Operational Research Consultants, Inc. (ORC)
External Certification Authority (ECA)
Certification Practice Statement Summary

Version 4.3.1.2

September 19, 2014

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

This page intentionally left blank

TABLE OF CONTENTS

1 Introduction

This External Certification Authority (ECA) Certification Practice Statement (CPS) summary describes the establishment and operation of an ECA in support of the Department of Defense (DoD) Public Key Infrastructure (PKI) and the policies and procedures relating to holding or using certificates issued by the Operational Research Consultants, Incorporated (ORC) ECA. This CPS is applicable to all agencies and individuals that will be interacting with ORC and the ORC ECA, including DoD activities, other government agencies, and associated individuals and contractors. The purpose of this CPS is to inform individuals relying (Relying Parties) on Certificates issued by ORC and Subscribers (holders of ORC certificates) of their duties and obligations. It is also to advise those parties of the policies, practices and procedures that ORC uses for issuing, validating and revoking ORC ECA issued certificates. This CPS is structured in accordance with Request For Comment (RFC) 3647 of the Internet Engineering Task Force (IETF).

This CPS has been written by ORC in response to the United States (US) Government Certificate Policy (CP) for External Certification Authorities (ECA), Version 4.3, dated January 4, 2012 The US Government ECA CP takes precedence in any policy discrepancies. In the event that a provision of this CPS conflicts with a signed agreement with DoD (e.g. MOA), that provision of the signed agreement with DoD or CP will take precedence over this CPS, in that order.

Security management services provided by the ORC ECA PKI include:

- Key Generation/Storage/Recovery;
- Certificate Generation, Update, Renewal, Re-key, and Distribution;
- Certificate Revocation List (CRL) Generation and Distribution;
- Directory Management of Certificate Related Items;
- Certificate token initialization/programming/management;
- Device Identity Management
- Privilege and Authorization Management; and
- System Management Functions (e.g., security audit, configuration management, archive, etc.).

Defining requirements on ORC's ECA PKI activities, including the following, ensures the security of these services:

- Subscriber identification and authorization verification;
- Control of computer and cryptographic systems;
- Operation of computer and cryptographic systems;

- Usage of keys and public key certificates by Subscribers and Relying Parties; and
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met.

1.1 Overview

DoD recognizes the need to interoperate with individuals outside of the DoD domain and has a requirement to establish trust relationships with other Certification Authorities (CAs) that achieve a satisfactory assurance level. The ORC ECA CAs will provide non-DoD personnel with certificate services that are interoperable with the DoD Public Key enabled applications.

This CPS applies to X.509 version 3 certificates with assurance levels as defined in the US Government ECA CP, as used to protect information up to and including unclassified information. The practices 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.

The ORC ECA has been established as a subordinate CA to the US Government ECA Root CA. The ORC ECA will continue to allow rapid support certification services to US Government contractors that are supporting specified programs currently requiring or will require PKI support. This CPS is the implementation document for the ORC ECA for the purpose of issuing certificates to individuals, contractor personnel and Foreign Nationals requiring access to government resources. The CPS describes the operations of the ORC ECA and the services that the ORC provides. These services include:

- Subscriber Enrollment
- Subscriber Registration
- Subscriber Validation
- Certificate Issuance
- Certificate Publishing
- Encryption Key Storage
- Key Recovery
- Certificate Status Information

1.2 Document Name and Identification

ORC operates the ECA in a manner consistent with the practices established in the US Government ECA CP. The ECA Object Identifiers (OIDs) are registered under Computer Security Objects Registry (CSOR)

maintained by the National Institute of Standards and Technology (NIST). Certificates created by the ORC ECA assert the policy OID for three levels of assurance as specified in the ECA Root CP:

Where {id-eca-policies} represents the prefix {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1) eca-policies(12)}

id-eca-medium	ID ::= {id-eca-policies 1}
id-eca-medium-hardware	ID ::= {id-eca-policies 2}
id-eca-medium-token	ID ::= {id-eca-policies 3}
id-eca-medium-sha256	ID ::= {id-eca-policies 4}
id-eca-medium-token-sha256	ID ::= {id-eca-policies 5}
id-eca-medium-hardware-pivi	ID ::= {id-eca-policies 6}
id-eca-cardauth-pivi	ID ::= {id-eca-policies 7}
id-eca-contentsigning-pivi	ID ::= {id-eca-policies 8}
id-eca-medium-device-sha256	ID ::= {id-eca-policies 9}

ORC ECA issued certificates contain one of the above policy OIDs. The ORC ECA and this CPS support all of the OIDs defined in the US Government ECA CP, listed above. Requirements for medium SHA-256, medium token SHA-256, and medium hardware SHA-256 are identical to medium, medium token and medium hardware respectively, except for the hash algorithm used in generating certificate, CRL, and OCSP response signatures. Requirements for Medium Device SHA-256 are identical to medium except for the hash algorithm, re-key and activation data. The requirements stipulated in this CPS apply to all assurance levels, unless otherwise noted.

1.3 PKI Participants

Under this CPS the ORC ECA Certification Authority Administrators (CAAs), ORC PIVotal ID, Automated Registration Authorities (ARA) and Registration Authorities (RAs) are considered “Certification Management Authorities” (CMAs) and are the only authorities with trusted access to the ORC ECA Certification Authority (CA) application and keys, as detailed in Section 5 of this CPS. The ARA has been added to the ORC ECA to provide additional technical controls for issuing via card management stations located outside of ORC’s security boundary..

Server-based Certificate Status Authorities (CSAs) (e.g. Online Certificate Status Protocol (OCSP) Responders and Server-based Certificate Validation Protocol (SCVP) status providers) operated by the ORC ECA are

also considered CMAs. All ORC ECA CMAs are operated in compliance with this CPS and the ECA CP, as detailed in Section 4.9 of this CPS.

1.3.1 ECA Policy Management Authority (EPMA)

The ECA Policy Management Authority (EPMA) is a US Government entity established to:

- Oversee the creation and update of this CP and plans for implementing any accepted changes;
- Provide timely and responsive coordination to approved ECAs and Government Agencies through a consensus-building process;
- Review the Certification Practice Statements (CPS) of CAs that offer to provide services meeting the stipulations of this CP;
- Accepting and processing applications from External PKIs desiring to cross-certify with the ECA PKI;
- Determining the mappings between ECA certificate policies and the External PKI certificate policies, and
- Review the results of ECAs' compliance audits to determine if the CAs are adequately meeting the stipulations of this CP and associated approved CPSs, and make recommendations to the CAs regarding corrective actions, or other measures that might be appropriate, such as revocation of CA certificates or changes to this CP.

1.3.2 Certification Authorities

The ORC ECA is authorized by the EPMA and is a subscriber to the off-line US Government ECA Root CA(s). The US Government ECA Root CA(s) have signed the ORC ECA signing certificate rendering the ORC ECA a subordinate of the “superior” US Government ECA Root CA(s). The ORC ECA generates and manages certificates and certificate revocation lists (CRLs). It posts those certificates and CRLs to a repository. A CAA, as defined herein, administers the ORC ECA. CAAs are the only individuals authorized to administer the ORC ECA application. CAAs are designated directly by ORC’s President. ORC CAAs perform tasks required for CA/ CRL management.

1.3.3 Card Management System

ORC PIVotal ID are the only ORC ECA Card Management System(s) (CMS) authorized for the process to issue ORC ECA PIV-I credentials, which contain printed card elements, certificates and private keys, and other data objects including digitally signed biometrics. ECA CP requirements

specified for CMSs are applicable to any ORC PIVotal ID that supports the issuance of certificates that assert any and all of the PIV-I OIDs. ORC PIVotal ID CMSs use a PIV-I Content Signing certificate to digitally sign data elements on the PIV-I credentials. A connector certificate with assigned privileges on the CA is issued to the ORC PIVotalID. The connector certificate is secured in the ORC PIVotalID's connected hardware security module (HSM). This certificate has assigned privileges on the CA for requesting certificate issuance and/or revocation. Trusted users on the ORC PIVotal ID who can direct it to perform certificate related actions are considered to be Registration Authorities (RAs), as described in Section 1.3.4. A CAA, as defined herein, administers the ORC PIVotal ID and is the only individual(s) authorized to administer the ORC PIVotal ID.

1.3.4 Registration Authority (RA)

RAs for the ORC ECA CA are human and non-human entities approved by an ORC CAA or ORC RA and are issued RA certificates for the purpose of collecting and submitting digitally signed verification of Subscriber identities and information to be entered into public key certificates. These RA certificates assert either Medium Hardware or Medium PIV-I Hardware certificate policy OIDs. PIVotal ID Issuers must have a Medium PIV-I Hardware certificate. RAs for the ORC ECA are designated in the following roles:

- RA (human, ORC personnel only)
- PIVotal ID Server (non-human)
- ARA Server (non-human)
- ORC PIVotal ID Issuer
- ORC ARA Issuer

Section 5.2 of this CPS provides details regarding each of these RA roles.

1.3.5 Subscribers

A Subscriber is the End Entity (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. ECA Subscribers are limited to the following categories of entities:

- Employees of businesses acting in the capacity of an employee and conducting business with a US government agency at local, state or Federal level
- Employees of state and local governments conducting business with a US government agency at local, state or Federal level

- Employees of foreign governments or organizations conducting business with a US Government agency at local, state or Federal level
- Individuals communicating securely with a US government agency at local, state or Federal level, and
- 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 US 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 ECA is 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 PIVotal ID and ARA are technically Subscribers which collect and manage the data to be placed in certificates and tokens. Only a connector Certificate and Content Signing Certificate are issued to the ORC PIVotal ID. Only a connector certificate is issued to an ARA.

1.3.6 Relying Parties

A Relying Party is an individual or organization who, by using another's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate, relies on the validity of the binding of the Subscriber's name to a public key. 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

1.3.7.1 Trusted Agents

ORC Trusted Agents are individuals who are Notaries Public, ORC LRAs, and approved DoD employees. ORC LRAs include ORC LRAs, ORC Partner LRAs, ORC PIVotal ID Registrars, ORC ARA Registrars, These roles perform identity proofing, as well as witness and acknowledgement functions. Section 5.2 of this CPS provides details regarding each of these roles. These personnel do not have any privileged access to the ORC ECA systems, including approval or rejection of certificate requests, or issuance or revocation of certificates.

1.3.7.1.1 Notaries Public

For jurisdictions within the United States, US Notaries Public may act as a Trusted Agent. These persons may validate the identity of individuals who are unable to present their identity credentials in person to an RA or LRA. In this situation, the Subscriber will be provided with a form including the Subscriber's name, organizational affiliation (if subscriber is affiliated with an organization), and certificate request number. The Subscriber will be required to present this form, along with required IDs and credentials identifying organizational affiliation (if subscriber is affiliated with an organization). Foreign Nationals being validated in this manner are required to present two (2) forms of official Photo ID, one having a unique identifier and expiration date and credentials identifying organizational affiliation. The Notary Public (or other persons legally empowered to witness and certify the validity of documents and to take affidavits and depositions, as stipulated by the EPMA) will witness and certify the form.

For jurisdictions other than the United States, requirements for registration must be witnessed and acknowledged by a US Notary Public that acts as a Trusted Agent. The Subscriber will submit the notarized form and copies of the information used to establish identity via certified mail to an RA.

1.3.7.1.2 Local Registration Authority (LRA)

ORC ECA LRAs are designated in the following roles:

- ORC LRA
- ORC Partner LRA
- ORC PIVotal ID Registrar
- ORC ARA Registrar

ORC RAs may delegate the identity proofing tasks to Local Registration Authorities (LRAs) who have been approved by an ORC RA. Upon performing their duties LRAs provide verification to the RA. If an ORC RA delegates duties to one or more LRAs, the ORC RA informs all other ORC RAs. LRAs may not designate other LRAs. Approval of certificates may only be approved by RA certificate holders of equal or higher levels of assurance.

ORC requires ORC employees serving as LRAs to hold Medium Hardware assurance certificates for performing their respective LRA duties. ORC requires that all Partner LRAs obtain (at a minimum) a Medium Assurance Identity Certificate. ORC Partner LRAs may or may not hold Medium Hardware assurance certificates for performing their respective LRA duties. However, ORC Partner LRAs who do not hold Medium Hardware assurance certificates may not perform LRA duties for applicants requesting Medium Hardware assurance certificates. All LRAs within the ORC ECA are limited

to performing LRA duties for applicants requesting certificates of equal or lower level of assurance as the level of assurance of the certificate held by the LRA. ORC PIVotal ID Registrars must hold an ORC ECA PIV-I card asserting id-eca-medium-hardware-pivi to perform their LRA duties. ORC ARA Registrars must hold an ORC ECA ARA card asserting id-eca-medium-hardware to perform their LRA duties.

Further description of the various LRA roles are described in Section 5.2.

1.3.7.2 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components and organizations that are named as public key certificate subjects. The PKI Sponsor works with ORC and, when appropriate, the Trusted Agents, to register components (routers, firewalls, etc.) in accordance with Section 3.2.3.3, and is responsible for meeting the obligations of Subscribers as defined throughout this document. PKI Sponsor is not considered a trusted role.

1.3.7.3 Affiliated Organization

An Affiliated Organization is an organization that has a relationship with a subscriber and sponsors that subscriber for obtaining a 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.

1.3.7.4 PKI Point of Contact (POC)

A PKI Point of Contact is a duly appointed Subscriber organization representative who has been granted signature authority for an organization/ agency. The PKI Point of Contact serves as the primary point of contact concerning the use and obligations related to all certificates issued and services provided under this CPS for the designated Subscriber organization/ agency. The PKI POC will provide the name-space for their organization (e.g. OU value for company name in sponsored Subscriber's distinguished name in the certificates). ORC will make the final determination with respect to name space control.

The PKI POC is to whom subscribers surrender their hardware cryptographic tokens when leaving the organization. The PKI POC will immediately zeroize or destroy the hardware token promptly upon receipt. Via digitally-signed e-mail, the PKI POC will notify the ORC RA with the following information: full name of Subscriber; revocation reason; date of token collection or reason for inability to collect token; and date of loss/separation.

1.3.7.5 Group/Role Manager

A Group/Role Manager is a duly appointed individual responsible for managing a Group/Role, but is not a trusted role. ORC ECA does not support the Group/Role entity.

1.3.7.6 Other Authorities

No other Authorities exist within the ORC ECA at this time.

1.3.7.6.1 Corporate Security Auditor

Compliance audits as stipulated in this CPS are independently administered. A Corporate Security Auditor is not in any way under the control of CAAs. Nor are CAAs under the control of the Corporate Security Auditor. The Corporate Security Auditor has responsibility for the maintenance and monitoring of the ORC internal audit system and is designated directly by ORC's President.

ORC's Corporate Security Auditor also coordinates and supports external auditing, as described in Section 8, including aperiodic audits. Audits of the ORC ECA will follow the guidelines and specifications of currently accepted standards and practices, as approved by the EPMA.

1.3.7.6.2 External Auditor

ORC retains as our external compliance auditor a nationally recognized firm with expertise in IT Security Auditing and Evaluation. The external auditing firm is an industry leader with focus on the design, implementation and operation of information assurance systems and the technologies that enable and support the implementation of information security services.

