt, servicing, and shipping hardware cryptographic modules
- Any known or suspected violations of physical security, suspected or known attempts to attack the equipment via network attacks, equipment failures, power outages, network failures, or violations of this certificate policy
- Certificate generation requests – including subject DN and transaction ID
- CA responses - transaction ID, subject DN, and status of request
- Interactions with CA - CA compromise or re-key
- Documentation of receipt and acceptance of certificates

Events to be recorded by the RA and/or LRA:

- Authentication of user identity - copies of photo ID, verification of organizational affiliation, and any forms filled out by users
- Certificate revocation requests – including issuer DN and serial number of certificate revoked, subject DN of certificate to revoke, revocation reason, and transaction ID
- Certificate Change Status – including issuer DN and serial number of certificate changed, reason for change, and transaction ID
- Manual interactions with EEs - telephone or in person requests for revocation
- Documentation of receipt of tokens
- Any actions taken in association with cryptographic modules of subscribers who have left their organizations

Any actions taken during the processing of a request and generation of a response will be recorded. Many RA responsibilities require out-of-band activity.

Records of such activity will be recorded in a logbook or other physical medium. A record of any paper forms or copies of photo IDs collected from users will be maintained.

The following events applying to humans and physical operations are audited:

- Appointment of CAA, IA, RA and LRA personnel
- Training of CAA, IA, RA and LRA personnel
- Physical access to the CA, CSA and IA equipment
- Operator initiated actions, the identity of the equipment operator who initiated the action

5.4.2 Frequency of Processing Log

The system audit logs and personnel access logs are consolidated (summarized) and reviewed at a minimum on a monthly basis by the Corporate Security Auditor. As stated in the NFI CP, 25% of all of the security audit data is reviewed, at a minimum. IAs review RA audit logs. The audit logs are removed monthly to CDROM for archival purposes and to ensure that the security audit data is transferred prior to overwriting or overflow of automated security audit log files.

All significant events are documented. ORC documents actions taken resulting from significant events using Incident Report forms and Service Interruption forms.

5.4.3 Retention of Audit Log

The information generated on the CA, IA and CSA equipment is kept on the CA, IA and CSA equipment until the information is moved to an appropriate archive facility. The SA, at the direction of the Corporate Security Auditor, performs deletion of the audit log from the CA, IA and CSA equipment. Security audit data is retained on-site for at least two months. Audit and security logs are retained off-site as archive records in accordance with this CPS and are made available during compliance audits.

5.4.4 Protection of Audit Log

Audit logs are protected from unauthorized modification or unauthorized deletion. No person is authorized to modify the content of audit logs, except for appending new audit records without overwriting existing audit records. The action of two parties is required to protect the data, as described in this CPS, the Operating Procedures, and the Roles Manual. This two party control ensures that audit data cannot be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing and that no unauthorized user is able to write to, modify, or delete the archive.

5.4.5 Audit Log Backup Procedures

Audit logs are backed up along with the rest of the data on the CA, IA and CSA equipment, as described in this CPS, in addition to the weekly and monthly consolidation. Detailed procedures for creating, verifying, packaging, transmitting, and storing CA archive information is provided in the ORC System Security Plan.

5.4.6 Audit Collection System (Internal vs. External)

The ORC security audit process is independently controlled through the Corporate Security Auditor and the SA. The audit system is internal to CA, IA and CSA equipment and operates at the network, operating system and application level. Should it become apparent that an automated security audit system has failed, the ORC DAA will determine if ORC NFI will cease/suspend all operation except for revocation processing until the security audit capability can be restored. ORC will invoke the audit processes at system startup and will cease audit processes only at system shutdown. An entry is made in the </etc/system> file which invokes each of the commands listed in it at start up. The process itself is programmed such that breaks are disabled so it cannot be interrupted, so that the audit process will stay up compulsorily from start-up to shut-down. At no time does ORC operate the CA, IA or CSA without a functioning audit capability.

RA audit logs are manually collected. Signed e-mail requests received by an IA are maintained as electronic audit records. An IA archives their inbox to a CDROM (or Policy Authority approved media) on a monthly basis.

5.4.7 Notification to Event-Causing Subject

ORC does not necessarily notify an entity of an auditable event caused by that entity.

5.4.8 Vulnerability Assessment

SAs and other operating personnel are instructed to be watchful for attempts to violate the integrity of the CA, including the equipment, physical location, and personnel. The intrusion detection audit logs are checked at the end of each week for anomalies in support of any suspected violation.

ORC operates secure systems in accordance with FISMA security guidelines and undergoes independent audit of its operations.

5.5 Records Archival

5.5.1 Types of Events Archived

The ORC NFI archive records are kept with sufficient detail to establish the validity of a signature and of the proper operations. At a minimum, the following data are archived:

During system initialization:

- Self accreditation documentation
- This CPS, policies and procedures
- Any contractual agreements
- System and equipment configuration

During ORC NFI operation:

- Modifications or updates to any of the above data items
- Certificate status requests and responses
- Audit logs of all data identified in this CPS
- Security audit data
- Data or applications sufficient to verify archive contents
- Authorized CA accreditation
- Modifications and updates to system or configuration
- Certificate requests
- Revocation requests
- Subscriber Identity Authentication data as per Section 3.1.9
- Documentation of receipt and acceptance of certificates
- Export of private keys
- Documentation of loading, shipping, receipt and zeroizing of tokens
- All certificates issued or published
- All changes to the certificate profile
- All changes to the revocation profile
- All changes to the revocation list profile
- All changes to the trusted public keys

- Record of Authorized CA re-key
- All CRLs and CARLs/ issued and/or published
- All routine certificate validation transactions
- All audit logs
- Data or applications to verify archive contents
- All work related communications to or from the Policy Authority, and compliance auditors

5.5.2 Retention Period for Archive

Archived records are retained for ten (10) years and six months. Prior to the end of the archive retention period, ORC will provide archived data to a Policy Authority approved archival facility, upon request. ORC could itself own that facility.

5.5.3 Protection of Archive

No unauthorized users are able to write to, modify, or delete the archive. Applications required to process the archive data shall also be maintained, for a period determined by the ORC.

5.5.4 Archive Backup Procedures

Audit data is backed-up on a weekly basis. ORC creates a monthly archive backup of audit data for off-site storage labeled with the ORC NFI name and date, and stored in a separate off-site location.

5.5.5 Requirements for Time-Stamping of Records

Archive records are automatically time-stamped as they are created. ORC date/time stamps conform to the ITU-T Recommendation X.690 and the X.690 v2, Information Technology – ASN.1 Encoding Rules, 1994.

5.5.6 Archive Collection System

Consolidated audit logs are stored on the ORC CA equipment until copied to unalterable media (e.g., recordable CDROM (CDR)). Consolidated audit logs are moved monthly to unalterable media. The unalterable media are stored off-site in a secure location. Additional consolidated logs may be stored on the media without modifying previously stored audit logs.

5.5.7 Procedures to Obtain and Verify Archive Information

Archive data is obtained from the archive media by the Corporate Security Auditor only in response to a verified request for review of archived information.

5.6 Key Changeover

A self-signed ORC Government Root CA signs the ORC NFI CA certificates. This Root CA private key is used only to sign CA certificates, cross certificates, and CRLs. A new self-signed Root CA signing authority certificate will be issued to sign CA certificates when the validity period of the CA exceeds the remaining validity period of the Root CA. The old Root CA certificate continues to be used to sign CRLs until all CA certificates issued by that Root CA certificate have expired.

ORC uses a signing (private) key for creating certificates; however, Relying Parties employ the ORC NFI CA certificates for the life of the subscriber certificate beyond that signing. Therefore, the CA does not issue subscriber certificates that extend beyond the expiration dates of its own certificates and public keys, and the CA certificate validity period will extend one subscriber certificate validity period (listed in this CPS) past the last use of the CA private key. To minimize risk to the PKI through compromise of the CA key, the private signing key is changed more frequently, and only the new key is used for certificate signing purposes from that time forward. This is accomplished by setting up a new CA with a new signing key. The older, but still valid, certificate will be available to verify old signatures until all of the subscriber certificates signed under it have also expired. Since the old private key is used to sign CRLs that contain certificates signed with that key and OCSP responder certificates, the old key will be retained and protected. Key changeover is accomplished in accordance with Certificate Management Protocol [RFC4210].