1.3.7.6.3 Code-Signing Attribute Authority (CSAA)

CSAAs who obtain ORC ECA Medium Hardware Assurance Identity certificates are authorized to act as Trusted Agents for the issuance of mobile code signing (MCS) certificates to employees of their organizations. CSAAs are not authorized to act as Trusted Agents for any other purpose, including the issuance of ORC ECA Identity certificates for designated code signers, unless they are also approved and authorized as an LRA.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The ORC ECA is intended to support the following security services: *confidentiality, integrity, authentication* and *technical non-repudiation*. The ORC ECA supports these security services by providing Identification and Authentication (I&A), integrity, and technical non-repudiation through digital signatures, and confidentiality through key exchange. These basic security

services support the long-term integrity of application data, but may not by themselves provide a sufficient integrity solution for all application circumstances. For example, when a requirement exists to verify the authenticity of a signature beyond the certificate validity period, such as contracting, other services such as trusted archival services or trusted timestamp may be necessary. These solutions are application based, and must be addressed by Subscribers and Relying Parties. The ORC ECA provides support of security services to a wide range of applications that protect various types of information, up to and including sensitive unclassified information.

1.4.1.1 Level of Assurance

The level of assurance associated with a public key certificate is an assertion by a CA of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate. Assurance level depends on the proper registration of Subscribers and the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of this CPS. Personnel, physical, procedural, and technical security controls, as described in this CPS, are used to maintain the assurance level of the certificates issued by the ORC ECA.

1.4.1.2 Factors in determining usage

The amount of reliance a Relying Party chooses to place on the certificate will be determined by various risk factors. Specifically, the value of the information, the threat environment, and the existing protection of the information environment are used to determine the appropriate level of assurance of certificates required to protect and authenticate the information.

1.4.1.3 Threat

Threat is any circumstance or event with the potential to cause harm. In terms of information systems, harm includes destruction, disclosure, or modification of data, processes, or processing components. Threats to systems include environmental disasters, physical damage, system penetration, and violation of authorization, human error, and communications monitoring or tampering. It is the responsibility of each relying party to assess the factor.

1.4.1.4 General Usage

This section contains definitions for two levels of assurance, and guidance for their application. The guidance is based on the previous discussion of information value and environmental protection. 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.

Medium and Medium Token Assurance - This level is intended for applications handling sensitive medium value information based on the relying party's assessment, with the exception of transactions involving issuance or acceptance of contracts and contract modifications. Examples of medium assurance applications 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

Medium Hardware and Medium Hardware PIV-I Assurance - 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
- Applications performing contracting and contract modifications

Card Authentication PIV-I Assurance: This level is intended only for use in physical access situations to support high volume throughput. Because Card Authentication assurance certificates do not require activation data to unlock the private key, validation of a Card Authentication certificate provides only proof of the physical presence of the smart card token. It provides no proof of the identity of the individual in possession of the token. PIV-I cards and their associated ORC ECA certificates are not intended to replace existing approval mechanisms for physical access, they may provide one layer of protection to identify the user.

Content Signing PIV-I Assurance: This level is intended only for use in digitally signing data objects on a PIV-I smart card and may not be used for any other purpose. ORC ECA Content Signing PIV-I certificates are only issued to Card Management Systems, per ECA policy.

1.4.2 Prohibited Certificate Uses

No Stipulation

1.5 Policy Administration

1.5.1 Organization Administering the Document

Operational Research Consultants, Inc.

11250 Waples Mill, South Tower, Ste 210

Fairfax, VA 22030

Operational Research Consultants, Inc. is responsible for the creation, revision and promulgation of this Certificate Practice Statement, in accordance with the requirements stipulated in the ECA Certificate Policy.

1.5.2 Contact Person

Ms. Denise Finnance is responsible for registration, maintenance, and interpretation of this CPS.

Ms. Denise Finnance COO

11250 Waples Mill, South Tower, Ste 210

Fairfax, VA 22030

Additional ORC contact persons are:

Mr. James Manchester, Operational Research Consultants, Inc., (703) 246-8568, e-mail manchesterj@orc.com.

Ms. Caroline Godfrey, Operational Research Consultants, Inc., (703) 246-8533, e-mail godfreyc@orc.com.

Mr. Richard Webb, Operational Research Consultants, Inc., (703) 246-8545, e-mail webbr@orc.com.

1.5.3 Person Determining CPS Suitability for the Policy

The EPMA determines the suitability of the ORC ECA using a CPS compliance analysis and approval process.

EPMA

9800 SAVAGE RD STE 6763

FT MEADE MD 20755-6763

1.5.4 CPS Approval Procedures

The EPMA will make the determination that a CPS complies with the policy for a given level of assurance. The compliance analysis is performed by an independent party. ORC has met all requirements for an approved CPS prior to commencing operations. This ORC ECA CPS has been determined to be an approved CPS in compliance with the X.509 Certificate Policy for External Certification Authorities (CP), Version 4.3, January 4, 2012.

1.5.5 Waivers

Normally, the EPMA will decide that variation in CMA practice is acceptable under a current policy, or the CMA will request a permanent change to the policy. Policy waivers may be granted by the EPMA to meet urgent, unforeseen ECA operational requirements. When a waiver is granted, the EPMA will post the waiver on a web site accessible by Relying Parties, and will either initiate a permanent change to the policy, or will place a specific time limit, not to exceed one year, on the waiver.

1.6 Definitions and Acronyms

See Sections 13 and 14.

2 Publications and Repository Responsibilities

2.1 Repositories

ORC operates and maintains repositories to support their PKI operations. The location of any publication is available to Subscribers and Relying Parties as stipulated in this CPS.

Information in the ORC repositories is protected in accordance with the Privacy Act of 1974 as set forth in ORC's Privacy Policy and Procedures documents.

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 Relying Party.

ORC posts CA Certificates at the following locations, accessible via HTTP:

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

ORC posts the Root Certificate at the following locations, accessible via HTTP:

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

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

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

ORC posts certificates and CRL information in a repository established by the ORC ECA PKI. Only information contained in the certificate(s) is posted in this directory to ensure compliance with the Privacy Act. Access to the directory is available via HTTPS, via a directory gateway interface at:

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

The ORC directory sub-trees identify the organization of the EE.

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

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

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 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.

2.2 Publication of Certification Information

The ORC ECA 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 ECA
- A current and accurate CRL
- An ORC ECA issued certificate for its certificate and CRL signing key
- A copy or link to the current US Government ECA CP
- An abridged version of this approved CPS, which will include at a minimum the sections itemized below and all obligations and requirements levied on entities external to ORC
  - Section 1.5, ECA Contact Information
  - Section 3.2, Initial Identity Validation
  - Section 4.9, Certificate Revocation and Suspension
  - Section 9, Other Business and Legal Matters
  - Any additional policy, waiver, or practice information that is supplemental to the US Government ECA CP or this CPS

The repository is located at http://eca.orc.com. ORC's maintains the repository using two separate but identical iterations run behind a load balancer. In addition, a copy of the repository is maintained off-site and is activated in the event of network outage. The primary location has

dedicated power and HVAC, separate from the facility, with a direct dedicated generator, as cited in Section 5. These capabilities allow ORC ECA to maintain availability of the repository overall per year and scheduled downtime not to exceed 0.5% annually.

2.3 Time or Frequency of Publication

Certificates are published to a repository at the time of issuance. CRL publication is in accordance with Section 4.9.7. At the time of issuance Certificates are published to a repository. The publication to the repository is an automated function which occurs at the time of issuance.

2.4 Access Controls on Repositories

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

There are no access controls on the reading of repository information, including certificates and CRLs. 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 RAs and CAAs as authorized to make changes. ORC protects any and all repository information not intended for public dissemination or modification. Access controls include:

- Access to ORC Electronic Resources is 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.
- For ORC PIVotal ID PIV-I certificates that contain the UUID in either the subject name field or the subject alternative name field or any other certificate field, publishing rules on the certificate authority restrict publication of those certificates while permitting PIV-I certificates that do not contain UUID information to be published to public repositories. PIV-I certificates containing UUID in any field are not externally published.

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 ECA conform to the X.500 Distinguished Name (DN) format for subject and issuer name fields and conform to the format specified in the certificate profiles in Section 10 of the DoD ECA CP.

Certificates issued to RAs use the X.500 DN form.

For subscriber certificates asserting the following OIDs, id-eca-medium, id-eca-medium-hardware, id-eca-medium-token, id-eca-medium-sha256, id-eca-medium-token-sha256, the distinguished name of ORC ECA affiliated subscribers will take the following form:

For subscribers affiliated with an organization:

C=US, o=U.S. Government, ou=ECA, ou=ORC, ou=[organization name], cn=[Surname].[Firstname].[Middle Name or Initial[1].][Generation[2].][ORC Unique Identification String[3]]

For subscribers not affiliated with an organization:

C=US, o=U.S. Government, ou=ECA, ou=ORC, ou=Unaffiliated, cn=[Surname].[Firstname].[Middle Name or Initial.][Generation.][ORC Unique Identification String]

For subscriber certificates asserting the following OID, id-eca-hardware-pivi, the distinguished name of ORC ECA affiliated subscribers will take the following form:

For subscribers affiliated with an organization:

C=US, o=U.S. Government, ou=ECA, ou=ORC, ou=[organization name], cn=[Surname].[Firstname].[Middle Name or Initial.][Generation.][ORC Unique Identification String]

For subscribers not affiliated with an organization:

C=US, o=U.S. Government, ou=ECA, ou=ORC, ou=Unaffiliated, cn=[Surname].[Firstname].[Middle Name or Initial.][Generation.][ORC Unique Identification String]

[1] For any subscriber who does not have a middle name or initial, this data element is left blank.

[2] For any subscriber who does not have a generational suffix, this data element is left blank.

[3] See Section 3.1.2 for detailed explanation of the Unique Identification String

For subscriber certificates asserting the following OID, id-eca-cardauth-pivi, the distinguished name of ORC ECA affiliated subscribers will take the following form:

For subscribers affiliated with an organization:

C=US, o=U.S. Government, ou=ECA, ou=ORC, ou=[organization name], serialNumber=[UUID]

For subscribers not affiliated with an organization:

C=US, o=U.S. Government, ou=ECA, ou=ORC, ou=Unaffiliated, serialNumber=[UUID]

The UUID will 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”) and is at most 36 characters long.

Additionally, subscriber certificates issued under id-eca-cardAuth-pivi will include a subject alternative name extension that includes the UUID and is encoded as a uniformResourceIdentifier as specified in Section 3 of [RFC 4122] (e.g. “urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6”). Subscriber certificates issued under id-eca-cardAuth-pivi will not include any other name in the subject alternative name extension.

For subscriber certificates asserting the following OID, id-eca-contentsigning-pivi, the organization administering the ORC ECA PIVotal ID system will take the following form:

C=US, o=U.S. Government, ou=ECA, ou=ORC, ou=[administering organization name], cn=[administering organization name] PIV-I contentsigner

Devices that are the subject of certificates issued under the ORC ECA will be assigned either a geo-political name or an Internet domain component name. Device names will take one of the following forms:

C=US, o=U.S. Government, ou=ECA, ou=ORC, ou=[organization name], cn=[device name]

where device name is a descriptive name for the device (e.g. Host URL; IP Address; Host Name; Unique Identifier (depending on device)), as detailed in Section 10.7 of this CPS.

Code-signing certificates issued under the ORC ECA will be assigned a unique code-signer identification number assigned by the requesting organization. Code-signing certificate names will take the following form:

C=US, o=U.S. Government, ou=ECA, ou=ORC, ou=[organization name], cn=CS.[organization name].[organization assigned unique code signer identification string]

The organization assigned code signer unique identification string is assigned by the subscriber organization to distinguish between multiple code-signing certificates issued to that organization. The organization

assigned code signer unique identification string is manually verified by the ORC LRA by searching the certificate repository prior to issuance to ensure no name-space collision occurs.

3.1.2 Need of Names to be Meaningful

Common names will be meaningful as individual names, as actual server URLs, IP addresses, unique device names or as code signing organizational names. Names will identify the person or object to which they are assigned. In the case of a request for a subscriber or device certificate affiliated with an organization, the ORC ECA will document that the subscriber has completed the Organizational Affiliation Letter, made available during the certificate request process, which asserts that an affiliation exists between the Subscriber and the organization. In the case of a request for an unaffiliated subscriber or device certificate, ORC is not obligated to verify the subscriber's relationship to any organization and will issue a certificate(s) that does not assert an organizational affiliation.

Within the Distinguished Name(DN), the common name(CN) will represent the Subscriber in a way that is easily understandable for humans. For human and device subscribers, the CN will take the form identified in Section 3.1.1.

The ORC ECA will only sign certificates with subject names from within a name-space approved by the EPMA. The ORC ECA will not certify other CAs.

ORC has been assigned by the EPMA a name space of:

C=US, o=U.S. Government, ou=ECA, ou=ORC

In addition, ORC builds a Unique Identification String for a new subscriber receiving certificates from the ORC ECA CA. The Unique Identification String consists of a 10-digit number, prefixed by an alpha-numeric string. An example is shown below:

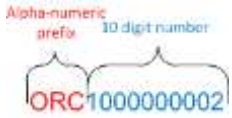

Figure 1 - Example of ORC Unique Identifier String for Subscriber.

The 10-digit number is assigned sequentially by ORC whenever a new subscriber receives certificates from the ORC ECA. Subscribers with existing certificates from the ORC ECA who have not changed name or organizational affiliation will be assigned the same 10-digit number from their previous certificates issued by the ORC ECA, in accordance with Section 3.2.3.1 and 3.2.3.2. Subscribers with existing certificates from the

ORC ECA whom have changed name or organizational affiliation will be assigned the next available sequential 10-digit number. The next available sequential 10-digit number is determined by a query against the ORC ECA certificate repository for all certificates issued to date. The alpha-numeric prefix of the Unique Identification String is assigned by the ORC ECA.

Additionally, the ORC ECA may append additional information to the end of the 10 digit number to identify the certificate type. This additional designation may be, but is not limited to, the following:

- .ID (for Signature Certificates)
- .encrypt (for Encryption Certificates)
- .Auth (for Authentication Certificates)

In cases where the additional information identifying certificate type is applied, the Unique Identification String will take the following form:

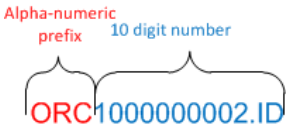

Figure 2 - ORC Unique Identification String with certificate type appended.

Once the ORC Unique Identification String has been fully constructed, the full ORC Unique Identification String is appended to the CN string. The full CN string for all subscribers will take the following form:

Figure 3 - Fully constructed CN for subscribers with appended ORC Unique Identification String.

3.1.3 Anonymity of Pseudonymity of Subscribers

ORC ECA 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), and are established by the EPMA established naming authority.

3.1.5 Uniqueness of Names

The ORC ECA RAs will comply with uniqueness of names as enforced by the EPMA, including X.500 DNs allocated from the EPMA. The ORC ECA RAs will enforce name uniqueness, as described in Section 3.1.1 and 3.1.2.

At a minimum, the ORC ECA RAs or PIVotal ID Issuer will ensure 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 ORC ECA CPS (Section 3.1.1 and 3.1.2)
- The ORC ECA complies with the EPMA 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. The ORC ECA will not issue that name to the rightful owner if it has already issued one sufficient for identification.

Trademarks will not be used as a name form or as any part of the name form for ORC ECA issued certificates. Trademarks will not be used as a name form or as a part of the name form for certificates issued to government employees unless the US 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, allied partners, coalition partners, NATO allies, foreign nationals, or organizations with specific permission.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

For ORC ECA Subscribers generating keys for requesting certificates (identity, device and non-escrowed encryption) that assert id-eca-medium, id-eca-medium-hardware, id-eca-medium-token, id-eca-medium-sha256, and id-eca-medium-token-sha256, id-eca-medium-device-sha256, id-eca-medium-hardware-pivi, id-eca-cardauth-pivi and id-eca-contentsigning-pivi, ORC authenticates the subscriber with a Proof of Possession (POP) test when requesting and retrieving the certificate by requiring the subscriber to perform a private key operation that verifies that the public key presented by the subscriber matches the private key. The ORC ECA uses CRMF and PKCS #10 in support of Proof of Possession.

To affect POP, the CA supplies a random challenge string to the browser as part of the KEYGEN tag.

For id-eca-medium and id-eca-medium-sha256, the public key generated by the browser's associated Cryptographic Service Provider (CSP) 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's CSP of the private key corresponding to that public key.

For id-eca-medium-device-sha256 and device certificates issued under id-eca-medium, the PKI Sponsor generates a key pair (private/public) using the device's associated Cryptographic Service Provider (CSP) and creates a signed PKCS10 object. The PKI Sponsor submits the PKCS10 object to the CA for certificate processing.

For id-eca-medium-hardware, id-eca-medium-token, and id-eca-medium-token-sha256, id-eca-medium-hardware-pivi, id-eca-cardauth-pivi and id-eca-contentsigning-pivi the key pair is generated by the CSP associated with the cryptographic device (smartcard or other crypto-token). 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 CSP 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 ORC ECA only provides escrow for the encryption certificate issued through the PIVotal ID CMS for certificates asserting the id-eca-medium-hardware-pivi. The Subscriber's private key for the PIV-I encryption certificate is generated in the HSM and stored encrypted and protected by the Key Encryption Key (KEK) in the PIVotal ID database, prior to the key being injected onto the PIV-I card. The Oberthur card used, enforces using a secure channel for writing this information to the card. During card personalization certificate keys are created in KMS under the protection of a HSM. In a secure channel session (SCP-03), the key is exchanged with the card. The secure channel is secured with AES keys, additionally, key data is encrypted with a AES data encryption key. The Subscriber's encryption keys are protected by a KEK, which is a 24 byte AES key. All cryptographic operations occur in the HSM. The private key is encrypted in the HSM with the KEK for secure storage in the database.

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.

3.2.2 Authentication of Organization Identity

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

- Subscriber requesting a certificate accompanied by a US Government sponsor. The Government Sponsor is vetted by presentation of a Government issued photo ID card (CAC/PIV). The Government sponsor will attest to the Subscriber's affiliation.
- Subscriber presenting a government-issued photo badge including the Subscribers company affiliation
- Subscriber providing a signed letter on company 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)
- Subscriber presenting an un-expired photo ID badge issued by the organization

In addition to verifying the Subscriber'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 ECA Certificate application. ORC verifies information concerning the Sponsoring Organization, such as legal company name, type of entity, year of formation, address (number and street, city, ZIP code), and telephone number. All Subscribers are notified, on the website application process, that the process is secure.

3.2.3 Authentication of Individual Identity

3.2.3.1 In-person Authentication

The following requirements apply to Subscribers for ORC ECA certificates (both U.S. citizens and non-U.S. citizens) located inside the U.S. Section 11 of this CPS specifies requirements for Subscribers for ORC ECA certificates located outside the U.S.

Verification of a Subscriber's identity will be performed prior to certificate issuance. The Subscriber will appear before one of the required identity verifiers, stipulated in Section 5.2.1 of this CPS, no more than 30 days prior to application of the CA's signature to the Subscriber's certificate, as detailed in Section 4.2. All Subscribers for medium assurance or medium

token assurance certificates are required to appear in person before an RA or a trusted agent, as listed in Section 1.3.4 or 1.3.7. All Subscribers for medium hardware assurance certificates are required to appear in person before an RA.

Subscribers for any/all ORC ECA certificates are required to present two official photo ID credentials along with other application information including proof of organization affiliation (if subscriber is affiliated with an organization), verification of citizenship of each Subscriber and the form generated during the certificate request process containing the certificate request number.

PIVotalID - For requests made through the ORC PIVotalID, the Registrar, as defined in Section 5.2, performs a verification of the identification documents presented and records that information into the ORC PIVotalID, see diagram in Section 4.1.2.2. The ORC PIVotal ID Issuer performs a verification of the identification documents presented and recorded in the ORC PIVotal ID during the registration process. The identification documents presented at the time of registration must match the identification documents presented at the time of issuance. For certificates asserting PIV-I certificate policies, individual Subscribers are to provide two identity source documents in original form which come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document must be a valid U.S. State or Federal Government-issued picture identification (ID).

ARA - For requests made through the ORC ARA, the ARA Registrar, as defined in Section 5.2, performs a verification of the identification documents presented and recorded in the ORC ARA during the registration process, see diagram in Section 4.1.2.2. The ARA Issuer performs a verification of the identification documents presented and recorded in the ORC PIVotal ID during the registration process. The identification documents presented at the time of registration must match the identification documents presented at the time of issuance.

Photo IDs must include one current and valid photo ID issued by a Government entity within the U.S., (e.g. passport, driver's license, government issued photo IDs).

The credential presented for citizenship verification must be one of the following:

For US citizens, only the following credentials will be accepted:

- U.S. Passport
- Certified birth certificate issued by the city, county, or state of birth, in accordance with applicable local law

- Naturalization Certificate
- Certificate of Citizenship
- FS-240 – Consular Report
- DS-1350 – Certification of Report of Birth

For non-US citizens,

- The only acceptable credential for proof of citizenship is an unexpired passport issued by the Subscriber's country of citizenship.
- A handwritten signature by the Subscriber in the presence of the person performing the identity verification

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

When a US Notary Public validates the Subscriber's identity, the RA will archive the original notarized request form and photo copies of all identification cards/passport used in the verification process. The notarized request and photo copies of identification are sent by the Subscriber to ORC. In all cases when a US Notary Public validates the Subscriber's identity, either an LRA will submit a digitally signed e-mail message or an ARA Registrar will generate an ARA transaction that will attest that the identity of the individual has been authenticated. At a minimum the LRA or ARA Registrar will record the subscriber's name, company name, citizenship, certificate request number, and whether the Subscriber was vetted for a medium assurance or medium token assurance certificate. Identity verification by a Notary Public does not apply to the PIVotalID process.

In all cases the LRA or ARA Registrar will record the following information:

- The Identity of the person performing the validation process
- A signed declaration by the identity-verifying agent that they verified the identity of the Subscriber
- The method used to authenticate the Subscriber's identity, including identification type and unique number or alphanumeric identifier on the ID
- The date of verification
- Serial number of token (if applicable)
- The citizenship of the Subscriber

If a US Notary Public[4] validates the Subscriber identity, the Subscriber will submit the notarized statement of identity along with copies of other

[4] Note that U.S. embassies and consulates provide notarial services for U.S. citizens residing outside the U.S.

information used to verify the Subscriber's identity directly to an ORC ECA RA, as defined in Section 1.3.4, as prescribed in the subscriber agreement.

Subscribers must fill out and sign a form acknowledging understanding and acceptance of the responsibilities associated with accepting a certificate. The Subscriber Agreement also serves as a testimonial to the accuracy of the information provided in the certificate request and declaration of identity of the subscriber.

For PIV-I certificates, an electronic facial image will be captured along with two fingerprints at the time of Subscriber's appearance before the Registrar. The electronic facial image will be used for printing facial image on the card, as well as for performing visual authentication during card usage for physical access. The PIV-I credential will contain an electronic representation (as specified in NIST Special Publication 800-73, Interfaces for Personal Identity Verification [SP800-73] and NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification [SP800-76]) of the Cardholder Facial Image printed on the card. A new facial image will be collected each time a card is issued, and if a new card is being issued to an existing subscriber, existing biometrics must be verified. Fingerprints will be stored on the card for automated authentication during card usage. Section 12 provides additional biometric formatting information. For PIV-I identity proofing, registration and issuance process, the ORC ECA PIVotal ID follows 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, as detailed in Section 5.2.4.

3.2.3.2 Electronic Authentication

The ORC ECA accepts electronic authentication for renewal and re-key requests using currently valid digital certificates issued by the ORC ECA asserting the following OIDs: id-eca-medium, id-eca-medium-hardware, id-eca-medium-token, id-eca-medium-sha256, id-eca-medium-token-sha256. For certificates asserting id-eca-medium and id-eca-medium-sha256, the ORC ECA accepts electronic authentication for re-key of a Subscriber's certificates as described in Section 4.7. For certificates asserting id-eca-medium-hardware, id-eca-medium-token and id-eca-medium-token-sha256, the ORC ECA accepts electronic authentication for renewal of a Subscriber's certificates as described in this Section 4.6.

3.2.3.3 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 5.2.1.3.8. The PKI Sponsor is responsible for providing the ORC ECA, or approved LRAs, 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 ECA to communicate with the PKI sponsor when required

An ORC RA 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 will be accomplished by one of the following methods:

- Verification of digitally signed messages sent from PKI sponsors (using ORC ECA certificates of equivalent or greater assurance than that being requested). This verification is performed by the LRA reviewing the certificate that signed the email. The LRA confirms that the certificate policies asserted in the signature certificate of the sender show a level of assurance equivalent to or higher and that the assurance level of the certificate being requested by accessing "Message Security" and "View Signature Certificate" and verifying the digitally signed email sent from PKI sponsors includes a valid digital signature, the message has not been altered since it was sent, and that the trust path consists of the ECA Root and an ORC ECA CA.
- 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.

For certificates asserting id-eca-contentsigning-pivi, the PKI Sponsor must either have their identity verified in-person by a CMA as stipulated in Section 3.2.3.1 or must have a certificate that asserts id-eca-medium-hardware or id-eca-medium-hardware-pivi issued by the ORC ECA, verified by examining the trust chain of the certificate to ensure that the CA certificate was issued by the ECA Root certificate and is an ORC ECA CA. PKI Sponsors for certificates asserting id-eca-contentsigning-pivi must also be appointed in writing by an approving authority or be party to a contract with ORC for issuance services explicitly specifying the individual. Certificates asserting id-eca-contentsigning-pivi will be issued in accordance with Section 4.3.

3.2.4 Non-Verified Subscriber Information

ORC ECA issued certificates only contain information that is verified through the application process and generated in accordance with the process described herein.

3.2.5 Validation of Authority

Certificates that contain explicit or implicit organization affiliations will be issued only after ascertaining the Subscriber has the authorizations to act on behalf of the organization in the implied capacity. Examples of these include CAA, RA, LRA, and Group/Role certificates. ORC accomplishes this validation for CAA, RA and LRA via an Organizational Affiliation letter which is available on the ORC ECA website. The Organizational Affiliation letter must be completed on company/organization letterhead and submitted with the certificate request documentation. ORC ECA does not currently support the issuance of Group/Role certificates.

3.2.6 Criteria for Interoperation

The Certificate and CRL Profile in this CPS form a basis for assessing interoperability with the ECA PKI. However, the decision to cross certify the ORC Certificate and CRL Profiles with the ECA will reside with the EPMA, as specified in Section 1 of the ECA CP.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The ORC ECA accepts electronic authentication for re-key using currently valid digital certificates issued by the ORC ECA to a subscriber. For certificates asserting the following OIDs: id-eca-medium and id-eca-medium-sha256 a Subscriber may submit a re-key request under a client authenticated TLS session within a window 30 days prior to expiration until expiration of the Subscriber's certificate. The Subscriber is provided a web form that resides on the ORC ECA. The web form initiates a client authenticated TLS session with the Subscriber's browser and queries the Subscriber's browser for an ORC ECA digital certificate that meets the following conditions:

- The certificate presented is issued by the ORC ECA.
- The certificate presented has a private key associated with it.
- The certificate presented is a digital signature certificate.
- The certificate is not expired.

- The certificate is within 30 days of its expiration date.
- The certificate is currently valid and does not appear on the Certificate Revocation List (CRL) of the Certificate Authority that issued the certificate.

Upon successful authentication of the Subscriber's certificate, the ORC ECA captures data elements from the Subscriber's certificate to include: CA Issuer, Distinguished Name (DN), and the certificate serial number. The ORC ECA searches the internal certificate repository for the original request tied to the Subscriber's certificate presented and retrieves that information for use in the submittal form. Additionally, the ORC ECA searches the certificate repository for currently valid encryption certificates that may be issued to that Subscriber. If a current and valid encryption certificate is found, the ORC ECA retrieves the original request information for the encryption certificate for use in the submittal form. The ORC ECA will verify in the certificate repository that the next in-person authentication date will not be exceeded or that the number of re-keys permitted without in-person authentication by the issuance of a re-keyed certificate. The ORC ECA accomplishes this by checking flag fields in the Subscriber's entry in the certificate repository that are set upon Subscriber's first certificate issuance. This flag field has values of 0,1 and 2 to denote the number of re-keys performed by the Subscriber without in-person authentication. A value of 2 denotes that the user has performed 2 re-keys without in-person authentication and will not be allowed to complete the re-keys process and be directed to the in-person authentication process to obtain new keys and certificates. If the value of the flag field is 0 or 1, the Subscriber may now submit re-key requests for their digital signature and encryption (if applicable) certificates at this time.

The re-key requests are pre-populated with the information from the previous requests and issued certificates and are unalterable by the Subscriber. This information will include:

- Assurance level of the certificate to be re-keyed is contained in the original request retrieved by the ORC ECA. This retrieved record contains the profile information on the ORC ECA that created the certificate presented during electronic authentication and the re-key request is submitted against that same profile. The Subscriber is unable to change the assurance level during the re-key process.
- The Distinguished Name (DN) of the certificate to be re-keyed which contains the ORC Unique Identification String previously assigned.

- All data in certificate that can be used to provide authentication information such as email address, Public Key Information and Subject Key Information.
- Validity period of request (Subscriber determined) cannot exceed the maximum key life determined by ECA policy. Maximum validity period that the Subscriber can request is 3 years.

In all cases, ORC may request additional information or verification if deemed necessary to confirm the requestor's identity. ORC LRAs will contact the Subscribers via phone or email.

3.3.2 Identification and Authentication for Re-Key After Revocation

Identification and authentication of individuals for re-key after certificate revocation requires the steps for initial registration, as outlined in Section 3.2.3.1.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated, refer to Section 4.9.3. Certificate revocation requests may be made using the same practices as certificate issuance requests in accordance with Section 4.9.3. In addition, certificate revocation requests may be made electronically using electronic mail digitally signed by a certificate of equal or greater level of assurance than that of the certificate that the request is for. In either case, the request must additionally include the reason for revocation. See Section 4.9 for details on certificate revocation procedures.

A Subscriber may request revocation of a certificate, by authenticating to the CA revocation web interface, regardless of whether or not it has been compromised. The ORC RA may revoke a subscriber's certificate for cause. The LRA will collect signed documentation stating the reason and circumstances for the revocation. If an LRA performs this on behalf of a subscriber, a formal, signed message format known to the ORC RA will be employed.

4 Certificate Life-Cycle Operational Requirements

The ORC ECA is comprised of components that include Certificate Authorities, Card Management Systems (CMS) and Card Management Workstations.

In all cases, ORC ARA, ORC PIVotal ID and RA Workstations are maintained with all controls and procedures for the RA workstation as described throughout this CPS.

4.1 Certificate Application

The ORC ECA offers certificates that may assert any of the policy OIDs listed in Section 1.2. The ORC ECA CAs are configured with certificate profiles for each of the types listed in Section 1.2. The profiles are configured with the appropriate extensions and values for each certificate type as specified in Section 7. Certificate policies are encoded in the certificate profile of the ORC ECA CAs and cannot be overwritten by any certificate policy asserted in the certificate request. Certificate requests are submitted against a particular profile on the ORC ECA CAs and cannot be transferred to a different profile.