The validity period of an ORC NFI CA signature certificate is 6 years. RA key lifetimes are as described for subscribers in this CPS.

Signature keys that have expired for the purposes of certificate signature may still be used for CRL signature.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Compromise or disaster notification and recovery procedures are employed by ORC to ensure a secure state. The security provided by the PKI is dependent on protection of the CA private keys. The CA keys are protected from compromise due to malicious attack or inadvertent loss of key/ activation data; as well as, from disasters causing the loss of essential equipment, by employing controls.

These measures minimize the risk of compromise due to use, storage, or knowledge of key activation mechanisms.

5.7.2 Entity (CA) Private Key Compromise Procedures

As required by the NFI MOA, ORC has in place an appropriate key compromise plan that addresses the procedures that are followed in the event of a compromise of the private signing key to issue certificates. This plan includes procedures for revoking all affected NFI Certificates and promptly notifying the Policy Authority, all subscribers and all Qualified Relying Parties.

In the case of an ORC NFI CA key compromise, the U.S. Government will immediately communicate the revocation of the ORC NFI certificate to relying parties. Subsequently, the CA installation will be re-established as described in ORC NFI Installation Manual. The ORC NFI CA will subsequently be re-keyed. The outstanding certificates will be re-issued using the new CA keys.

In case of an ORC CSA key compromise, the ORC CA that issued the CSA a certificate will revoke that CSA's certificate, and the revocation information will be published immediately in the most expedient manner. The ORC CSA is subsequently re-keyed. The ORC CSA does not use self-signed certificates.

5.7.3 Business Continuity Capabilities after a Disaster

ORC maintains a Disaster Recovery Plan (DRP) in accordance with guidelines provided by OMB Circular A-130, NIST SP 800-34, GSA Order 2100.1D, and all supporting GSA security guidelines.

The ORC NFI directory operates in a replicated configuration that is two or more platforms located at different sites that contain replicas of the directory information. In the event one fails, users are still able to obtain necessary information from the second directory server through a load balancer.

5.7.4 Customer Service Center

ORC NFI CAs maintain a Customer Service Center (Help Desk) to provide assistance and services to Subscribers and Relying Parties, and a system for receiving, recording, responding to, and reporting problems within ORC and for reporting such problems to FBCA. The ORC NFI CA ensures that there is a capability to provide help to users when a security incident occurs in the system.

5.8 CA or RA Termination

In the event that ORC ceases operation of its participation as an Authorized CA in NFI or is otherwise terminated:

- All subscribers, Sponsoring Organizations, and Qualified Relying Parties must be promptly notified of the cessation, via the NFI website.
- All NFI Certificates issued by ORC under this CPS will be revoked no later than the time of cessation
- All current and archived NFI identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data will be transferred to the Policy Authority within 24 hours of cessation and in accordance with this CPS. Transferred data will not include any non-NFI data

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1CA Key Pair Generation

ORC's CA certificate-signing keys are generated in FIPS 140-2 Level 3 validated cryptographic Hardware Security Modules (HSM). Subscriber Key Pair Generation

Users generate the key pair, as stipulated in Section 6.1.1.2. This is accomplished in a FIPS 140-2 Level 1 Approved Web browser (such as Netscape Communicator, Mozilla/ FireFox, etc.) for medium assurance certificates or in a FIPS 140-2 Level 2 validated hardware token for medium hardware assurance certificates.

6.1.1.2Subscriber Key Pair Generation

Subscribers are required to use a FIPS 140-2 validated cryptographic module for generation of keys. In the case of a Level 1 cryptographic module, the ORC NFI CAs perform a browser check prior to registration to ensure compliance against a list of FIPS 140-2 Level 1 browsers and upon submitting a registration request. ORC NFI CAs only allows compliant key pair generation. In the case of Level 2 tokens, required for medium hardware assurance certificates, key pair generation is accomplished with a Level 2-compliant token in the presence of an ORC RA or LRA, or other specifically assigned authority.

FPCPF PIV certificates the keys are generated and the certificates are issued on a PIV card via a GSA FIPS-201 approved Card Management System (CMS), refer to FIPS 201 Evaluation Program Approved Product List (http://fips201ep.cio.gov/apl.php).

6.1.2 Private Key Delivery to Subscriber

The ORC NFI subscriber’s private key is generated directly on the subscriber’s token, or in a key generator that benignly transfers the key to the subscriber’s token. The subscriber is in possession and control of the private key from the time of generation or benign transfer.

6.1.3 Public Key Delivery to Certificate Issuer

As part of the NFI Certificate application process, the subscriber’s public key is transferred to the ORC NFI CAs in a way that ensures:

- It has not been changed during transit
- The sender possesses the private key that corresponds to the transferred public key
- The sender of the public key is the legitimate user claimed in the certificate application

Public keys are delivered to the certificate issuer in a PKCS#10 or Certificate Request Message Format (CRMF) certificate request.

6.1.4 CA Public Key Delivery to Relying Parties

ORC supports delivery of the ORC NFI CA and trust anchor public keys (including the FPCPF trust anchor) via a web interface to a protected server using SSL. The public key is stored such that it is unalterable and not subject to substitution. Relying Parties must contact the help desk to receive the official certificate hashes to compare them with the certificates downloaded from the site.

In the case of the FPCPF trust anchor information will be provided to the certificate subject through one of the following secure processes (that will be identified in the sponsoring agencies RPS):

- ❑ Government RA provides the trust anchor to the certificate subject during in person identity proofing.
- ❑ Government RA provides a hash of the trust anchor information (a.k.a., a “fingerprint”) to the certificate subject during in-person identity proofing; the certificate subject downloads the trust anchor information from the ORC NFI website and verifies the “fingerprint”. The ORC NFI website includes instructions to the certificate subject on how to verify the “fingerprint”.
- ❑ The certificate subject obtains the trust anchor information from the ORC NFI website (or other Government sponsored web server) and calculates

the “fingerprint”. The ORC NFI website includes instructions to the certificate subject on how to calculate the “fingerprint”. The subject confirms the fingerprint against a value obtained through a secure independent process, such as a letter sent through first class mail from a Government RA or ORC RA.

6.1.5 Key Sizes

All FIPS-approved signature algorithms are in accordance with the ORC NFI CP.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters for use with the RSA algorithm defined in PKCS#-1 are generated and checked in accordance with PKCS#-1.

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

ORC certifies keys for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension. The key usage extension is included in all certificates and is always marked critical in order to limit the use of public key certificate for its intended purpose, as stipulated in the X.509 Certificate and CRL Extensions Profile for the FPCPF [FPKI-PROF].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [current version of FIPS140]. Cryptographic modules are validated to the FIPS 140 Level in accordance with FBCA requirements.

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

A single person is not permitted to activate an ORC CA signature key or access any cryptographic module containing a complete CA private signing key. See Section 5.2.1. Access to the CA signing keys backed up for disaster recovery is under the same multi-person control as the original CA signing key.

The CA and CSA private keys are controlled under a ‘n of m’ (two or more) person control.

Private encryption keys requested by other than the subscriber/PKI sponsor may only be extracted from key recovery databases under two-person control, as described in the ORC KRPS. The names of the parties used for two-person control are maintained on a list that is made available for inspection during compliance audits.

6.2.3 Private Key Escrow

Under no circumstances is an ORC CA signature key used to sign certificates or CRLs escrowed.

Under no circumstances will a signature key be escrowed. ORC does not require private key escrow for confidentiality keys. However, ORC recommends to EEs that they locally escrow a copy of the confidentiality private key.

For some purposes (such as data recovery), some organizations may desire key archival and key retrieval for the private component of the encryption certificate key pair. To facilitate this, ORC offers a key escrow and recovery capability.

The method, procedures and controls which apply to the storage, request for, extraction and/or retrieval, delivery, protection and destruction of the requested copy of an escrowed key are described in the ORC KRPS.