The ORC ECA is not authorized to issue a certificate for another Certification Authority or a subordinate ORC ECA Certification Authority.

4.1.1 Who Can Submit a Certificate Application

ORC only accepts certificate applications from Subscribers, either for themselves or as the designated certificate holder for a component or device. ORC does not allow for certificate requests to be made by an RA on behalf of a subscriber.

4.1.2 Enrollment Process and Responsibilities

The ORC ECA employs various methods for enrolling Subscribers, utilizing either a manual process or automated processes controlled by either the ORC ARA or the ORC PIVotal ID. ORC ECA provides either a Federal Information Processing Standards (FIPS) 140-2 level 3 Secure Socket Layer (SSL) connection to the certification authority, or a FIPS 201-approved Card Management System (CMS) via a FIPS 140-2 level 1 or 2 client for connection during enrollment. These various processes are detailed in this section.

4.1.2.1 Manual Enrollment Process and Responsibilities

The ORC ECA employs manual enrollment processes for the following certificate types:

- Subscriber Identity and Encryption
- Subscriber Code Signing
- Component that include:
  - Server (SSL)
  - Domain Controller
  - Device Identity

4.1.2.2 ORC PIVotal ID and ARA Enrollment Process and Responsibilities

The ORC PIVotal ID is used to manage the enrollment process for only the following certificate types:

- id-eca-medium-hardware-pivi
- id-eca-cardauth-pivi

Subscribers asserting an Organizational Affiliation must be authorized by a PKI Point of Contact for that Organization, as defined in Section 1.3.5.4. Subscribers asserting no Organization Affiliation will assert an Organization Unit value of Unaffiliated in their Distinguished Name.

Subscribers requesting certificates via the ARA are required to follow the identity proofing requirements in accordance with Section 3.2.3.1 to complete the enrollment process.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

All certificate requests will be validated through the authentication procedures in Section 3. It is the responsibility of the Subscriber to present the required information to the identity-verifying agent (RA or Trusted Agent) truthfully and in person.

4.2.2 Approval or Rejection of Certificate Applications

Identification and Authentication procedures will be performed as detailed in Section 3.

No certificates will be issued prior to proper authentication.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

.

At the time of issuance, the RA:

- determines the proposed subscriber DN,
- verifies uniqueness of subscriber DN against the subscriber base

  (this includes a search of current and prior CAs to avoid duplications/collisions)
- verifies the DN string integrity and uniformity within a specific organization, where applicable
- RA matches the request ID number provided in the request
- reviews certificate body content against LRA approval
- issues certificate, ensuring proper publication to the repository
- sends certificate issuance notification (CIN) to subscriber's

In the case of issuance using the ORC PIVotal ID, an ORC PIVotal ID Issuer accesses an ORC PIVotal ID workstation comprised of a desktop or laptop and various peripherals. An ORC PIVotal ID Issuer follows the workflow via the ORC PIVotal ID workstation for issuance of id-eca-medium-hardware-pivi and id-eca-cardauth-pivi only.

The ORC PIVotal ID Issuer will compare the identity documentation provided by the Subscriber against the identity documentation presented and recorded during the registration process described in Section 4.1.2.3. Upon successful verification of the identity documentation, the ORC PIVotal ID Issuer will print the Subscriber's PIV-I credential in accordance with Section 12. After the card has been successfully printed, the Subscriber will authenticate with one of the fingerprints captured during the registration process and create a numeric PIN as specified in Section 6.4.1. Upon successful fingerprint match and setting of PIN, Subscriber's card begins the activation process. Upon successful completion of the PIV-I Card Activation, the Subscriber must attest to the Subscriber Obligations. Upon acceptance by the Subscriber of the Subscriber Obligations, the ORC PIVotalID Issuer will release the activated card to the Subscriber.

In the case of issuing using the ORC ECA ARA, the ARA workstation is similar to the PIVotal ID workstation, but may also include tokens other than smartcards. The process for the ORC ECA ARA follows a similar

methodology as the PIVotal ID process, but is only for the issuance of id-eca-medium, id-eca-medium-hardware, id-eca-medium-token, id-eca-medium-sha256, id-eca-medium-token-sha256, id-eca-medium-device-sha256 certificates.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The ORC ECA RA will notify the certificate Subscriber of certificate issuance through electronic mail. The notification will include the URL that the Subscriber will use to receive the approved certificate. ORC uses a delivery template Certificate Issuance Notification email which contains a URL to download the Subscriber's issued certificate based on the issuing CA and Subscriber's certificate serial number. The ORC ECA will verify possession of the Subscriber's private key at the time the Subscriber accepts the issued certificate, as described in Section 3.2.1.

The notification will inform the Subscriber of the creation of a certificate, direct the Subscriber to the certificate contents page and reaffirm the Subscriber's responsibilities. The notification will inform the Subscriber if the private key has been escrowed. The Subscriber Obligations Agreement includes the following Subscriber obligations. The Subscriber will:

- Accurately represent themselves in all communications with the ORC ECA infrastructure
- Protect their private keys at all times, in accordance with this CPS as stipulated in their certificate acceptance agreements, and local procedures
- Notify, in a timely manner, the ORC ECA of 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 Obligations Agreement), and the certificate can only be accepted during a proof of possession of private key test. The ORC ECA will log the acceptance of the certificate.

It is not possible for a Subscriber to make effective use of their private key until they import their issued certificate. Successful importation constitutes certificate acceptance. The CA records the importation to the directory

entry for that respective certificate. A Subscriber who does not import his or her approved certificate will forfeit all claims he or she may have against the ORC ECA infrastructure in the event of a dispute arising from the failure to fulfill the obligations above., A Subscriber who is found to have acted in a manner counter to these obligations will have their certificate revoked, and will forfeit all claims he or she may have against the ORC ECA infrastructure in the event of a dispute arising from the failure to fulfill the obligations above.

For issuance from the ORC PIVotal ID or ARA, the Subscriber is notified at time of certificate issuance. An ORC PIVotalID Issuer accesses the CMS in order to provide issuance services. This Issuer will review the identity documentation provided by the Subscriber. This Issuer will capture a single representation of a fingerprint from the Subscriber for comparison against a representation captured by the Registrar. This Issuer will capture a user-defined numeric PIN from the Subscriber. Upon acceptance by the Subscriber of the Subscriber Obligations, the ORC PIVotal ID Issuer will issue the activated card to the Subscriber.

4.4 Certificate Acceptance

Successful importation constitutes certificate acceptance. The ORC ECA CA records the importation to the directory entry for that respective certificate. For issuance from the ORC PIVotal ID or ARA, the Subscriber electronically acknowledges acceptance of certificates at the time of issuance, as described in Section 4.3.2.

4.4.1 Conduct Constituting Certificate Acceptance

Subscriber signature (wet or digital) on certificate application and lack of objection to published certificate constitutes certificate acceptance. The Subscriber signature is collected before the ORC ECA CA allows a Subscriber to make effective use of its private key.

For issuance from the ORC PIVotal ID or ARA, electronic acknowledgement at the time of issuance constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

The ORC ECA CA certificates and Subscriber encryption certificates are published to the appropriate repositories. The ORC ECA 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 ECA
- A current and accurate CRL for all Certificate Authorities of the ORC ECA
- A copy or link to the current US Government ECA CP
- An abridged version of this approved CPS, which will include at a minimum the sections itemized below and all obligations and requirements levied on entities external to the ORC ECA
- Section 1.5.2, ORC ECA Contact Information
- Section 3.2, Initial Identity Validation
- Section 4.9, Certificate Revocation and Suspension
- Section 1.5, Certificate Policy Administration
- Any additional policy, waiver, or practice information that is supplemental to the US Government ECA CP or this CPS

The repository is located at http://eca.orc.com.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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 not use the signature private key after the associated certificate has been revoked or expired
- Subscriber may use decryption private key solely to decrypt previously encrypted information after the associated certificate has been revoked or expired
- To protect the certificate private key from unauthorized access, as stipulated in their certificate acceptance agreements, and local procedures
- To immediately report to an RA, as defined in Section 3.2.3.1, and request certificate revocation if private key compromise is suspected
- To use the certificate only for authorized PKE certificate enabled applications which have met the requirements of the US Government ECA CP and this CPS

- To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension
- Wherever the extended key usage extension is present in Subscriber certificates, Subscriber will use the associated certificate for only the purposes defined in the extended key usage extension
- To report any changes to information contained in the certificate to the appropriate RA, as defined in Section 1.3.4, 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 or issuance process for ORC PIVotal ID or ARA, in the form of a Subscriber Agreement that the Subscriber must agree to prior to process completion. Additional Subscriber obligations can be found in Section 4.1.2. Theft, compromise or misuse of the private key may cause the Subscriber, Relying Party and their organization legal consequences.

4.5.2 Relying Party Public Key and Certificate Usage

The ORC ECA will publicly post a summary of this CPS on the ORC ECA website (eca.orc.com) to provide the relying party information regarding the expectation of the ORC ECA. 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 ECA who issued the certificate they are about to rely on as stipulated in the US Government ECA CP
- To establish trust in the ECA Root and the ORC ECA 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 ECA,

this trust anchor will be the US Government ECA 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 US Government ECA 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

4.6 Certificate Renewal

The ORC ECA accepts electronic authentication for certificate renewal using currently valid digital certificates issued by the ORC ECA asserting id-eca-medium-hardware, id-eca-medium-token and id-eca-medium-token-sha256.

Subscribers may submit a renewal request under a client authenticated TLS session within a window 30 days prior to expiration until expiration of the Subscriber's certificate.

4.6.1 Circumstances for Certificate Renewal

The ORC ECA accepts requests for certificate renewal pursuant to the following circumstances:

- Public key of the Subscriber has not reached the end of its validity
- The Subscriber certificate has not been revoked
- Total lifetimes of certificate issued to the Subscriber (including new certificate) for that public key has not exceeded the next in-person identity proofing date
- Associated private key of the Subscriber's certificate has not been compromised
- Subscriber's name and attributes in the current valid certificate remain the same.

4.6.2 Subscribers are notified via automated email, 30 days prior to expiration and again 15 days prior to expiration, that their Subscriber certificates about to expire. The automated email provides a link to the ORC ECA website where subscribers may submit certificate renewal requests. Who May Request Renewal

Subscribers, as defined in Section 1.3.5, RAs, as defined in Section 1.3.4 LRAs, as defined in Section 1.3.7.1.2 and ORC Partner LRAs as defined in Section 1.3.7.1.3 who have certificates asserting id-eca-medium-hardware, id-eca-medium-token and id-eca-medium-token-sha256 may renew their certificates as detailed in Section 4.6.

4.6.3 Processing Certificate Renewal Requests

The renewal process will be in accordance with the certificate issuance process described in Section 3.2. Identity validation may be in accordance with either Section 3.2.3.1 or Section 4.3.1.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to other Entities

See Section 4.4.3.

4.7 Certificate Re-Key

The ORC ECA accepts electronic authentication for re-key using currently valid digital certificates issued by the ORC ECA asserting id-eca-medium and id-eca-medium-sha256. No other certificate types are re-keyed under the ORC ECA.

Subscribers may submit a re-key request under a client authenticated TLS session within a window 30 days prior to expiration until expiration of the Subscriber's certificate that meets the following conditions:

- The certificate presented is issued by the ORC ECA.
- The certificate presented has a private key associated with it.
- The certificate presented is a digital signature certificate.
- The certificate is not expired.
- The certificate is within 30 days of its expiration date.
- The certificate is currently valid and does not appear on the Certificate Revocation List (CRL) of the Certificate Authority that issued the certificate.
- The certificate asserts an OID for which re-key is permitted.

4.7.1 Circumstances for Certificate Re-Key

The ORC ECA accepts requests for certificate re-key pursuant to the following circumstances:

- Subscriber certificate can no longer be renewed, as stipulated in Section 4.6
- The Subscriber certificate has not been revoked
- Total lifetimes of certificate issued to the Subscriber (including new certificate) for that public key has not exceeded the next in-person identity proofing date
- Associated private key of the Subscriber's certificate has not been compromised
- Subscriber's name and attributes in the current valid certificate remain the same.

4.7.2 Who May Request Certification of a New Public Key

The Subscriber or LRA may request issuance of the re-key of a Subscriber certificate.

4.7.3 Processing Certificate Re-Keying Requests

Requests for certificate re-key are marked as "certificate renewal request"[5]. ORC will not issue a certificate such that the Subscriber would have more than one valid, certificate of the same assurance level and type to the same entity. If a Subscriber should make such a certificate request, ORC would revoke any certificate that would otherwise lead to a Subscriber possessing more than one valid certificate at one time. Such situations can arise when a Subscriber experiences technical issues and has failed to make

[5] The use of the term "renewal" is used for simplification on the part of the subscriber so as not to confuse between renew and re-key. This is done for internal use only.

operational copies of their certificates. ORC does not revoke the certificate in the case where a certificate nearing expiration is re-keyed to produce a certificate that becomes valid as the old certificate expires.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

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 ECA may choose to update a certificate of a Subscriber who mistyped their email address. The old certificate is revoked, and therefore cannot be further re-keyed, renewed, or updated.

4.8.1 Circumstances for Certificate Modification

An ORC ECA issued certificate may be modified if some of the information other than the DN, such as the e-mail address, 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 requests certificate modification to the LRA. The LRA confirms the desired modification of a Subscriber certificate and forwards the modification request to the RA. The LRA will validate any changes in the subscriber authorizations reflected in the certificate such as email address, or length of validity period 1, 2, or 3 year.

4.8.3 Processing Certificate Modification Requests

Subscribers submit requests for certificate modification in writing, via email, or via help-desk requests. ORC ECA personnel may verify the need for the modification and gather data (such as certificate CN/DN, serial numbers, validity dates, etc.) to pass on to the RA/LRA.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A Subscriber, or a Sponsoring Organization (where applicable), is responsible for promptly requesting revocation of any ORC ECA certificate for any of the reasons listed below. Certificates will only be revoked in the following circumstances:

- The certificate holder requests that the certificate be revoked
- The certificate holder can be shown to have violated the Subscriber Obligations, including non-payment of any required fees
- The certificate holder is no longer authorized to hold the certificate (e.g. termination of employment, change in responsibilities)
- 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 ECA issued certificate at its discretion.

Whenever any of the above circumstances occur, the associated certificate will be revoked and placed on the CRL. 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 via that compromised key from the date of known compromise forward will be revoked, as detailed in Section 4.9.12. Certificates will remain on the CRL until they expire. They are removed after they expire, but must at least appear in one CRL.

Subscribers leaving the organization that sponsored their participation in the ECA PKI are required to surrender to their organization's PKI PoC (through any accountable mechanism) all cryptographic hardware tokens that were issued, under the sponsoring organization, prior to leaving the organization. The sponsoring organization is responsible for taking possession of all cryptographic hardware tokens containing ECA certificates and issued under the sponsoring organization. The PKI PoC must zeroize or destroy the token promptly upon surrender and must protect the token from malicious use from the time of surrender. In all cases, regardless of certificate assurance level, the organization must promptly notify an ORC LRA to revoke the certificate, providing the

- Subscriber’s name,
- Subscriber’s Organization name,
- Subscriber’s email address, and
- Subscriber’s Issuer Distinguished Name (CA name)

The ORC LRA searches the ORC ECA CAs for certificates issued to the Subscriber and identifies certificates by verifying Subscriber Name, Organization, email address. The LRA then notes the serial number(s) and date of issuance of every current certificate issued to that Subscriber and sends a request to the RA for revocation of those certificates. The organization must also attest to the disposition of the token (if applicable), via a digitally signed e-mail. Cryptographic hardware tokens can be

identified by their unique 'serial number' (often a CUID number on the chip) and/or by the certificates on the cryptographic hardware token.

For certificates asserting id-eca-medium-hardware-pivi and id-eca-cardauth-pivi that express an organizational affiliation, the organization's PKI Point of Contact (PoC) must inform the ORC ECA of any changes in a Subscriber's affiliation through a digitally signed email or through a digitally signed transaction through the ORC PIVotal ID. If the Affiliated Organization no longer authorizes the affiliation of a Subscriber, the ORC ECA will revoke any certificates issued to that Subscriber containing the organization affiliation. If an Affiliated Organization terminates its relationship with the ORC ECA such that it no longer provides updates to organizational affiliation information, the ORC ECA will revoke all certificates containing that Affiliated Organization's information.

For certificates asserting id-eca-contentsigning-pivi and issued to an Affiliated Organization that is party to a contract with ORC for issuance services, upon completion, termination or breach of contract the ORC ECA will revoke the certificate asserting id-eca-contentsigning-pivi for that Affiliated Organization. The ORC ECA will also revoke all certificates issued by the PIVotalID system to which the revoked content signer certificate was issued. PIVotalID credentials issued from that system are identified by the connector certificate issued to that PIVotalID system. Any Subscriber certificates with an "issuedby" that connector certificate will be revoked.

4.9.2 Who Can Request Revocation

The following authorized parties may request a revocation of a certificate:

- Any Subscriber may request revocation of their own certificate(s) and LRAs, ORC PIVotal ID Issuers, ORC PIVotal ID Registrars or PKI Point of Contact may request revocation of any Subscriber certificate on behalf of the Subscriber or other authorized party
- The ORC RA may revoke any ORC ECA issued certificate for reasons identified in this CPS
- Persons appointed by the EPMA to request revocation of any subscriber or CA certificate.

- Other parties may also request revocation of certificates through an LRA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar or ORC Partner LRA (only within their domain). The RA or LRA will validate the credentials of the requesting party, including verification that the revocation request is from an LRA within the same organization/domain as the Subscriber and the RA will determine if the revocation request meets the requirements. The process the RA uses to verify the revocation request includes:

- Revocation forms provided on the website (both for individual and for organizational) and submitted to ORC
- Email requests that are digitally signed are verified via the signing certificate
  - Verifying Issuer DN
  - Verifying CN
  - Verifying email signing certificate match
  - Verifying current validity date
- Email requests that are not signed require additional investigation by the RA as to the relationship of the revocation requestor to the individual whose certificate is being requested to be revoked.

When the LRA validates the credentials of the requesting party, the LRA subsequently notifies the RA or CMS Registrar via signed email that the credentials of the requesting party have been validated

- When revocation of an end entity certificate is requested by a duly authorized representative of the end entity's organization the LRA will verify the credentials and authority of the duly authorized representative to request revocation

If any individual has reason to believe that a certificate private key has been compromised, that individual is required to notify an LRA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar or ORC Partner LRA of the compromise suspicion. It is the responsibility of the RA or ORC PIVotal ID Registrar to investigate the information and determine if certificate revocation is warranted, based on communications with either the end entity, an LRA or a duly authorized representative of the end entity's organization. The RA will verify the Subscriber Name, Organization and email address associated with the certificate to be revoked. If there is ambuiguity, ORC will investigate for additional information to ensure accuracy.

If so, the RA or ORC PIVotal Registrar will forward the revocation request via digitally signed email to the RA or ORC PIVotal Issuer, along with documentation of the reason for the request to the RA. ORC will send a written notice and brief explanation for the revocation to the Subscriber.

4.9.3 Procedure for Revocation Request

Revocation requests can be made through the Helpdesk or an ORC RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, LRA, or ORC Partner LRA via any process that sufficiently ensures identity validation of the party making the request, a clear explanation of the reason for revocation and

also the confirmation of the identity of the certificate to be revoked (e.g. certificate CN, certificate serial number, subscriber name, subscriber email address, subscriber organizational affiliation, issuer DN, date of issue). If a revocation request is not made to an ORC RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, LRA, or ORC Partner LRA, rather via a Help Desk call or directly to an RA or PIVotal ID Issuer, the revocation request will be forwarded to an ORC RA or ORC PIVotal ID Registrar for verification and processing. This process will be through digitally signed e-mail from our Trusted Role email account (i.e. ORC RA or our helpdesk email account) or manually through a signed letter delivered to ORC. A “form letter of revocation request” will be made available at the ORC ECA website or can be provided via a help desk request.

Upon receipt of a revocation request, an RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, LRA, or ORC Partner LRA will validate the credentials of the party making the request, either through digital signature verification or hard-copy written request. Hard-copy written requests will be on letterhead from the organization to which the certificate holder is, or was, associated with for possession of the certificate. If the named subscriber is requesting revocation of his/her own certificate, RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, LRA, ORC or Partner LRA action is required. RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, LRA, or ORC Partner LRA will validate the revocation requestor using the procedures outlined for initial certificate request validation. If an RA or PIVotal ID Issuer chooses to revoke a certificate because of sufficient evidence of noncompliance with this CPS, an RA, ORC PIVotal ID Issuer will document the reason for certificate revocation and will notify the subscriber of the revocation via the certificate authority management system and will notify the subscriber of the revocation via email.

An RA, ORC PIVotal ID Issue, ORC PIVotal ID Registrar, LRA,or ORC Partner LRA may request revocation of other entity certificates (e.g. code-signing certificates, component certificates). The RA, or ORC PIVotal ID Issuer will document the reason for the request via the certificate authority management system and archive this documentation. The ORC PIVotal ID Registrar, LRA, ORC Partner LRA will notify an RA, ORC or PIVotal ID Issuer of the revocation request, using a digitally signed e-mail. The RA or ORC PIVotal ID Issuer verifies the request by verifying the signature on the email from the RA or ORC PIVotal ID Issuer - by clicking on the icon red envelope in the upper right hand corner of the email message security – Message is signed “This messaged includes a valid signature” – View Identity certificate.

Other parties (e.g. existing subscribers, Organizational POCs, relying parties) requesting certificate revocation will present their request via digitally signed email or hardcopy to an ORC PIVotal ID Registrar, LRA, or

ORC Partner LRA. The ORC PIVotal ID Registrar, LRA or ORC Partner LRA will first determine if the party making the request is authorized to make such request against a list of authorized POCs maintained by the ORC RAs. Once this is completed, the ORC PIVotal ID Registrar, LRA or ORC Partner LRA will ascertain the circumstances prompting the request, validate the credentials of the party making the request, and determine if the revocation request is valid through an out of band investigation. If so, the ORC PIVotal ID Registrar, LRA or ORC Partner LRA will forward the request to an RA or PIVotal ID Issuer. The RA, ORC PIVotal ID Issuer will validate that the revocation request signer is an authorized ORC PIVotal ID Registrar, LRA or ORC Partner LRA by checking the certificate used to sign the request.

If the RA or ORC PIVotal ID Issuer determines there is a need to revoke the certificate once an authorized request is received, the RA or ORC PIVotal ID Issuer will revoke the certificate by accessing the certificate management system and selecting the “revoke certificate” option, which then places the serial number and certificate revocation date on a CRL. The RA or ORC PIVotal IDIssuer will also remove the certificate from the master directory and any replicated directories.

Whenever the reason for revocation is due to key compromise or suspected fraudulent use, both the Subscriber and the , RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, LRA, ORC Partner LRA must so indicate that reason in their respective revocation request email.

Subscribers leaving the organizations that sponsored their participation in the PKI will surrender to their organization's PKI point of contact (through any accountable mechanism) all cryptographic hardware tokens that were issued, under the sponsoring organization, prior to leaving the organization. PIVotalID and ARA systems associate the hardware token to the Subscriber during the issuance process. The PKI point of contact will zeroize (only if token reuse is desired and allowed, and if token unlock code is known) or destroy the token promptly upon surrender and will protect the token from malicious use between surrender and zeroization or destruction. Subscriber tokens are the responsibility of the sponsoring organization, including procurement and final disposition. At the time of certificate request, the LRA will record the serial number of the token for the Subscriber and include that information in the email sent to the ORC RA. In all cases, whether software or hardware tokens are involved, the organization will promptly notify an ORC PIVotal ID Registrar, LRA, or ORC Partner LRA to revoke the certificate, via a digitally signed email. In all cases, whether software or hardware tokens are involved, when key compromise is suspected or confirmed by the sponsoring organization, the PKI point of contact will immediately notify an ORC PIVotal ID Registrar, LRA, ORC Partner LRA to revoke the certificates issued. In the event that the subscriber does not surrender their hardware tokens to PKI point of contact, the PKI point of

contact must immediately notify an ORC PIVotal ID Registrar, LRA, ORC Partner LRA to revoke the certificates issued to that token. The PKI PoC will be authenticated/validated, as described at the top of this section. Certificates issued via the ORC ECA PIVotal ID will be revoked via the ORC PIVotal ID CMS for reason of Key Compromise. Certificates issued via the ORC ARA will be revoked via the ARA for reason of Key Compromise. For any certificate not issued via an ORC ECA PIVotal ID workstation or ORC ECA ARA workstation, the certificate(s) will be revoked by an ORC RA via the ORC RA workstation for reason of key compromise.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which CA Must Process the Revocation Request

The ORC ECA processes all revocation requests within one hour of receipt. CRL issuance frequency is addressed in Section 4.9.7.

4.9.6 Revocation Checking Requirements for Relying Parties

It is the responsibility of the relying party to verify that certificates have not been revoked. Certificates may be stored locally by a relying party, but should be validated at least daily before use. The relying party will always check a certificate against a CRL that has not expired.

Any relying party that downloads the CRL will verify the authenticity of the CRL by verifying the signature and associated certification path. They should also check the CRL date to confirm that old CRLs are not presented in a replay attack. The following text will be included in the Subscriber Agreement and posted on the ORC ECA website:

USE OF REVOKED CERTIFICATES COULD HAVE DAMAGING OR CATASTROPHIC CONSEQUENCES IN CERTAIN APPLICATIONS. THE MATTER OF HOW OFTEN NEW REVOCATION DATA SHOULD BE OBTAINED IS A DETERMINATION TO BE MADE BY THE RELYING PARTY AND THE SYSTEM ACCREDITOR. IF IT IS TEMPORARILY INFEASIBLE TO OBTAIN REVOCATION INFORMATION, THEN THE RELYING PARTY MUST EITHER REJECT USE OF THE CERTIFICATE, OR MAKE AN INFORMED DECISION TO ACCEPT THE RISK, RESPONSIBILITY, AND CONSEQUENCES FOR USING A CERTIFICATE

WHOSE AUTHENTICITY CANNOT BE GUARANTEED TO THE STANDARDS OF THIS PRACTICE STATEMENT.

4.9.7 CRL Issuance Frequency

The ORC ECA is required to issue CRLs daily. The ORC ECA chooses to issue a CRL every 12 hours. The CRLs are issued with a validity period of 7 days. A new CRL will be issued twice per day even if there are no changes or updates to be made. The "nextUpdate" field in the CRL will be no more than 7 days from "thisUpdate" field of the CRL. If a revocation request is granted for the reason of key compromise, a new CRL will be generated as quickly as is feasible and will be posted within 12 hours of receipt of the request. Superseded CRLs will be removed from the repository upon posting of the latest CRL.

HTTP CRL locations can be found in the CRL DP attribute of each certificate issued by the ORC ECA. .

The above CRL information is provided to Subscribers during certificate request or issuance, and is made readily available to any potential Relying Party via the ORC ECA website.

The EPMA will notify immediately any externally certified CAs in the event of ECA Root CA or any subordinate CA revocation for any reason.

4.9.8 Maximum Latency for CRLs

CAs are configured to auto-issue a CRL every 12 hours, and the CRL will be posted upon generation, but within no more than four hours after generation. The system is configured to publish to our public repository 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

The ORC ECA CSA (a delegated-trust OCSP responder) ensures that:

- An accurate and up-to-date CRL, from the authorized ECA, is used to provide the revocation status
- Latency of certificate status information meets or exceeds the requirements for CRL issuance;

- The ORC ECA CSA processes requests and provides responses compliant with RFC 2560; and
- Each ORC ECA Certification Authority issues an OCSP Responder certificate according to the profile stipulated in Section 10.13.

The ORC ECA CSA is a centralized validation server that provides OCSP responses for all certificates the ORC ECA issues. All OCSP Responder keys are unique to the Certification Authority they represent and are protected by a hardware security module. OCSP Responder certificates signing responses for certificates that assert id-eca-medium, id-eca-medium-hardware and id-eca-medium-token will use the SHA-1 algorithm and only sign requests for those certificate policies. OCSP Responder certificates signing responses for certificates that assert id-eca-medium-sha256, id-eca-medium-token-sha256, id-eca-medium-hardware-pivi, id-carduth-pivi, id-eca-contentsigning-pivi and id-eca-medium-device-sha256 will use the SHA-256 algorithm and only sign requests for those certificate policies. No SHA-1 OCSP Responder certificate will sign responses for a SHA-256 ORC ECA certificate. Conversely, no SHA-256 OCSP Responder certificate will sign responses for a SHA-1 ORC ECA certificate.

This process is a manual process performed under two-person control in the cage where the ORC ECA CA and ORC ECA OCSP Responders are physically located. The CAA accesses the ORC ECA server and then the SA provides root access. The CAA then accesses the CSA software and generates a new certificate signing request (CSR) based on a new private key being generated. The CAA then submits the CSR to the ORC ECA CA for signing. The CAA issues the certificate in accordance with Section 10.13. The CAA then installs the new certificate into the CSA. The ability to issue OCSP certificates is restricted to the CAAs using procedural means; RAs are trained to not request or revoke OCSP Responder certificates.

The ORC ECA CSA is configured to retrieve the CRL from each CA every 15 minutes. The ORC ECA CSA will only retrieve the CRL if the CRL is different from the CRL it currently has for that ORC ECA CA.

ORC disclaims any liability for loss due to use of any validation information relied on by any party that does not comply with this stipulation.

4.9.10 On-Line Revocation Checking Requirements

As stipulated by the ECA CP:

- Relying Parties may optionally use on-line status checking. Since some relying parties may not be able to accommodate on-line communications, the ORC ECA supports CRLs. Client software using on-line revocation checking need not obtain CRLs.

- Relying parties (including CMAs) will only rely upon OCSP Responders approved in accordance with the requirements of the ECA CP.

ORC ECA OCSP responders have been evaluated and found to be in compliance with and approved for use by relying parties for ORC ECA revocation status checking.

4.9.11 Other Forms of Revocation Advertisements Available

The ORC ECA generates, issues and publishes CRLs. The ORC ECA also provides OCSP responder service. The ORC ECA does not support any other forms of revocation advertisement.