6.2.4 Private Key Backup

6.2.4.1Backup of CA Private Signature Key

ORC may back up the CA private key on a separate cryptographic module in order to alleviate the need to re-key in the case of cryptographic module failure. The backup module is an HSM that meets FIPS 140 Level 3 requirements and Level 3 key management requirements. The module is under the protection of the CAA and the SA under lock and key at all times, in accordance with this CPS. When ORC re-keys, the private key in the backup module is zeroed or otherwise destroyed.

6.2.4.2Backup of Subscriber Private Signature Key

ORC recommends to users that they make backup copies of software based encryption private keys and provides recommended procedures on the NFI website. Backup of private signature keys for the sole purpose of key recovery will not be made. Backup copies are stored in an encrypted form and protected by a password from unauthorized access. The subscriber (PKI Sponsor for Component) is responsible for ensuring that all copies of private keys, including those that might be embedded in component backups, are protected. This includes protecting any workstation on which any of its private keys reside.

In the case of individual subscriber certificates on a smart card asserting a FPCPF OID, private signing keys are generated on the smart card (PIV) and are not backed up.

6.2.4.3Backup of Subscriber Private Key Management Key

Subscribers are permitted to backup their own private keys. Backed up subscriber private key management keys may not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.4Backup of CSS Private Key

CS*A* private keys may be backed up. When backed up, all copies *are* accounted for and protected in the same manner as the original.

6.2.4.5Backup of PIV-I Content Signing Key

At present, ORC does not back-up Content Signing private signature keys. In the future, should back-up of Content Signing private keys become standard practice, the backup procedure will require multi-person control.

6.2.5 Private Key Archival

Under no circumstances is a non-repudiation signature or authentication key archived. Archival of confidentiality keys is recommended if any information encrypted with those keys is archived in its encrypted state.

Escrowed keys are stored in a protected KED, in accordance with the ORC KRPS. The KED consists of equipment dedicated to the key recovery and archival functions.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys are generated by and in a cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140.

6.2.8 Method of Activating Private Key

A password will be used to activate the private key for subscriber medium assurance and medium hardware assurance (e.g. PIV). Passwords will be generated by the subscriber and entered at the time of key generation (at the RA/LRA workstation in the case of medium hardware assurance) and managed according to the FIPS 140-2 guidance for strong passwords in accordance with the subscriber obligation agreement. Entry of activation data will be protected from disclosure. The strength of the passwords and the controls used to limit guessing attacks will have a probability of success of less than 2-23 chance (1 chance in 8,338,608) of success over the life of the password. ORC uses the

NIST E-Authentication Token Strength Module (TSM) to calculate resistance to online guessing. The strength of password will be at least eight (8) characters with the following diversity: one upper case alpha, one lower case alpha, one numeric, and one special.

6.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated will not be left unattended or otherwise available to unauthorized access. Private keys stored in hardware tokens, excluding end user tokens, will be removed from the token reader and stored in a locked container when not in use. End users will protect his or her token in accordance with the subscriber obligation agreement. The CA hardware token will be stored in a locked container when not in use.

Private keys stored in software will be deactivated via a logout procedure. End entities will be advised to also implement a time-out procedure for automatically deactivating private keys after a period of 15 minutes of non-use.

6.2.10 Method of Destroying Private Key

Private signature keys will be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, is accomplished by overwriting the data. For hardware cryptographic modules, this is accomplished by executing a “zero” command. Physical destruction of hardware should not be required. Destruction of the private signature key is then documented via signed email.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Archival of public keys is achieved via certificate archival.

6.3.2 Certificate Operational Periods and Key Usage Periods

The maximum validity period of an ORC NFI CA signature certificate is 6 years. RA key lifetimes are as described for subscribers in this CPS.

The validity period of an ORC NFI end entity certificate is 3 years, with a maximum of 2 renewals before requiring re-key.

The maximum validity period of an ORC CA signature certificate asserting a FPCPF OID is 6 years. RA key lifetimes are as described for subscribers in this CPS.

Certificates issued to end entities by an ORC CA asserting a FPCPF OID have a maximum validity period of three years. In no case will ORC renew certificates issued asserting the FPCPF OIDs.

The ORC Certificate Status Authority (CSA) is the Certificate Status Server (CSS) that provides revocation status for all ORC issued certificates. The signing certificates for ORC's CSA are issued with a certificate validity period of 31 days.

6.3.3 Restrictions on CA Private Key Usage

The private key used by ORC NFI CAs for issuing NFI Certificates is used only for signing such Certificates and, optionally, CRLs or other validation services responses.

A private key held by a CMA, if any, and used for purposes of manufacturing ORC NFI Certificates is considered the ORC NFI CA's signing key, is held by the CMA as a fiduciary, and is not used by the CMA for any other purposes, except as agreed by ORC. Any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of ORC.

The private key used by each RA employed by an ORC in connection with the issuance of ORC NFI Certificates is used only for communications relating to the approval, issuance, or revocation of such certificates.

Under no circumstances will the ORC NFI CA signature keys used to support non-repudiation services be escrowed by a third party.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Subscribers will sign and return a subscriber advisory statement to help understand responsibilities for the use and control of the cryptographic module. Not all software currently available allows for technically enforced password expiration. Activation data (password or pass-phrase) is generated by the subscriber in accordance with the stipulations of the subscriber's agreement.

ORC does not support transport of activation data.

6.4.2 Activation Data Protection

Cryptographic modules are used to protect activation data and critical security parameters in accordance with FIPS 140-2 requirements.

The subscribers will protect their activation data from access by others, in accordance with the subscriber's agreement. If the activation data is not entered directly in the cryptographic module, procedures or protocols will be used so that the activation data is protected against eavesdropping and replay. Examples of protocol are encrypting the data with a new random session key each time, and challenge response.

6.4.3 Other Aspects of Activation Data

If during the life of the PIV-I card the card becomes locked due to failed PIN attempts, the PIN may be reset. To complete a PIN reset the cardholder must appear in-person to the PCI Facility and perform a 1:1 biometric match of the PIV cardholder against the biometric included in the PIV card prior to releasing the unlocked PIV/PIV-I card back to the cardholder. This biometric 1:1 match can only be conducted by a trusted agent of the Card Management System.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Upon establishment and periodically thereafter, the most current DoD system security audit script are run on the ORC PKI infrastructure.

6.5.2 Computer Security Rating

ORC equipment meets and is operated at U.K. Information Technology Security Evaluation and Certification E2/F-C2 rating. This equates with C2 in the U.S. TCSEC / Orange Book. ORC equipment operating at C2 implement discretionary access control, object reuse controls, individual identification and authentication, and a protected audit record.

The ORC CA software is evaluated at Common Criteria Evaluation Assurance Level (EAL) 4.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Individuals filling trusted roles within the ORC facility use security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements that check the integrity of the system data, software, discretionary access controls, audit profiles, firmware, and hardware to ensure secure operation.

6.6.2 Security Management Controls

All ORC PKI system security features described in this CPS are configured and enabled. The configuration of the ORC NFI system (including hardware, software, and operating system) as well as any modifications and upgrades are documented and controlled with mechanisms for detecting unauthorized modification to the software or configuration.

6.6.3 Object Reuse

Procedures for sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media) and controlled storage, handling, or destruction of spoiled media, or media that cannot be effectively sanitized for reuse are documented in ORC's Policies and Procedures, and ORC's System Security Plan.

6.6.4 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

Access to the CA data is protected.

Network security controls for LRA equipment are the responsibility of the LRA's organization, whether the LRA is an employee of ORC or another organization. The PKI Sponsor will ensure that the LRA equipment is protected, as specified in the U.S. Government CA CP for CMA equipment. Where practical, the subscriber's organization will only allow services to and from LRA equipment limited to those required to perform LRA functions. However, additional services consistent with the organization's policy may be enabled. Protection will be provided against known network attacks. All unused network ports and services will be turned off. Any network software present on LRA equipment will be necessary to the LRA function. Boundary control devices used to protect LRA equipment will deny all but necessary services to the LRA equipment even if those services are enabled for devices on the network. Firewall will meet the security functional requirements as specified in the DoD for medium robustness Firewall Protection Profile [FWPP]. Boundary control devices will include an Intrusion Detection capability that meets the security functional requirements as specified in the Intrusion Detection System Protection Profile [IDSPP]. The PKI Sponsor will certify compliance with these requirements, in writing to the ORC Corporate Security Auditor, prior to approval of performing LRA functions and will certify compliance with these requirements, in writing to the ORC Corporate Security Auditor, annually.

6.8 Time-Stamping

ORC date/time stamps conform to the ITU-T Recommendation X.690 and the X.690 v2, Information Technology – ASN.1 Encoding Rules, 1994. Asserted times are accurate to within three minutes. Clock adjustments are auditable events.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

ORC NFI Certificates contain public keys used for authenticating the sender and receiver of an electronic message and verifying the integrity of such messages, i.e., public keys used for digital signature verification.

ORC creates and maintains NFI Certificates that conform to the ITU-T Recommendation X.509, "The Directory: Authentication Framework," June 1997.

All ORC NFI Certificates include a reference to an OID for this CPS within the appropriate field, and contain the required certificate fields according to this CPS and the GSA NFI MOA.

Complete certificate profile information, including key generation methods, for ORC certificates can be found in the X.509 Certificate and CRL Extensions Profile for the Common Policy [CCP-PROF] and the applicable ORC CA build document.

7.1.1 Version Number(s)

ORC issues X.509 v3 NFI certificates (populate version field with integer 2).

7.1.2 Certificate Extensions

ORC NFI certificate profiles are in accordance with the requirements of the certificate profiles described in the NFI CP and the applicable ORC CA build document. In the case of certificates issued under this CPS and asserting a FPCPF OID, profiles are in accordance with the requirements of the certificate profiles described in the X.509 Certificate and CRL Extensions Profile for the FPCPF [FPKI-PROF] and the applicable ORC CA build document.

Access control information may be carried in the subjectDirectoryAttributes non-critical extension. The syntax is defined in detail in [SDN702].

7.1.3 Algorithm Object Identifiers

Certificates issued by ORC CAs use the following OIDs for signatures.

id-dsa-with-sha1	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3 }
sha-1WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

ORC does not implement RSA with PSS padding.

Certificates issued under this CP shall use the following OIDs to identify the algorithm associated with the subject key.

id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }
RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
Dhpublicnumber	{ iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1 }

id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }

Where a certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip192r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }
ansit163k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 1 }
ansit163r2	{ iso(1) identified-organization(3) certicom(132) curve(0) 15 }
ansip224r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 33 }
ansit233k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 26 }
ansit233r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 27 }
ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
ansit283k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 16 }
ansit283r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 17 }
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }
ansit409k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 36 }
ansit409r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 37 }
ansip521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }
ansit571k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 38 }
ansit571r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 39 }

7.1.4 Name Forms

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280.

The subject alternative name extension shall be present and include a PIV-I FASC-N [or equivalent] name type in certificates issued under id-orc-nfissp-pivi-hardware and id-orc-nfissp-pivi-cardAuth.

7.1.5 Certificate Policy Object Identifiers

Certificates issued by the ORC CAs assert the OID appropriate to the level of assurance with which it was issued, as defined in Section 4.3.

7.1.6 Usage of Policy Constraints Extension

No Stipulation, unless cross-certification policy stipulates use of policy constraints.

7.1.7 Policy Qualifiers Syntax and Semantics

The certificates issued under this CPS will not contain policy qualifiers.

7.1.8 Processing Semantics for the Critical Certificate Policies Extension

ORC does not set the certificate policies extension to be critical. Relying Parties whose client software does not process this extension operate in this regard at their own risk. Processing semantics for the critical certificate policy extension used by ORC conforms to [FPKI-PROF] and [CCP-PROF].

7.2 CRL Profile

ORC CRL profiles addressing the use of each extension are provided in and conform to the X.509 Certificate and CRL Extensions Profile for the FPCPF [CCP-PROF] and the applicable ORC CA build document.

7.2.1 Version Number(s)

CRLs issued under this CPS assert a version number as described in the X.509 standard [ISO9594-8]. CRLs assert Version 2.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are available and described in the X.509 Certificate and CRL Extensions Profile for the FPCPF [CCP-PROF] and are in accordance with the NFI CP CRL profile. The CA supports CRL Distribution Points (CRL DP) in all EE certificates. The CRL DP is as follows:

ldap://orc-ds.orc.com/cn=ORC NFI <CA Name>, o=ORC PKI, c=US?certificateRevocationList;binary

http://crl-server.orc.com/CRLs/<CA Name>.crl

In the case of subordinate CAs:

ldap://orc-ds.orc.com/cn=<ORC Root>, o=ORC PKI, c=US?certificateRevocationList;binary

http://crl-server.orc.com/CRLs/<ORC Root>.crl

7.3 OCSP Profile

OCSP requests are not required to be signed (refer to RFC2560 for detailed syntax). OCSP requests and responses contain the following formats.

Field	Expected Value
Version	V1 (0)
Requester Name	Not Required
Request List	List of certificates – generally this should be the list of two certificates: ORC certificate and end entity certificate
Signature	Not Required
Extensions	Not Required

OCSP Request Format

The following table lists which fields are populated by an ORC OCSP Responder:

Field	Expected Value
Response Status	Successful | Malformed Request | Internal Error | Try Later
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Hash of Responder public key
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status[2], thisUpdate, nextUpdate[3],
Extension	
Nonce	Will be present if nonce extension is present in the request
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Signature	Present
Certificates	Applicable certificates issued to the OCSP Responder

OCSP Response Format

[2] If the certificate is revoked, the OCSP Responder will provide revocation time and revocation reason from CRL entry and CRL entry extension.

[3] The OCSP Responder will use thisUpdate and nextUpdate from CA CRL.

7.3.1 Version Number(s)

The Certificate Status Authority operated under this CPS uses OCSP version 1.

7.3.2 OCSP Extensions

Critical OCSP extensions are not used.

8 Compliance Audit and Other Assessments

ORC conducts an compliance audits to ensure that the requirements of this CPS are being implemented and enforced.

8.1 Frequency of Audit or Assessment

The ORC NFI systems are periodically independently audited for conformance to the appropriate policies and procedures.

Security controls are reviewed and updated accordingly on an annual basis for the purpose of determining the extent to which controls are correctly implemented and operating, and meeting the system's security needs.

The completion of the most recent security assessment is cited in the ORC System Security Plan.

8.2 Identity/ Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CPS and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. ORC contracts qualified external auditor(s) and budgets for C&A, annual audits, and any additional auditing requirements as part of each year's fiscal planning. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

A certified IT auditing firm (approved by the NFI PMO) audits ORC annually, in accordance with industry best practices for compliance (e.g.FISMA). ORC is also audited aperiodically by: GSA, DoD and NSA. ORC has an independent internal department that performs weekly procedures in order to attest to ORC's compliance with this CPS. Audit and inspection is accomplished in accordance with the NIST SP 800-53 or current industry accepted standards and practices.

8.3 Assessor’s Relationship to Assessed Entity

The compliance auditor either will be a private firm that is independent from the entities (CA and RAs) being audited, or it will be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity’s CA Facility or certificate practices statement. The FPKIPA will determine whether a compliance auditor meets this requirement.

The Organization/Agency PMA is responsible for identifying and engaging a qualified auditor of organization/agency operations implementing aspects of this CP.

ORC relies upon the combined efforts of an independent external IT auditor, which is an entity separate from ORC, and an internal audit capability that is sufficiently organizationally separated from those entities operating the CA, so as to provide an unbiased, independent evaluation. ORC performs internal audits of NFI CSA, IA, RA and LRA facilities, conducted by a Corporate Security Auditor, as defined herein.

8.4 Topics Covered by Assessment

The purpose of ORC NFI compliance audits is to verify that ORC and its recognized trusted roles comply with all the requirements of the current versions of the CP and this CPS. All aspects of the ORC NFI operation are subject to compliance audit inspections.