4.9.12 Special Requirements Related to key Compromise

If a certificate is revoked because of suspicion of private key compromise, the following additional steps (in addition to steps specified above) occur:

- If the compromised certificate was an RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, ARA Issuer, ARA Registrar, LRA, or ORC Partner LRA certificate as defined in section 1.3, ORC will immediately revoke any subscriber certificates approved for issuance via that RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, ARA Issuer, ARA Registrar or LRA, ORC Partner LRA certificate issued after the date of the suspected compromise, and instruct those subscribers to make new certificate requests. ORC will determine the Subscriber population affected through review of emails notifying RAs for approval, ORC ECA CA certificate database that records certificates issued by an RA and ORC PIVotal ID and ARA that records certificates enrolled and /or issued by ORC PIVotal ID Registrar and Issuer and ORC ARA Registrar and Issuer.
- If an RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, ARA Issuer, ARA Registrar, LRA, or ORC Partner LRA as defined in section 1.3 key is compromised (or is suspected to be compromised), the certificate is revoked and a new CRL is published within the time specified in Section 4.9.7 and the RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, ARA Issuer, ARA Registrar, LRA, ORC Partner LRA obtains a new certificate, as authorized by the CAA.
- If an RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, ARA Issuer, ARA Registrar, LRA, or ORC Partner LRA as defined in section 1.3 key is compromised (or is suspected to be

compromised) and it cannot be determined, 1) on what date the compromise occurred or 2) if any subscriber certificates were submitted to the ORC ECA using the compromised key, all certificates issued based on that RA, ORC PIVotal ID Issuer, ORC PIVotal ID Registrar, ARA Issuer, ARA Registrar, LRA, or ORC Partner LRA key are immediately revoked. ORC will determine the Subscriber population affected through email notifying RAs for approval, ORC ECA CA certificate database that records certificates issued by an RA and ORC PIVotal ID and ARA that records certificates enrolled and /or issued by ORC PIVotal ID Registrar and Issuer and ORC ARA Registrar and Issuer.

The ORC ECA uses reason codes and has the ability to transition any reason code to compromise. The process is a manual process that must be accomplished by a CAA accompanied by an SA directly on the internal database managing the respective CA.

4.9.13 Circumstances for Suspension

The ORC ECA does not support certificate suspension. The ORC RAs are trained to use only approved revocation reasons of keyCompromise, caCompromise, affiliationChangede, superceded and cessationOfOperation. The ORC ECA PIVotal ID and the ORC ARA are configured to not allow a reason code certificateHold (Suspension).

4.9.14 Who Can Request Suspension

Not applicable, see Section 4.9.13.

4.9.15 Procedure for Suspension Requests

Not applicable, see Section 4.9.13.

4.9.16 Limits on Suspension Period

Not applicable, see Section 4.9.13.

4.10 Certificate Status Services

The ORC ECA operates a Certificate Status Authority (CSA) using an OCSP responder that provides revocation status. The ORC ECA CSA (OCSP responder) practices conform to the stipulations of the US Government ECA CP, applicable Internet Standards and this CPS. All ORC ECA CSA (OCSP responder) practice updates, as well as any subsequent

changes will be updated in this CPS and submitted to the EPMA for conformance assessment. The ORC ECA CSA (OCSP responder) practices include:

- Conformance to the stipulations of the US Government ECA CP, applicable Internet Standards and this CPS
- Ensuring that certificate and revocation information is accepted only from valid ORC ECA CAs
- Include only valid and appropriate responses
- Maintain evidence that due diligence is exercised in validating certificate status
- CSA certificates conform to OCSP profile in Section 10.13
- CSA certificates are valid for thirty (30) days, and renewed every seven (7) days
- ORC does not issue pre-signed OCSP responses
- ORC does not issue nonce-based OCSP responses

The ORC ECA does not implement CSS except OCSP, as described in this CPS. The ORC ECA does not currently support SCVP.

4.10.1 Operational Characteristics

ORC ECA Certificate Status Authorities will comply with the requirements of this CPS and the ECA CP, as detailed in Section 4.10.

4.10.2 Service Availability

The ORC ECA Certificate Status Authorities maintain service availability by striving to operate at 99% up-time annually.

4.10.3 Optional Features

The ORC ECA Certificate Status Authorities do not currently operate any optional features beyond those specified by the ECA CP, if any. .

4.11 End of Subscription

Subscription is synonymous with the certificate validity period. The subscription ends when the certificate is revoked or expired.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The ECA key escrow recovery policy is described in Key Recovery Policy for External Certification Authorities [ECAKRP].

The ORC ECA has established the ORC ECA Key Recovery Practice Statement (KRPS). The ORC ECA acknowledges that its KRPS must be approved by the EPMA prior to issuing and archiving encryption keys/certificates. The ORC ECA will follow the format and contents of the KRP, which provides a more detailed and concrete list of security requirements, which the key escrow and recovery system must satisfy in order to be approved by the EPMA.

ORC does not support escrow of ECA Medium, Medium SHA256, Medium HW, Medium Token, and Medium Token SHA256 encryption certficates.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

ECA and the ORC ECA do not support key recovery using key encapsulation techniques.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

ORC CA, RA workstation, ORC PIVotal ID, ARA, and CSA (OCSP responder) equipment consists of equipment dedicated to the CA, RA, ORC PIVotal ID, ARA, and CSA (OCSP responder) functions, and will not perform non-related functions. The equipment includes, but is not limited to, the system running the CA, RA, ORC PIVotal ID, ARA, and CSA (OCSP responder) software, hardware cryptographic modules, and databases and directories located on the equipment. Databases and directories located on the equipment will not be accessible to the Subscribers and Relying Parties.

Unauthorized use of ORC CA, RA, ORC PIVotal ID, ARA, and CSA (OCSP responder) 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.

5.1.1 Site Location and Construction

{Redacted for security purposes}

5.1.2 Physical Access

The ORC ECA server equipment is always protected from unauthorized access. Physical access security {Redacted for security purposes}.

5.1.3 Power and Air Conditioning

{Redacted for security purposes}

5.1.4 Water Exposure

{Redacted for security purposes}

5.1.5 Fire Prevention and Protection

{Redacted for security purposes}

5.1.6 Media Storage

{Redacted for security purposes}

5.1.7 Waste Disposal

{Redacted for security purposes}

5.1.8 Off-Site Backup

{Redacted for security purposes}

5.2 Procedural Controls

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. Details {Redacted for security purposes}

5.2.2 Number of Persons Required for Task

{Redacted for security purposes}

5.2.3 Identification and Authentication for Each Role

{Redacted for security purposes}

5.2.4 Roles Requiring Separation of Duties

{Redacted for security purposes}

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

{Redacted for security purposes}

5.3.2 Background Check Procedures

CAAs, RAs, SAs, and Security Auditors will either hold a US security clearance or go through a thorough background check covering the past seven years performed by a qualified investigator.

5.3.3 Training Requirements

{Redacted for security purposes}

5.3.4 Retraining Frequency and Requirements

{Redacted for security purposes}

5.3.5 Job Rotation Frequency and Sequence

{Redacted for security purposes}

5.3.6 Sanctions for Unauthorized Actions

{Redacted for security purposes}

5.3.7 Independent Contractor Requirements

{Redacted for security purposes}

5.3.8 Documentation Supplied to Personnel

{Redacted for security purposes}

5.4 Audit Logging Procedures

{Redacted for security purposes}

5.5 Records Archival

{Redacted for security purposes}

5.6 Key Changeover

{Redacted for security purposes}

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

{Redacted for security purposes}

5.7.2 Computing Resources, Software, and/or Data are Corrupted

{Redacted for security purposes}

5.7.3 Entity Private Key Compromise Procedures

{Redacted for security purposes}

5.7.4 Business Continuity Capabilities After a Disaster

{Redacted for security purposes}

5.8 CA or RA Termination

{Redacted for security purposes}

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

{Redacted for security purposes}

6.1.2 Private Key Delivery to Subscriber

In accordance with the ORC ECA and this CPS, in all cases the key is generated directly on the Subscriber's token. The Subscriber is in possession and control of the private key from the time of generation or benign transfer.

{Redacted for security purposes}

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered to the certificate issuer in a PKCS#10 certificate request only. The identification documents presented at the time of registration must match the identification documents presented at the time of issuance.

6.1.4 CA Public Key Delivery to Relying Parties

ORC will deliver the US Government ECA Root CA and ORC ECA CA public keys via a web interface to a protected server using SSL. The ORC ECA CA issues the web server its certificate. The public key will be 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 addition, during in-person authentication as described in Section 3.2.3.1, the ORC ECA will provide the ECA Root to these Subscribers.

6.1.5 Key Sizes

All ORC ECA keys employ at least 2048 bit RSA keys or 256 bit or stronger ECDSA modulus for issuing certificates and CRLs. Digital Signature Standard (DSS) is not supported.

6.1.6 Public Key Parameters Generation and Quality Checking

All RSA key pairs, including the prime numbers, are generated in accordance with the Digital Signature Standard [FIPS186-2], including primality tests. Public exponent is in the range specified in [FIPS 186-2].

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

The ORC ECA will certify keys for use in signing or encrypting, but not both with the exception of Component SSL certificates as specified in Section 10.7. The use of a specific key is determined by the key usage extension. The key usage extension will be included in all certificates and is always marked critical in order to limit the use of public key certificate for its intended purpose.

Certificates that assert id-eca-contentsiging-pivi will include an extended key usage of *id-fpki-pivi-content-signing* as described in the certificate profile in Section 10. Details {Redacted for security purposes}.

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 FIPS140-2]. Cryptographic modules used for the ORC ECA are validated to the FIPS 140-2 level identified in this section. All ORC ECA keys generated are done so using the associated FIPS 140-2 method inherent within the respective FIPS validated device (e.g. browser, HSM). Details {Redacted for security purposes}.

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

{Redacted for security purposes}.

6.2.3 Private Key Escrow

Under no circumstances will a non-repudiation signature key be escrowed, or held in trust by a third party other than the subscriber. ORC does not require private key escrow for confidentiality keys.

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

For certificates asserting id-eca-medium-token, id-eca-medium-token-sha256, id-eca-medium-hardware, id-eca-medium-hardware-pivi, and id-eca-medium-cardauth-pivi, Subscribers are notified that private signature keys may not be backed up or copied.

For id-eca-medium assurance only, ORC will recommend to Subscribers that they make an operational copy of software based encryption private keys (but not signature) and will provide recommended procedures. The backup private keys must be stored on a removable media and cannot be kept online.

Subscribers will also be advised that backup of private signature keys for the sole purpose of key recovery must not be made.

{Redacted for security purposes}.

6.2.5 Private Key Archival

See Sections 6.2.3 and 6.2.4.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Private keys will be generated by and in a cryptographic module using the FIPS 140-2 approved method inherent within the respective cryptographic module. {Redacted for security purposes}.

6.2.7 Private Key Storage on Cryptographic Module

The private key stored in the cryptographic module is protected from unauthorized access and use in accordance with the FIPS 140-2 requirements applicable for the module.

6.2.8 Method of Activating Private Key

6.2.9 {Redacted for security purposes}.Method of Deactivating Private key

{Redacted for security purposes}.

6.2.10 Method of Destroying Private Key

{Redacted for security purposes}.

6.2.11 Cryptographic Module Rating

Requirements for cryptographic modules are as stated above in Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Archival of public keys will be achieved via certificate archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The key usage periods for keying material are described in Section 4.7 and Section 5.6.

6.3.3 Subscriber Private Key Usage Environment

Subscribers affirm in the Subscriber agreement to use their private keys only on the machines that are protected and managed using commercial best practices.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

{Redacted for security purposes}.

6.4.2 Activation Data Protection

{Redacted for security purposes}.

6.4.3 Other Aspects of Activation Data

{Redacted for security purposes}.

6.5 Computer Security Controls

{Redacted for security purposes}.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

ORC ECA CAAs and SAs follow established procedures to ensure that the operational systems and networks adhere to the security requirements. These procedures are documented in the ORC System Security Plan and the supporting ORC policies and procedures. Integrity checks of the system data, software, discretionary access controls, audit profiles, firmware, and hardware are performed throughout the system life-cycle to ensure secure operation. Any system change to the ORC ECA is controlled and managed via ORC's Configuration Control Board process, as detailed in ORC's Systems Security Plan.

Details {Redacted for security purposes}.

6.6.2 Security Management Controls

{Redacted for security purposes}.

6.6.3 Life-Cycle Security Controls

{Redacted for security purposes}.

6.7 Network Security Controls

{Redacted for security purposes}.

6.8 Time-Stamping

The ORC ECA system provides time stamps for use in audit record generation. The ORC ECA synchronizes internal information system clocks.

7 Certificate, CRL, and OCSP Profiles

Section 10 contains the formats for the various certificates and CRLs.

7.1 Certificate Profile

7.1.1 Version Numbers(s)

The ORC ECA will issue X.509 Version 3 certificates.

7.1.2 Certificate Extensions

ORC ECA certificate profiles are in accordance with the requirements of the certificate profiles described in the US Government ECA CP.

Access control information may be carried in the subjectDirectoryAttributes non-critical extension.

7.1.3 Algorithm Object Identifiers

Certificates issued by the ORC ECA will use the following OIDs for signatures.

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha-256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
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}

Certificates under this Policy will use the following OIDs for identifying the algorithm for which the subject key was generated.

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-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public key-type (2) 1}
id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)}

For certificates that contain an elliptic curve public key, the parameters will be specified as one of the following named curves. In order to provide cryptographic separation for a closed community, when the subject public key is of the form id-ecDH, a private OID may be asserted to indicate a different base point on one of these curves.

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34}
ansip521r1	{iso(1) identified-organization(3) certicom(132) curve(0) 35}

The ORC ECA will certify only public keys associated with the crypto-algorithms identified above, and will only use the signature crypto-algorithms described above to sign certificates, certificate revocation lists and ORC's CSA (OCSP responder) ECA OCSP responses.

7.1.4 Name Forms

DNs will be used by the ORC ECA in the issuer and in subject fields of the certificates. X.500 Directories use the DN for lookups. All Relying Parties will have the ability to process DNs. If communities request to use other names, for example certificates used to implement a hardware protocol, where device addresses are most useful and certificate lookup is not performed ORC will define alternate name forms to be included in the subjectAltName extension and provide the alternative name form to the EPMA. Any name form defining GeneralName in [ISO9594-8] will be used, in accordance with the required profile (Section 7.1.2).

For attribute values other than domain component: The ORC ECA encodes all CA Distinguished Names (in various fields, e.g., Issuer, Subject, Subject Alternative Name, Name constraints) as printable strings. The ORC ECA encodes all subscriber DN portions that name constraints apply to as printable strings. For other portions of the subscriber DN, the ORC ECA encodes these values as printable strings, if possible. If a portion cannot be encoded as a printable string, then and only then will it be encoded using a different format and that format will be UTF8.

For domain component attribute values, The ORC ECA encodes all domain component attribute values as an IA5 string.

7.1.5 Name Constraints

Not applicable

7.1.6 Certificate Policy Object Identifier

Certificates issued by the ORC ECA will assert the OID appropriate to the level of assurance with which it was issued.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by the ORC ECA will not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The ORC ECA will not set the certificate policies extension to be critical. Relying Parties whose client software does not process this extension do so at their own risk.

7.2 CRL Profile

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are described in Section 10 and are in accordance with the US Government ECA CP CRL profile. The ORC ECA supports CRL Distribution Points (CRL DP) in all End Entity certificates.

7.3 OCSP Profile

Section 10 contains the format (profile) for OCSP requests and responses.

7.3.1 Version Number(s)

See OCSP request and response profiles in Section 10.

7.3.2 OCSP Extensions

See OCSP request and response profiles in Section 10.

8 Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

The ORC ECA has compliance audits performed annually of all CMA operations to validate that CMAs are operating in accordance with the security practices and procedures described in this CPS. ORC acknowledges the requirement for subsequent periodic or aperiodic inspection or compliance audit of its support facilities as determined necessary by the EPMA.

ORC acknowledges the EPMA's right to require periodic and aperiodic inspections and compliance audits of the ORC ECA CMA facility to validate that the ORC ECA CMAs are operating in accordance with the security practices and procedures set forth in this CPS.