8.5 Actions Taken as a Result of Deficiency

When a compliance auditor finds a discrepancy between an ORC CMA’s operation and the stipulations of this CPS, the following actions will occur:

- The compliance auditor will note the discrepancy
- The compliance auditor will notify the parties identified in Section 8.6 of the discrepancy
- ORC will propose a remedy, including expected time for completion, to the NFI Program Office.

Any remedy may include permanent or temporary ORC NFI cessation or termination of ORC NFI accreditation. However, several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes, and the disruption to the certificate using community.

Remedies will be defined by the NFI Program Office and communicated to ORC as soon as possible to limit the risks created. The NFI Program Office and ORC will determine a time for completion. The implementation of remedies will be coordinated between the NFI Program Office and ORC and subsequently communicated to the appropriate authority. A special audit may be required to confirm the implementation and effectiveness of the remedy.

Subsequent to the ORC NFI being granted Authorization to Operate (ATO), which is primarily based upon a Certification and Accreditation (C&A) review performed by an external auditor, the C&A process will be performed every three years. Results of the initial C&A and all subsequent C&A reviews will be made available to FBCA, to be used in determining the CA's suitability for initial and continued performance as a cross-certified CA.

8.6 Communication of Results

The results of any inspection or audit will be communicated, in whole, to ORC and to the NFI Program Office by the auditor. Required remedies will be defined and communicated to ORC as soon as possible to limit the risks created. The implementation of remedies will be communicated to the appropriate authority. A special audit may be required to confirm the implementation and effectiveness of the remedy.

If a CMA entity is found not to be in compliance with this CPS, or the policy identified in the NFI CP, ORC will notify the NFI Program Office immediately upon completion of the audit.

9 Other Business and Legal Matters

9.1 Fees

All fees are set in accordance with the terms of the ORC NFI MOA. Fees are published on the ORC website or established contractually. Fees are published at http://NFI.orc.com and may change with a 7-day notice.

9.1.1 Certificate Issuance or Renewal Fees

A fee per validity year, unless otherwise negotiated, is levied by ORC to issue Identity and Encryption certificates. A fee per year, unless otherwise negotiated, is levied by ORC to issue Server and Code Signer certificates. Likewise, a fee per each additional year, unless otherwise negotiated, is levied by ORC to renew an ORC NFI certificate. A fee per encryption certificate is levied for the escrowing of encryption keys.

A fee, unless otherwise negotiated, is levied by ORC for the replacement of certificates and or tokens when the subscriber's private key has not been compromised and there are no changes to the certificate.

Fees for tokens are separate from Certificate Issuance, Renewal, and Replacement Fees.

9.1.2 Certificate Access Fees

ORC does not impose any certificate access fees on subscribers with respect to its own NFI Certificate(s) or the status of such Certificate(s). No fee is levied by ORC for access to information about any certificate issued by the ORC that is requested under a court order. ORC assesses a fee from subscribers and Relying Parties for recovering archived certificates.

9.1.3 Revocation or Status Information Access Fees

Fees may be assessed for certificate validation services as set forth in the Authorized ORC-GSA NFI MOA. ORC CSA services are priced separate from certificate issuance services, on a transaction and subscription basis.

9.1.4 Fees for other Services

No fee is levied for online access to policy information. A reasonable fee to cover media reproduction and distribution costs may be levied for a physical media copy of this policy information. A consulting fee per hour is levied for certificate support required in addition to the detailed instructions delivered with the notification of subscriber certificate issuance. This additional support includes documentation, telephone and on-site support.

9.1.5 Refund Policy

Refunds may be negotiated on a case-by-case basis.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

CA information not requiring protection is made publicly available. Public access to organizational information, as determined by ORC and the respective organization, is provided via means determined by ORC and the respective organization.

9.3.1 Scope of Confidential Information

Authorized ORC NFI CAs take steps to protect the confidentiality of any ORC, Relying Party, Subscriber, or other Government information provided to the Authorized ORC NFI CA. These steps include vetting of personnel placed in trusted roles; protection of confidential data in transit and while at rest; physical and logical controls; archive protection; all of which are described throughout this CPS. Such information is used only for the purpose of providing Authorized ORC NFI CA Services and carrying out the provisions of this CPS, and are not disclosed in any manner to any person except as may be necessary for the performance of the Authorized ORC NFI CA Services in accordance with the this CPS and any existing MOA(s).

9.3.2 Information not within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

The ORC NFI takes steps, as required, to protect the confidentiality of any Relying Party, Subscriber, or other Government information provided to the ORC NFI CA. Such information is used only for the purpose of providing ORC NFI CA Services and carrying out the provisions of the ORC NFI Certificate Policy, and is not disclosed in any manner to any person except as may be necessary for the performance of the ORC NFI CA Services in accordance with the ORC NFI CP.

9.4 PRIVACY OF PERSONAL INFORMATION

Relying Party, Subscriber, and Government information provided to the ORC NFI CA shall be used only for the purpose of providing ORC NFI CA Services and carrying out the provisions of this CPS and the ORC NFI CP, and shall not be disclosed in any manner to any person except as may be necessary for the performance of the ORC NFI CA Services in accordance with this CPS and the ORC NFI CP.

9.4.1 Privacy Plan

ORC protects all subscriber identifying information. All Subscriber identifying information will be maintained in accordance with applicable laws.

9.4.2 Information Treated as Private

Information requested from individuals during the certificate issuance process other than that information, which is specifically included in the certificate, is withheld from release. This information may include personal information as described in Section 3.1 and is subject to the Privacy Act. All information in the ORC NFI record (not repository) is handled as SBU, and access will be restricted to those with official needs.

Certificate private keys are considered sensitive and access will be restricted to the certificate owner, except as stipulated in the ORC KRPS. Private keys held by the ORC NFI will be held in strictest confidence. Under no circumstances will any private key appear unencrypted outside the ORC NFI hardware. Private keys held by the ORC NFI will be released only to a trusted authority in accordance with this CPS, or law enforcement official, in accordance with U.S. law, the NFI CP, and this CPS (see Section 2.8.2).

Audit logs and transaction records as a whole are considered sensitive and will not be made available publicly.

9.4.3 Information not Deemed Private

No sensitive information will be held in certificates, as certificate information is publicly available in repositories. Information not considered sensitive includes the subscriber’s name, electronic mail address, certificate public key, and certificate validity period.

9.4.4 Responsibility to Protect Private Information

ORC will not disclose certificate-related information to any third party unless authorized by the NFI Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. ORC will authenticate any request for release of information. This does not prevent ORC from disclosing the certificate and certificate status information (e.g., CRL, OCSP Requests and Responses, etc.).

9.4.5 Notice and Consent to Use Private Information

All notices will be in accordance with the applicable laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Sensitive data will be released to law enforcement officials only under a proper court order. The ORC NFI will not disclose certificate or certificate-related information to any third party unless expressly authorized by the NFI CP, required by criminal law, government rule or regulation, or order of a criminal court with jurisdiction. ORC NFI will authenticate such requests prior to disclosure. External requests must be made via the subscriber's organization, unless under court order.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

Unless otherwise agreed, property interests in the following security-related information materials and data are regarded as the property of the parties indicated below:

- Certificates and CRLs are the personal property of ORC. Permission is granted to reproduce and distribute certificates issued by the ORC NFI on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Certificates and CRLs will not be published in any publicly accessible repository or directory without the express written permission of ORC
- This CPS is the sole property of Operational Research Consultants, Inc.
- Private keys are the personal property of the subscribers who rightfully use or are capable of using them (or their employer or principal), regardless of the physical medium within which they are stored and protected
- Public keys are the personal property of subscribers (or their employer or principal), regardless of the physical medium within which they are stored and protected
- ORC NFI Certificates, including ORC NFI public keys, are the property of ORC. ORC licenses relying parties to use such keys only in conjunction with FIPS 140-2 validated encryption modules

Distinguished names are the property of the individuals named or their employer

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

ORC warrants that its procedures are implemented in accordance with this CPS, and that any issued certificates that assert the policy OIDs identified in Section 1.2, are issued in accordance with the stipulations of this CPS. ORC warrants that CRLs issued and keys generated by ORC are in conformance with this CPS.

ORC warrants that any IA, RA, LRA, Code Signer Certificate Subscriber or designated authority will operate in accordance with the applicable sections of this CPS.

Subscriber (applicant) organizations that authorize and employ PKI Sponsor(s), CSAA(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) warrant that:

- The PKI Sponsor(s), CSAA(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) procedures are implemented in accordance with the NFI CP and this CPS
- All PKI Sponsor(s), CSAA(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) actions are accomplished in accordance with this CPS
- The PKI Sponsor(s), CSAA(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) operate in accordance with the applicable sections of this CPS
- The PKI Sponsor(s), CSAA(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) meet the personnel and training requirements stipulated in this CPS
- The applicant organization will cooperate and assist ORC in monitoring and auditing that authorized the PKI Sponsor(s), CSAA(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) are operating in accordance with the applicable sections of this CPS
- Network security controls to the PKI Sponsor(s), CSAA(s), LRA(s) and/ or Code Signer Certificate Subscriber(s) equipment are in accordance with the applicable sections of this CPS

ORC does not warrant the actions of Notaries Public or other persons legally empowered to witness and certify the validity of documents and to take affidavits and depositions, as stipulated by the NFI Program Office.

9.6.2 RA Representations and Warranties

RAs are obligated to accurately represent the information prepared for the ORC NFI and to process requests and responses in a timely and secure manner. RAs may designate LRAs, however LRAs may not designate other LRAs under this

CPS. RAs under this CPS are not authorized to assume any other NFI administration functions.

When validating subscriber requests for certificates issued under this CPS, an RA accepts the following obligations:

- To validate the accuracy of all information contained in the subscriber’s certificate request
- To validate that the named subscriber actually requested the certificate
- To verify to the IA that the certificate request originated from the named subscriber and that the information contained in the certificate request is accurate
- To use the RA certificate only for purposes associated with the RA function
- To use private keys only on the machines that are protected and managed using commercial best practices.
- To request revocation and verify reissue requirements of a subscriber’s certificate upon notification of changes to information contained in the certificate
- To request revocation of the certificates of Subscribers found to have acted in a manner counter to Subscriber obligations
- To inform subscribers and the IA of any changes in the RAs status
- To protect the RA certificate private keys from unauthorized access
- To immediately revoke their own RA certificate and report to the IA if private key compromise is suspected
- To ensure that obligations are imposed on Subscribers in accordance with Section 2.1.6
- To inform Subscribers of the consequences of not complying with those obligations
- An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

9.6.3 Subscriber Representations and Warranties

When requesting and using a certificate issued under this CPS, a subscriber accepts the following obligations:

- To accurately represent themselves in all communications with ORC and the PKI

- To protect the certificate private key from unauthorized access in accordance with Section 6.2, as stipulated in their certificate acceptance agreements, and local procedures
- To immediately report to an RA or LRA and request certificate revocation if private key compromise is suspected
- To use the certificate only for authorized applications which have met the requirements of the NFI CP and this CPS
- To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension
- To use private keys only on the machines that are protected and managed using commercial best practices.
- To report any changes to information contained in the certificate to the appropriate RA or LRA for certificate reissue processing
- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates
- These obligations are provided to the Subscriber during the registration process in the form of a Subscriber Agreement that the Subscriber must read and agree to prior to completing registration. Theft, compromise or misuse of the private key may cause the Subscriber, Relying Party and their organization legal consequences.

9.6.4 Relying Party Representations and Warranties

ORC will publicly post a summary of this CPS on the ORC NFI website (NFI.orc.com) to provide the relying party information regarding the expectation of the ORC NFI. When accepting a certificate issued under this CPS, a relying party accepts the following obligations:

- Perform a risk analysis to decide whether the level of assurance provided by the certificate is adequate to protect the Relying Party based upon the intended use
- To ensure that the certificate is being used for an appropriate approved purpose
- To check for certificate revocation prior to reliance
- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension)
- To verify the digital signature of the ORC NFI who issued the certificate they are about to rely on as stipulated in the NFI CP

- To establish trust in the ORC NFI who issued the certificate by verifying the chain of CA certificates starting from a trust anchor of the relying party in accordance with the guidelines set by the X.509 Version 3 Amendment (for ORC NFI, this trust anchor will be the NFI Root CA with no additional chaining)
- To acknowledge all warranty and liability limitations
- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data
- To abide by all the terms, conditions and restrictions levied upon the use of the issued private key(s) and certificate(s) as stipulated in the NFI CP
- Note: Data format changes associated with application upgrades may invalidate digital signatures and will be avoided
- Relying parties that do not abide by these obligations assume all risks associated with the certificates upon which they are relying
- Check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance

9.6.5 Representations and Warranties of Other Participants

9.6.5.1Repository Representations and Warranties

ORC warrants that the ORC NFI procedures are implemented in accordance with this CPS and the NFI CP, and that any certificates issued that assert the policy OIDs identified in this CPS are issued in accordance with the stipulations of the NFI CP.

ORC warrants that ORC RAs or Trusted Agents operate in accordance with the applicable sections of this CPS and the NFI CP.

ORC posts NFI certificates and CRL information in an LDAP enabled directory established by the ORC NFI. Only information contained in the certificate will be posted in this directory to ensure compliance with the Privacy Act. Access is available via an interoperable implementation of the LDAP, with certificate storage accomplished for the sub-tree identified by the organizational unit (ou) identifier, ou=ORC. Access is also available via Hypertext Transfer Protocol (HTTP) through a directory gateway interface. The ORC NFI directory sub-tree identifies the identifier ou=ORC. The ORC NFI directory gateway is located at:

https://NFI.orc.com/dsgw/bin/csearch?context=dsgw.

The certificate repository meets the following obligations:

- To list all un-expired certificates for the ORC NFI to relying parties
- To contain an accurate and current CRL for the ORC NFI for use by relying parties
- To be publicly accessible through a web server gateway using HTTPS and FIPS 140-2 approved encryption
- To be physically accessible, via certificate authenticated access control over SSL, for authorized requests coordinated with the CA point of contact during normal business hours for the operating organization
- To be maintained in accordance with the practices specified in this CPS
- To meet or exceed the requirement of 99% availability for all components within the control of the operating organization NOTE: Communication failures as a result of Internet problems external to the operating organization will not count against this availability requirement.

ORC maintains a copy of at least all certificates and CRLs it issues and provides this information to the US Government for archiving. ORC provides this information on a certificate accessed web server posted no later than 10 days after the end of the collection of the data. If desired, the archive information can be delivered to the US Government on CDROM or other NFI Program Office approved media.

9.6.5.2Trusted Agent Representations and Warranties

Trusted Agents will perform Subscriber identity verification in accordance with this CPS and in accordance with the NFI CP.

9.7 Disclaimers of Warranties

Without limiting other subscriber obligations stated in this CPS, all subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures with the certificate, reasonably rely on the representations contained therein.

ORC disclaims all warranties and obligations of any type other than those listed.

9.8 Limitations of Liability

9.8.1 Loss Limitation

ORC disclaims any liability for loss due to use of certificates issued by the ORC NFI provided that the certificate was issued in accordance with the NFI CP and this CPS and that the relying party has used validation information that complies with the NFI CP and this CPS. ORC acknowledges professional liability with respect to the ORC NFI, ORC CMAs and/ or the ORC RAs and ORC LRAs.

The limit for losses per transaction due to improper actions by the ORC NFI or and ORC CMA is limited to $1,000 (U.S. Dollars). The limit for losses per incident due to improper actions by the ORC NFI or an ORC CMA is $1 million (U.S. Dollars).

9.8.2 Other Exclusions

Certificate applicants and Subscribers signify and guarantee that their application does not interfere with or infringe upon the rights of any others regarding their trademarks, trade names or any other intellectual property. Certificate applicants and subscribers will hold ORC harmless for any losses resulting from any such act.

As a result of issuing a certificate that identifies a person as an employee or member of an organization, ORC does not represent that the individual has authority to act for that organization.

9.8.3 U.S. Federal Government Liability

In accordance with the NFI CP Subscribers and Relying Parties will have no claim against the US Federal Government arising from use of the Subscriber’s certificate or an ORC NFI CMA determination to terminate (revoke) a certificate. In no event will the Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued or revoked by the ORC NFI under this CPS.