ORC ECA and EPMA will state the reason(s) for any aperiodic compliance audit.

8.2 Identity/Qualifications of Assessor

ORC engages the services of an auditor that is competent in the field of security compliance audits of Information Technology systems and is thoroughly familiar with the CPS. In all cases, the selected auditor will have experience in information security, cryptography and PKI.

8.3 Assessor's Relationship to Assessed Entity

The auditor is an independent entity. ORC also performs internal audits of ECA, CSA (OCSP responder), RA and LRA facilities, conducted by a Corporate Security Auditor, as defined herein.

8.4 Topics Covered by Assessment

The purpose of a compliance audit is to verify that the ORC ECA has in place a system to assure the quality of the ECA services that it provides, and that it complies with all of the requirements of the US Government ECA CP and this CPS. All aspects of ORC's ECA operation as specified in this CPS are subject to audit compliance inspection.

Any discrepancies between an ORC ECA operation and the stipulations of this CPS and the relevant policy will be noted. The EPMA will be immediately notified of all discrepancies. The EPMA will determine the appropriate remedy, and the EMPA and ORC will determine a time for completion.

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 EPMA

Any remedy may include permanent or temporary ORC ECA cessation or termination of ORC ECA through revocation. 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 EPMA and communicated to ORC as soon as possible to limit the risks created. The EPMA and ORC will determine a time for completion. The implementation of remedies will be coordinated between the EPMA and ORC and subsequently communicated to the appropriate authority. A special audit may be required to confirm the implementation and effectiveness of the remedy.

8.6 Communications of Results

The results of any inspection or audit will be communicated, in whole, to ORC and to the EPMA by the auditor. ORC will determine appropriate remedies and will communicate the remedies to the EPMA as soon as possible to limit the risks created. The implementation of remedies will be communicated to the EPMA . 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 US Government ECA CP, ORC will notify the EPMA immediately upon completion of the audit.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

A fee per validity year, unless otherwise negotiated, will be levied by ORC to issue ECA certificates. A fee per year, unless otherwise negotiated, will be levied by ORC to issue Server and Code Signer certificates. Likewise, a fee per each additional year, unless otherwise negotiated, will be levied by ORC to renew an ORC ECA issued certificate. Fees are published at http://eca.orc.com.

9.1.2 Certificate Access Fees

No fee will be levied by ORC for access to any certificate issued by the ORC ECA. No fee will be levied by ORC for access to information about any certificate issued by the ORC ECA under a court order. ORC will assess a fee from Subscribers and Relying Parties for recovering archived certificates and providing ORC CSA (OCSP responder) validation responses.

9.1.3 Revocation or Status Information Access Fees

No fee will be levied by ORC for access to the ORC CRL. ORC will assess a fee from Relying Parties for providing archived revocation information. ORC CSA (OCSP responder) services will be priced separate from CA services on a transaction and subscription basis.

9.1.4 Fees for Other Services

No fee will be levied for on-line access to policy information about ORC ECA. A reasonable fee to cover media reproduction and distribution costs may be levied for a physical media copy of this policy information. A fee per encryption certificate will be levied for the escrowing of encryption keys. A consulting fee per hour will be 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

No stipulation.

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.

9.2.4 Fiduciary Relationships

Issuance of certificates in accordance with this CPS does not make an ORC ECA, RA/LRA/Issuer/Registrar, an agent, fiduciary, trustee, or other representative of subscribers or relying parties. The relationship between the ORC (the ORC ECA or its designated authorities) and subscribers and that between the ORC (the ORC ECA or its designated authorities) and relying parties is not that of agent and principal. Neither subscribers nor relying parties have any authority to bind the ORC (the ORC ECA or its designated authorities), by contract or otherwise, to any obligation. ORC, the ORC ECA and its designated authorities will make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

9.3 Confidentiality of Business Information

9.3.1 Scope of Business Confidential Information

Not applicable. The ECA will not collect business confidential information.

9.3.2 Information Not Within the Scope of Business Confidential Information

Not applicable. The ECA will not collect business confidential information.

9.3.3 Responsibility to Protect Business Confidential Information

Not applicable. The ECA will not collect business confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

ORC protects all subscribers identifying information. All Subscribers identifying information will be maintained in accordance with applicable laws. Electronic subscriber information is collected and maintained within the CA environment. Hard-copy subscriber information is collected and maintained at ORC's facility in Fairfax, VA in secure containers. Archived hard-copy subscriber information is either maintained within ORC's Fairfax, VA facility or in an off-site storage facility.

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 ECA record (not repository) is handled as Sensitive But Unclassified (SBU), and access will be restricted to those with official needs. Only ORC employees with assigned roles within the ORC ECA have access to the information, which when not being reviewed or processed is maintained in locking file cabinets within ORC's secure suite.

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

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 ECA 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 publicly available 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 ECA will not disclose certificate or certificate-related information to any third party unless expressly authorized by the US Government ECA CP, required by criminal law, government rule or regulation, or order of a criminal court with jurisdiction. ORC ECA 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 ECA 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 ECA certificates issued to ORC personnel or ORC components/devices, including ORC ECA 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 ORC ECA CA Representations and Warranties

The ORC ECA 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. The ORC ECA warrants that CRLs issued and keys generated by The ORC ECA are in conformance with this CPS.

The ORC ECA warrants that any RA/LRA/Issuer/Registrar, Code Signer Certificate Subscriber or designated authority will operate in accordance with the applicable sections of this CPS, and that the ORC ECA:

- Will provide to the EPMA this CPS, as well as any subsequent changes, for conformance assessment
- Will conform to the stipulations of the ECA CP and this CPS, upon approval
- Ensures that registration information is accepted only from RAs/LRAs/Issuers/Registrars who understand and are obligated to comply with this CPS and the ECA CP
- Includes only valid and appropriate information in the certificate, and maintains evidence that due diligence was exercised in validating that information contained in the certificate
- Ensures that obligations are imposed on Subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations
- Revokes the certificates of Subscribers found to have acted in a manner counter to Subscriber obligations

- Notifies Subscribers and makes public for the benefit of Subscribers and Relying Parties any changes to the CA operations that may impact interoperability or security. The ORC ECA will post the notification of any change to the eca.orc.com website.
- Operates or provides for the services of an on-line repository that satisfies the obligations under Section 9.6.5.2,
- Posts certificates and CRLs to the repository

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

- Procedures are implemented in accordance with the US Government ECA CP and this CPS
- all All actions are accomplished in accordance with this CPS
- they They will operate in accordance with the applicable sections of this CPS
- they They meet the personnel and training requirements stipulated in this CPS
- the The applicant organization will cooperate and assist the ORC ECA in monitoring and auditing that they are operating in accordance with the applicable sections of this CPS
- network Network security controls are in accordance with the applicable sections of this CPS

The ORC ECA 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 EPMA.

With respect to Subscriber or Relying Party Agreements or Obligations made by a U.S. 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).

9.6.2 RA Representations and Warranties

RAs are obligated to accurately represent the information prepared for the ORC ECA 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 ECA administration functions.

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

- Approve the issuance of certificates only when both the subscriber's request and the trusted agent validation have been received;
- To validate the accuracy of all information contained in the subscriber's certificate request
- To validate that the named subscriber actually requested the certificate
- Revoke certificates with properly validated revocation requests;
- Notify the subscriber through electronic mail or other means that the certificate request has or has not been granted in accordance with Section 4.3.2;
- Notify a subscriber of certificate revocation in accordance with Section 4.9.2 (or delegate this action to another RA or an LRA);
- To use the RA certificate only for purposes associated with the RA function;
- To immediately revoke one's own RA certificate and report to the CA if private key compromise is suspected;
- To immediately revoke an RA, LRA or subscriber certificate and inform the certificate holder if private key compromise is suspected;
- To revoke and approve reissue of subscriber certificates, if necessary, that were validated by an RA or LRA whose private key is suspected to be compromised;
- To inform trusted agents and the CA of any changes in RA status;
- To protect the RA certificate private key from unauthorized access;
- Validating the credentials of RAs and LRAs;
- Training RAs and LRAs;
- Posting certificates to the repository
- To verify that the certificate request originated from the named subscriber and that the information contained in the certificate request is accurate

- 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 contrary to Subscriber obligations
- To ensure that obligations are imposed on Subscribers in accordance with Section 4.1.2.1
- To inform Subscribers of the consequences of not complying with their 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 LRA Representations and Warranties

LRAs are obligated to accurately represent the information prepared for the ORC ECA and to process requests and responses in a timely and secure manner. ORC LRAs may designate other LRAs or ORC Partner LRAs, however ORC Partner LRAs may not designate other LRAs under this CPS. LRAs under this CPS are not authorized to assume any other ORC ECA administration functions.

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

- To operate in accordance with the stipulations of this ORC ECA CPS
- 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 RA that the certificate request originated from the named subscriber and that the information contained in the certificate request is accurate
- To use the LRA certificate only for purposes associated with the LRA function
- To use private keys only on machines 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 RA of any changes in the LRA's status
- To protect the LRA certificate private keys from unauthorized access
- To immediately request revocation of their LRA certificate and report to the RA if private key compromise is suspected
- To ensure that obligations are imposed on Subscribers in accordance with the Subscriber Obligations
- 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.

When validating subscriber requests for certificates issued under this CPS, an ORC PIVotal ID Registrar accepts the following obligations:

- To operate in accordance with the stipulations of this ORC ECA CPS
- To validate the accuracy of all information contained in the subscriber's request documentation
- To process, archive and protect Subscriber's information from unauthorized disclosure.
- To submit digitally signed authentication of user identity to a PIVotal ID Issuer, either for issuance or revocation functions.
- To provide Subscriber information to no one except those individuals and systems authorized to receive such information.
- To protect all information regarding all current, past, and prospective subscriber.
- To notify the ORC ECA of any changes to the Registrar status.
- To immediately request a certificate revocation in the event:
    - the subscriber can be shown to have violated the stipulations of their obligations;
    - there is reason to believe an associated private key has been compromised; or

- the subscriber or other authorized party asks for their certificate to be revoked.

When validating subscriber requests for certificates issued under this CPS, an ORC PIVotal ID Issuer accepts the following obligations:

- To operate in accordance with the stipulations of this ORC ECA CPS
- To protect Subscriber's information from unauthorized disclosure.
- To provide subscriber information to no one except those individuals and systems authorized to receive such information.
- To notify the ORC ECA of any changes to Issuer status.
- To protect all information regarding all current, past, and prospective subscribers.
- To immediately request revocation of a certificate in the event:
  - the subscriber can be shown to have violated the stipulations of their obligations;
  - there is reason to believe an associated private key has been compromised; or
  - the subscriber or other authorized party asks for their certificates to be revoked.

9.6.4 Subscriber Organization for ARA and PIVotal ID Representations and Warranties

Subscriber organizations that authorize and employ individuals filling roles in support of ORC ECA PIVotal ID and/or ARA systems, as well as that organization's respective PIVotal ID and/or ARA Subscriber(s) warrant that:

- Procedures are implemented in accordance with the US Government ECA CP and this CPS
- All actions are accomplished in accordance with this CPS
- They will operate in accordance with the applicable sections of this CPS
- They meet the personnel and training requirements stipulated in this CPS
- The Subscriber organization will cooperate and assist the ORC ECA in monitoring and auditing that they are operating in accordance with this CPS
- Physical and Network security controls are in accordance with the applicable sections of this CPS

9.6.5 Subscriber Representations and Warranties

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

- To operate in accordance with the stipulations of this ORC ECA CPS
- 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 US Government ECA 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.

In addition, PKI Sponsors (as described in Section 1.3.7.2) assume the obligations of Subscribers for the certificates associated with their components.

9.6.6 Relying Party Representations and Warranties

The ORC ECA will publicly post a summary of this CPS on the ORC ECA website (eca.orc.com) to provide the relying party information regarding the expectation of the ORC ECA. 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 ECA who issued the certificate they are about to rely on as stipulated in the US Government ECA CP
- 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 US Government ECA 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

9.6.7 Representations and Warranties of Other Participants

9.6.7.1 Repository Representations and Warranties

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

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

The ORC ECA posts ORC ECA certificates and CRL information in a repository established by the ORC ECA. Only information contained in the certificate will be posted in this repository to ensure compliance with the Privacy Act. Access is available via Hypertext Transfer Protocol (HTTP)

through a directory gateway interface. The ORC ECA directory sub-tree identifies the identifier ou=ORC. The ORC ECA directory gateway is located at:

https://eca.orc.com?context=eca.

The certificate repository meets the following obligations:

- To list all un-expired certificates for the ORC ECA to relying parties
- To contain an accurate and current CRL for the ORC ECA for use by relying parties
- To be publicly accessible through a web server gateway using HTTPS and FIPS 140-2 approved encryption
- 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.

The ORC ECA maintains a copy of all certificates and CRLs 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.

9.6.7.2 Trusted Agent Representations and Warranties

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

9.6.7.3 Affiliated Organizations Representations and Warranties

Affiliated Organizations are required to authorize the affiliation of subscribers with that organization, and must immediately inform the ORC ECA of any severance of affiliation with any currently affiliated subscriber.

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 ECA provided that the certificate was issued in accordance with the US Government ECA CP and this CPS and that the relying party has used validation information that complies with the US Government ECA CP and this CPS. ORC acknowledges professional liability with respect to the ORC ECA, ORC CMAs and/ or the ORC RAs, ORC LRAs, ORC PIVotal ID Issuers, and ORC PIVotal ID Registrars.

The limit for losses per transaction due to improper actions by the ORC ECA 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 ECA or an ORC CMA is $1 million (U.S. Dollars).

9.8.2 Other Exclusions

Certificate Subscribers 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 Subscribers 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 US Government ECA 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 ECA 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 ECA under this CPS.

ORC will have no claim for loss against the EPMA, including but not limited to the revocation of the ORC ECA 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 ECA, CSA (OCSP responder), and by the US Federal Government.

9.9 Indemnities

Agents of the ORC ECA (e.g., RA/LRA/Issuer/Registrar, 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 a new ECA CP is approved by the PMA, an updated ORC ECA CPS supplants this CPS, or the ECA 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

ORC will notify the EPMA of any changes to this CPS. ORC will also post notification of changes on the web site associated with the ECA operations as applicable to the ECA summary and other publicly available documentation. ORC will notify subscribers of any changes to subscriber obligations via posting to the ORC ECA website. ORC will post a summary of this CPS on its ECA web site. Subscriber obligation changes will be published within 7 days.

9.12.1.1 CPS and External Approval Procedures

The EPMA 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 EPMA will be the sole arbiter of disputes over the interpretation or applicability of the ECA 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 US Government ECA CP and the Memorandum of Understanding between the EPMA and ORC (the ECA provider).

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

No stipulation.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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.

10 Certificate and CRL Formats

Global Unique Identifier (GUID) used in certificates will conform to A Universally Unique IDentifier (UUID) URN Namespace [RFC 4122] requirement. Since GUID is associated with a PIV-I card, the same GUID will be asserted as UUID in all applicable certificates and in all other applicable signed objects on a PIV-I card.

None of the certificates (including roots), CRL or OCSP Responses that are valid beyond 12/31/2030 will be signed using or containing 2048 bit or lower security RSA keys.

10.1 ECA Root CA Self-Signed Certificate

NOT CONTAINED IN THIS CPS, REFER TO US GOVERNMENT ECA CP.