ORC will have no claim for loss against the NFI Program Office, including but not limited to the revocation of the ORC NFI certificate.

Subscribers and Relying Parties will have no claim against the US Federal Government arising from erroneous certificate status information provided by the servers and services operated by the ORC NFI, CSA, and by the US Federal Government.

9.9 Indemnities

Agents of the ORC NFI (e.g., RA, Trusted Agents, etc.) assume no financial responsibility for improperly used certificates.

9.10 Term and Termination

9.10.1 Term

This CPS will remain in effect until the NFI Program Office approves a new NFI CP, an updated ORC NFI CPS supplants this CPS, or the NFI PKI is terminated.

9.10.2 Termination

This CPS will survive any termination of the CA. The requirements of this CPS remain in effect through the end of the archive period for the last certificate issued.

9.10.3 Effect of Termination and Survival

The responsibilities for protecting business confidential and personal information, and for protecting the Government's intellectual property rights will survive termination of this CPS.

Intellectual property rights will survive this CPS, in accordance with the IP laws of the United States.

9.11 Individual Notices and Communications with Participants

ORC will use commercially reasonable methods to communicate with all parties.

9.12 Amendments

9.12.1 Procedure for Amendment

The NFI Program Office will review the NFI CP at least once every year. Corrections, updates, or changes to the CP will be publicly available. Suggested changes to the CP will be communicated to the contact in section 1.5.2; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.1.1 CPS and External Approval Procedures

The NFI Program Office will make the determination that this CPS complies with the policy identified in Section 1.2.

9.12.2 Notification Mechanism and Period

ORC will publish information (including this CPS with sensitive data redacted) on a web site.

9.12.3 Circumstances Under Which OID Must be Changed

The policy OID will only change if the change in the CP results in a material change to the trust by the relying parties.

9.13 Dispute Resolution Provisions

The NFI Program Office will be the sole arbiter of disputes over the interpretation or applicability of the NFI CP.

With respect to Subscriber or Relying Party Agreements or Obligations made by an entity by purchasing the services associated with this CPS an attempt will be made to resolve any dispute through an independent mediator, mutually agreed to by all disputing parties. If mediation is unsuccessful in resolving such a dispute, it will be resolved by arbitration in accordance with applicable statutes.

9.14 Governing Law

The laws of the United States of America will govern the enforceability, construction, interpretation, and validity of this CPS with respect to the NFI CP and the schedule operated by ORC (the NFI provider) under the GSA Federal Supply Schedule (FSS).

With respect to Subscriber or Relying Party Agreements or Obligations made by a US Government entity by purchasing the services associated with this CPS, Agreement and interpretation will be governed by the Contracts Disputes Act of 1978 as amended (codified at 41 U.S.C. section 601). If the individuals or organizations purchasing the services associated with this CPS are not within the jurisdiction of the US Government, the laws of the Commonwealth of Virginia will apply.

Various laws and regulations may apply, based on the jurisdiction in which a certificate is issued or used. It is the responsibility of the certificate holder, or user, to ensure that all applicable laws and regulations are adhered to.

9.15 Compliance with Applicable Law

Operation of the ORC CA(s) are required to comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

All contracts negotiated, for the purpose of providing ORC NFI services under the policy, will contain clauses that ensure continuity and stability of the ORC NFI operation.

Should it be determined that one section of this policy is incorrect or invalid, the other sections will remain in effect until the policy is updated. Requirements for updating this policy are described in Section 9.12. Responsibilities, requirements, and privileges of this document are transferred to the newer edition upon release of that newer edition.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

9.17.1 Waivers

No stipulation.

10 Bibliography

The following documents were used in part to either directly or indirectly develop this CPS:

ABADSG Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.

CIMC Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.

FIPS 140-2 Security Requirements for Cryptographic Modules May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS 186-2 Digital Signature Standard, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

FIPS 201 Personal Identity Verification (PIV) of Federal Employees and Contractors http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

FOIACT 5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html

FPKI-E Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997 http://csrs.nist.gov/pki/FPKI7-10.DOC

FPKI-Prof Federal PKI X.509 Certificate and CRL Extensions Profile

ISO9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.

ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NIST SP 800-73 InterfNFI for Personal Identity Verification (4 Parts) http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-76 Biometric Data Specification for Personal Identity Verification http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

NIST SP 800-78 Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV) http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf

NSD42 National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)

NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PIV-I Profile X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Date: April 23 2010, Reference Link: http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf

PKCS#12 Personal Information Exchange Syntax Standard, April 1997. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 3647 Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003.

11 Acronyms and Abbreviations

AID	Application Identifier
CA	Certification Authority
CARL	Certification Authority Revocation List
CMS	Card Management System
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FPKI MA	Federal Public Key Infrastructure Management Authority
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKI	Federal Public Key Infrastructure
FPKI-E	Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
GPEA	Government Paperwork Elimination Act of 1998
GSA	General Services Administration
HTTP	HyperText Transfer Protocol
HSM	Hardware Security Module
IETF	Internet Engineering Task Force

ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
LDAP	Lightweight Directory Access Protocol
MOA	Memorandum of Agreement (as used in the context of this CPS, between an Entity such as ORC and the FPKIPA allowing interoperation between the FBCA and ORC's Principal CA)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PIV-I	Personal Identity Verification – Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
UPN	User Principal Name
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code

UUID	Universally Unique Identifier (defined by RFC 4122)
WWW	World Wide Web

12 Glossary

Access Ability to make use of any information system (IS) resource. [NS4009]

Access Control Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]

Accreditation Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]

Activation Data Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Affiliated Organization Organizations that authorize affiliation with Subscribers of PIV-I certificates.

Applicant The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]

Archive Long-term, physically separate storage.

Attribute Authority An entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity.

Audit Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]

Audit Data Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]

Authenticate To confirm the identity of an entity when that identity is presented.

Authentication Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]

Backup Copy of files and programs made to facilitate recovery if necessary. [NS4009]

Binding Process of associating two related elements of information. [NS4009]

Biometric A physical or behavioral characteristic of a human being.

Certificate A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CPS, the term “Certificate” refers to certificates that expressly reference the OID(s) of this CPS in the “Certificate Policies” field of an X.509 v.3 certificate.

Certification Authority (CA) An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.

Certification Authority Revocation List (CARL) A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.

CA Facility The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate Management Authority (CMA) A Certification Authority or a Registration Authority.

Certification Authority Software Key Management and cryptographic software used to manage certificates issued to subscribers.

Certificate Policy (CP) A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practices Statement (CPS) A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

Certificate-Related Information Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.

Certificate Revocation List (CRL) A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.

Certificate Status Authority A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

Client (application) A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.

Common Criteria A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Compromise Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]

Computer Security Objects Registry (CSOR) Computer Security Objects Registry operated by the National Institute of Standards and Technology.

Confidentiality Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]

Cross-Certificate A certificate used to establish a trust relationship between two Certification Authorities.

Cryptographic Module The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]

Cryptoperiod Time span during which each key setting remains in effect. [NS4009]

Data IntegrityAssurance that the data are unchanged from creation to reception.

Digital Signature The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer’s digital certificate; and (2) whether the message has been altered since the transformation was made.

Dual Use Certificate A certificate that is intended for use with both digital signature and data encryption services.

Duration A field within a certificate which is composed of two subfields; “date of issue” and “date of next issue”.

E-commerce The use of network technology (especially the internet) to buy or sell goods and services.

Encrypted Network A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.

Encryption Certificate A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

End-entity Relying Parties and Subscribers.

Entity For the purposes of this document, “Entity” refers to an organization, corporation, community of interest, or government agency with operational control of a CA.

Entity CA A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government.

FBCA Management Authority (FPKI MA) The Federal Public Key Infrastructure Management Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.

Federal Public Key Infrastructure Policy Authority (FPKI PA) The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter-Entity PKI interoperability that uses the FBCA.

Firewall Gateway that limits access between networks in accordance with local security policy. [NS4009]

High Assurance Guard (HAG) An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

Information System Security Officer (ISSO) Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]

Inside threat An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Integrity Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Intellectual Property Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Intermediate CA A CA that is subordinate to another CA, and has a CA subordinate to itself.

Key Escrow A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]

Key Exchange The process of exchanging public keys in order to establish secure communications.

Key Generation Material Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Key Pair Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Local Registration Authority (LRA) A Registration Authority with responsibility for a local community.

Memorandum of Agreement (MOA) Agreement between the FPKIPA and ORC allowing interoperability between ORC and the FBCA.

Mission Support Information Information that is important to the support of deployed and contingency forces.

Mutual Authentication Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

Naming Authority An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.

National Security System Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]

Non-Repudiation Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID) A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the seven policies and cryptographic algorithms supported.

Out-of-Band Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).

Outside Threat An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.

Physically Isolated Network A network that is not connected to entities or systems outside a physically controlled space.

PKI Sponsor Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.

Policy Management Authority (PMA) Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.

Principal CA The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.

Privacy Restricting access to subscriber or Relying Party information in accordance with Federal law and Entity policy.

Private Key (1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key (1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.

Public Key Infrastructure (PKI) A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA) An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate) To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying PartyA person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Renew (a certificate) The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.

Responsible Individual A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate To prematurely end the operational period of a certificate effective at a specific date and time.

Risk An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Risk Tolerance The level of risk an entity is willing to assume in order to achieve a potential desired result.

Root CA In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

ServerA system entity that provides a service in response to requests from clients.

Signature Certificate A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subordinate CA In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Subscriber A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device

Superior CA In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).

System Equipment Configuration A comprehensive accounting of all system hardware and software types and settings.

System High The highest security level supported by an information system. [NS4009]

Technical non-repudiation The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.

Threat Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]

Trust List Collection of trusted certificates used by Relying Parties to authenticate other certificates.

Trusted Agent Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfNFI with Certification Authorities.

Trusted Certificate A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Trusted Timestamp A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Trustworthy System Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

Two-Person Control Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]

Update (a certificate) The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.

Zeroize A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

13 APPENDIX A

PIV-INTEROPERABLE SMART CARD DEFINITION

The intent of PIV-I is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Agency. Thus, reliance on PIV-I Cards requires compliance with technical specifications and specific trust elements. This appendix defines the specific requirements of a PIV-I Card. It relies heavily on relevant specifications from the National Institute of Standards and Technology (NIST).

The following requirements apply to ORC PIV-I Cards:

1. To ensure interoperability with Federal systems, ORC PIV-I Cards use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).

2. ORC PIV-I Cards conform to [NIST SP 800-73[1]].

3. ORC X.509 Certificates for Authentication are issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.

4. All ORC certificates issued a policy OID cross certified with the PIV-I Hardware policy OID conform to [PIV-I Profile].

5. ORC PIV-I Cards contain an asymmetric X.509 Certificate for Card Authentication that:

a. conforms to [PIV-I Profile];

b. conforms to [NIST SP 800-73]; and

c. is issued under the PIV-I Card Authentication policy.

6. ORC PIV-I Cards contain an electronic representation (as specified in SP 800-73 and SP 800-76) of the Cardholder's Facial Image printed on the card.

7. The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.

8. Visual distinction of a PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on ORC PIV-I Cards are not placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201].

Special attention is paid to UUID requirements for PIV-I.

9. ORC PIV-I Card physical topography includes, at a minimum, the following items on the front of the card:

a. Cardholder facial image;

b. Cardholder full name;

c. Organizational Affiliation, if exists; otherwise the issuer of the card; and

d. Card expiration date.

10. ORC PIV-I Cards have an expiration date not to exceed 5 years of issuance.

11. Expiration of an ORC PIV-I Card does not extend beyond the expiration of PIV-I Content Signing certificate on the card.

12. The digital signature certificate that is used to sign objects on an ORC PIV-I Card (e.g., CHUID, Security Object) contains a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID. ORC PIV-I Content Signing certificates conform to [PIV-I Profile].

13. ORC PIV-I Content Signing certificates and corresponding private key are managed within a trusted Card Management System as defined by Appendix B.

14. At issuance, the RA activates and releases the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.1.

15. ORC PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system performs a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys are set to be specific to each PIV-I Card. That is, each ORC PIV-I Card contains a unique card management key. Card management keys meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78]

14 APPENDIX B

CARD MANAGEMENT SYSTEM REQUIREMENTS

ORC CAs have a responsibility to ensure a certain level of security from the CMS(s) that manage the token on which ORC certificates reside, and to which ORC issues certificates for the purpose of signing PIV-I Cards. This appendix provides additional requirements to those found above that apply to ORC CMS(s) that are trusted under the Certificate Policy.

The Card Management Master Key will be maintained in a FIPS 140-2 Level 2 Cryptographic Module and conform to [NIST SP 800-78] requirements. Diversification operations will also occur on the Hardware Security Module (HSM). Use of these keys requires PIV-I Hardware or commensurate. Activation of the Card Management Master Key will require strong authentication of Trusted Roles. Card management will be configured such that only the authorized CMS can manage issued cards.

The PIV-I identity proofing, registration and issuance process will adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV-I credential without the cooperation of another authorized person.

All personnel who perform duties with respect to the operation of the CMS will receive comprehensive training. Any significant change to CMS operations will have a training (awareness) plan, and the execution of such plan will be documented.

Audit log files will be generated for all events relating to the security of the CMS and will be treated the same as those generated by the CA (see Sections 5.4 and 5.5).

A formal configuration management methodology will be used for installation and ongoing maintenance of the CMS.

ORC’s Configuration Management Plan (CMP) enables system owners to proceed with system changes as needed while ensuring that the appropriate controls are in place to manage the level of risk during a configuration change. CM is conducted using four interrelated functions:

- Configuration Identification
- Change control
- Status Accounting
- Configuration Audits

The ORC CMP applies to all ORC projects or components.

The ORC CMP describes the use of a change control methodology to establish the system configuration baseline and define, schedule, review, and monitor changes to that configuration between baselines. It outlines roles, responsibilities, organizational relationships, functions, processes, and procedures that will be used to implement CM. The plan is designed to track any changes made to the components from the baseline throughout the lifecycle, in accordance with Federal laws, regulations, and IT Security Policy.

The ORC CMP incorporates rigorous change control processes and procedures. These controls ensure that the appropriate due diligence and evaluations have been completed, and that additional risks are not introduced into the without prior knowledge, careful consideration, and conscious acceptance. Strong configuration management processes also ensure that:

1. The status of system configuration activity is accurate and readily available.
2. System configuration change history is controlled and documented.
3. Each design requirement is traceable to the system configuration.
4. Each configuration item is uniquely identified.

To accomplish these goals, the ORC CMP includes the following CM best practices:

1. Configuration Identification – Configuration Identification is used to establish and maintain a definitive basis for control and status accounting throughout all life cycle phases of the project.
2. Configuration Control – Configuration Control is the systematic proposal, justification, evaluation, coordination, approval (or disapproval), and implementation of changes after formal establishment of a configuration baseline.
3. Configuration Status Accounting – Configuration Status Accounting is to record, store, maintain, correlate, and report the status of an evolving configuration item throughout the system life cycle.
4. Configuration Audits and Reviews – A Configuration Audit is a formal review of a project for the purpose of assessing compliance with the CMP. A

Configuration Review is any activity that is conducted to evaluate the effectiveness of controls and status accounting.

The ORC CMP may be updated periodically to adapt to changes in procedures, rules, regulations, and best-practices as necessary to maintain proper CM practices and maintain coverage of all components.

ORC has documented incident handling procedures that are approved by the head of the organization responsible for operating the CMS. The documentation for incident handling is accomplished through the combination of the ORC Policy 18-0, Incident Reporting, ORC Procedure 18-1 Incident Reporting, and the ORC Contingency Plan. If the CMS is compromised, all certificates issued to the CMS will be revoked, if applicable. The damage caused by the CMS compromise will be assessed and all Subscriber certificates that may have been compromised will be revoked, and Subscribers will be notified of such revocation. The CMS will be re-established.

All Trusted Roles who operate a CMS will be allowed access only when authenticated using a method commensurate with PIV-I Hardware.

The computer security functions listed below are required for the CMS:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see Section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.