10.2 Subordinate CA Certificate

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Issuer Distinguished Name	cn=ECA Root CA [#] , ou=ECA, o=U.S. Government, c=US
Validity Period	6 years from date of issue in UTCT format
Subject Distinguished Name	cn=ORC ECA <UNIQUE NAME #>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} or Algorithm OID: ecPublicKey { 1 2 840 10045 2 1} Parameters: namedCurve P-256 { 1 2 840 10045 3 1 7 } SubjectPublic Key: Uncompressed EC Point
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}, {2 16 840 1 101 3 2 1 12 3}
Policy Mapping	Not Present
Subject Alternative Name	Not Present

Field	Certificate Value
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	c=yes; cA=True; path length constraint = 0
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	c=no; pointer to ECA Root certificate (optional)
CRL Distribution Points[6]	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.disa.mil/getcrl?ECA%20Root%20CA%20<#> [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://crl.gds.disa.mil/cn%3dECA%20Root%20CA%20<#>%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?certificateRevocationList;binary

10.3 Identity (Signature) Certificate

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	1, 2, or 3 years from date of issue
Subject Distinguished Name	<cn=Subscriber Name>, <ou=Subscriber Company Name >, ou=ORC, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	At least 2048 bit RSA key modulus, rsaEncryption or Algorithm OID: ecPublicKey { 1 2 840 10045 2 1} Parameters: namedCurve P-256 { 1 2 840 10045 3 1 7 } SubjectPublic Key: Uncompressed EC Point
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Authority key identifier[7]	c=no; octet string
Subject key identifier[8]	c=no; octet string

[6] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[7] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[8] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
key usage	c=yes; digitalSignature, nonRepudiation
Extended key usage	c=no; id-kp-clientAuth {1 3 6 1 5 5 7 3 2}; id-kp-emailProtection {1 3 6 1 5 5 7 3 4}
Private key usage period	Not Present
Certificate policies	c=no; one or more of {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}, and {2 16 840 1 101 3 2 1 12 2 3} for sha1, one or more of {2 16 840 1 101 3 2 1 12 4} and {2 16 840 1 101 3 2 1 12 5} for sha256
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains RFC822 e-mail address
Issuer Alternative Name	Not Present
Subject Directory Attributes[9]	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[10]
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://eva.orc.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eca.orc.com/caCerts/<UNIQUE CA>.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://eca-ds.orc.com/cn%3dORC%20ECA%20<UNIQUE CA>%2cou%3dCertification%20Authorities%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?cACertificate;binary,crossCertificatePair;binary
CRL Distribution Points[11]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://eca.orc.com/CRLs/ORCECA<UNIQUE CA>.crl

10.3.1 Optional Identity (Signature) Certificate w/ Smart Card Logon (medium hardware or medium token assurance only)

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique

[9] Before July 1, 2007, if citizenship is not known, the subjectDirectoryAttributes extension shall be omitted. After July 1, 2007, citizenship information is required and the subjectDirectoryAttributes extension shall be populated with this information.

[10] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

[11] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Field	Certificate Value
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	1, 2, or 3 years from date of issue
Subject Distinguished Name	cn=<Subscriber Last Name>.<Subscriber First Name>.<Subscriber Middle Initial or Name>.<ORC UNIQUE IDENTIFIER STRING>.ID, <ou=Subscriber Company Name >, ou=ORC, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption or Algorithm OID: ecPublicKey { 1 2 840 10045 2 1} Parameters: namedCurve P-256 { 1 2 840 10045 3 1 7 } SubjectPublic Key: Uncompressed EC Point
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Authority key identifier[12]	c=no; octet string
subject key identifier[13]	c=no; octet string
key usage	c=yes; digitalSignature, nonRepudiation
Extended key usage[14]	c=no; id-kp-clientAuth {1 3 6 1 5 5 7 3 2}; id-kp-emailProtection {1 3 6 1 5 5 7 3 4}; Smart Card Logon-[15] {1 3 6 1 4 1 311 20 2 2}
Private key usage period	Not Present
Certificate policies	c=no; one or more of {2 16 840 1 101 3 2 1 12 2}, and {2 16 840 1 101 3 2 1 12 2 3} for sha1, {2 16 840 1 101 3 2 1 12 5} for sha256
Policy Mapping	Not Present
Subject Alternative Name Other Name[16]	c=no; always present, contains RFC822 e-mail address Principal Name{1 3 6 1 4 1 311 20 2 3} = <ORC UNIQUE IDENTIFICATION STRING[17]>.@DODECA; }
Issuer Alternative Name	Not Present
Subject Directory Attributes[18]	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[19]
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present

[12] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[13] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[14] RFC3280 indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension.

[15] Microsoft Smart Card Logon.

[16] UPN = domain login. The UPN value must be an ASN1-encoded UTF8 string. ORC will populate the UPN in the form ORC<unique identifier string for subscriber>@DODECA.

[17] See Section 3.1.2 for Unique Identification String information.

[18] Before July 1, 2007, if citizenship is not known, the subjectDirectoryAttributes extension shall be omitted. After July 1, 2007, citizenship information is required and the subjectDirectoryAttributes extension shall be populated with this information.

[19] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

Field	Certificate Value
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://eva.orc.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eca.orc.com/caCerts/<UNIQUE CA>.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://eca-ds.orc.com/cn%3dORC%20ECA%20<UNIQUE CA>%2cou%3dCertification%20Authorities%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?cACertificate;binary,crossCertificatePair;binary
CRL Distribution Points[20]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://eca.orc.com/CRLs/ORCECA<UNIQUE CA>.crl

10.4 Encryption Certificate

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>,ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	1, 2, or 3 years from date of issue
Subject Distinguished Name	<cn=Subscriber Name>, <ou=Subscriber Company Name >, ou=ORC, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption or Algorithm OID: ecPublicKey { 1 2 840 10045 2 1} Parameters: namedCurve P-256 { 1 2 840 10045 3 1 7 } SubjectPublic Key: Uncompressed EC Point
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Authority key identifier[21]	c=no; octet string
Subject key identifier[22]	c=no; octet string
Key usage	c=yes; Required: keyEncipherment or keyAgreement; Prohibited: All Others
Extended key usage	Not Present

[20] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[21] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[22] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
Private key usage period	Not Present
Certificate policies	c=no; one or more of {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}, and {2 16 840 1 101 3 2 1 12 2 3} for sha1, one or more of {2 16 840 1 101 3 2 1 12 4} and {2 16 840 1 101 3 2 1 12 5} for sha256
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains RFC822 e-mail address
Issuer Alternative Name	Not Present
Subject Directory Attributes[23]	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[24]
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C= no; always present, [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://eva.orc.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eca.orc.com/caCerts/<UNIQUE CA>.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://eca-ds.orc.com/cn%3dORC%20ECA%20<UNIQUE CA>%2cou%3dCertification%20Authorities%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?cACertificate;binary,crossCertificatePair;binary
CRL Distribution Points[25]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://eca.orc.com/CRLs/ORCECA<UNIQUE CA>.crl

10.5 Subscriber Medium Hardware PIV-I Authentication Certificate

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	1, 2, or 3 years from date of issue

[23] Before July 1, 2007, if citizenship is not known, the subjectDirectoryAttributes extension shall be omitted. After July 1, 2007, citizenship information is required and the subjectDirectoryAttributes extension shall be populated with this information.

[24] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

[25] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Field	Certificate Value
Subject Distinguished Name	<cn=Subscriber Name>, <ou=Subscriber Company Name > or Unaffiliated, ou=ORC, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha256WithRSAEncryption
Authority key identifier[26]	c=no; octet string
Subject key identifier[27]	c=no; octet string
key usage	c=yes; digitalSignature
Extended key usage	c=no; id-kp-clientAuth {1 3 6 1 5 5 7 3 2}; id-kp-emailProtection {1 3 6 1 5 5 7 3 4}; Smart Card Logon-[28] {1 3 6 1 4 1 311 20 2 2}
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 6}
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains RFC822 e-mail address; Required: URI[29] urn:uuid:<32 character hex representing 128 bit GUID>; Principal Name{1 3 6 1 4 1 311 20 2 3} = <ORC UNIQUE IDENTIFICATION STRING[30]>@DODECA
Issuer Alternative Name	Not Present
Subject Directory Attributes[31]	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1.3.6.1.5.5.7.9.4} CountryOfCitizenship ::= PrintableString (SIZE (2)) -- ISO 3166 Country Code}[32]
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present

[26] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[27] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[28] Microsoft Smart Card Logon.

[29] Note this name form is tagged [6] and encoded as IA5String.

[30] See Section 3.1.2 for Unique Identification String information.

[31] Before July 1, 2007, if citizenship is not known, the subjectDirectoryAttributes extension shall be omitted. After July 1, 2007, citizenship information is required and the subjectDirectoryAttributes extension shall be populated with this information.

[32] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

Field	Certificate Value
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://eva.orc.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eca.orc.com/caCerts/<UNIQUE CA>.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://eca-ds.orc.com/cn%3dORC%20ECA%20<UNIQUE CA>%2cou%3dCertification%20Authorities%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?cACertificate;binary,crossCertificatePair;binary
CRL Distribution Points[33]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://eca.orc.com/CRLs/ORCECA<UNIQUE CA>.crl

10.6 Card Authentication PIV-I Certificate

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	1, 2, or 3 years from date of issue
Subject Distinguished Name	Sn=<GUID>, <ou=Subscriber Company Name > or Unaffiliated, ou=ORC, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha256WithRSAEncryption
Authority key identifier[34]	c=no; octet string
Subject key identifier[35]	c=no; octet string
key usage	c=yes; digitalSignature
Extended key usage	id-PIV-cardAuth {2.16.840.1.101.3.6.8}
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 7}

[33] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[34] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[35] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

Field	Certificate Value
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, URI[36] urn:uuid:<32 character hex representing 128 bit GUID>
Issuer Alternative Name	Not Present
Subject Directory Attributes[37]	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://eva.orc.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eca.orc.com/caCerts/<UNIQUE CA>.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://eca-ds.orc.com/cn%3dORC%20ECA%20<UNIQUE CA>%2cou%3dCertification%20Authorities%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?cACertificate;binary,crossCertificatePair;binary
CRL Distribution Points[38]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://eca.orc.com/CRLs/ORCECA<UNIQUE CA>.crl

10.7 Component Certificate

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>,ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	1, 2, or 3 years from date of issue
Subject Distinguished Name	<cn=Host URL | IP Address | Host Name>, <ou=Host Company Name>, ou=ORC, ou=ECA, o=U.S. Government, c=US

[36] Note this name form is tagged [6] and encoded as IA5String.

[37] Before July 1, 2007, if citizenship is not known, the subjectDirectoryAttributes extension shall be omitted. After July 1, 2007, citizenship information is required and the subjectDirectoryAttributes extension shall be populated with this information.

[38] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Field	Certificate Value
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption or Algorithm OID: ecPublicKey { 1 2 840 10045 2 1} Parameters: namedCurve P-256 { 1 2 840 10045 3 1 7 } SubjectPublic Key: Uncompressed EC Point
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Authority key identifier[39]	c=no; octet string
Subject key identifier[40]	c=no; octet string
Key usage	c=yes; Required: keyEncipherment, digitalSignature
Extended key usage	Required: Client Authentication {1 3 6 1 5 5 7 3 2} Server Authentication {1 3 6 1 5 5 7 3 1}
Private key usage period	Not Present
Certificate policies	c=no; one or more of certificate policy OIDs from Section 1.2 as appropriate except for PIV-I certificate policy OIDs
Policy Mapping	Not Present
Subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://eva.orc.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eca.orc.com/caCerts/<UNIQUE CA>.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://eca-ds.orc.com/cn%3dORC%20ECA%20<UNIQUE CA>%2cou%3dCertification%20Authorities%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?cACertificate;binary,crossCertificatePair;binary
CRL Distribution Points[41]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://eca.orc.com/CRLs/ORCECA<UNIQUE CA>.crl

[39] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[40] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[41] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

10.7.1 Device Certificate – Includes Domain Controllers, VPN, Machine Identification and TBD Devices

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>,ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	1, 2 or 3 years from date of issue
Subject Distinguished Name	<cn=Host URL | IP Address | Host Name | Unique Identifier (depending on device)>, <ou=Host Company Name>, ou=ORC, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption or Algorithm OID: ecPublicKey { 1 2 840 10045 2 1} Parameters: namedCurve P-256 { 1 2 840 10045 3 1 7 } SubjectPublic Key: Uncompressed EC Point
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Authority key identifier[42]	c=no; octet string
Subject key identifier[43]	c=no; octet string
Key usage	c=yes; Required: keyEncipherment or keyAgreement; Prohibited: All Others
Extended key usage	c=yes Required: Client Authentication {1 3 6 1 5 5 7 3 2} Server Authentication {1 3 6 1 5 5 7 3 1}; for domain controller; c=no for other device certificates; OID definition will be dictated by device type (e.g. for domain controller - Client Authentication (1.3.6.1.5.5.7.3.2), Server Authentication (1.3.6.1.5.5.7.3.1); for device Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2), IP security end system (1.3.6.1.5.5.7.3.5), IP security tunnel termination (1.3.6.1.5.5.7.3.6), IP security user (1.3.6.1.5.5.7.3.7), IP security IKE intermediate (1.3.6.1.5.5.8.2.2))
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1}
Policy Mapping	Not Present
Subject Alternative Name	c=no; DNS Name=<fully qualified computer name> e.g. orc-01.orc.com Other Name=DC GUID {1.3.6.1.4.1.311.25.1}=<GUID of Device receiving certificate>
Certificate Template {1.3.6.1.4.1.311.20.2.3}[44]	c=no; BMPString: DomainController; The actual extension value in HEX: 1E200044006F006D00610069006E0043006F006E00740072006F006C006C00650072
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present

[42] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[43] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[44] Field is specific to Domain controller certificates, may not appear in other device certificates

Field	Certificate Value
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://eva.orc.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eca.orc.com/caCerts/<UNIQUE CA>.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://eca-ds.orc.com/cn%3dORC%20ECA%20<UNIQUE CA>%2cou%3dCertification%20Authorities%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?cACertificate;binary,crossCertificatePair;binary
CRL Distribution Points[45]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://eca.orc.com/CRLs/ORCECA<UNIQUE CA>.crl

10.8 Code Signing Certificate

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>,ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	1, 2, or 3 years from date of issue
Subject Distinguished Name	cn=CS.<Code Signer Organization Name>.<optional number>, <ou=Code Signer Company Name>, ou=ORC, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption or Algorithm OID: ecPublicKey { 1 2 840 10045 2 1} Parameters: namedCurve P-256 { 1 2 840 10045 3 1 7 } SubjectPublic Key: Uncompressed EC Point
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Authority key identifier[46]	c=no; octet string

[45] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

[46] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

Field	Certificate Value
Subject key identifier[47]	c=no; octet string
Key usage	c=yes; digitalSignature, nonRepudiation
Extended key usage	c=yes; { iso(1) identified-organization(3) DoD(6) internet(1) security(5) mechanisms(5) pkix(7) id-kp(3) id-kp-codesigning (3)}
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 2}, {2 16 840 1 101 3 2 1 12 3}, {2 16 840 1 101 3 2 1 12 5}
Policy Mapping	Not Present
Subject Alternative Name	always present; c=no; cn=<private key holder name>, <ou=Code Signer Company Name>, ou=ORC, ou=ECA, o=U.S. Government, c=US
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://eva.orc.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eca.orc.com/caCerts/<UNIQUE CA>.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://eca-ds.orc.com/cn%3dORC%20ECA%20<UNIQUE CA>%2cou%3dCertification%20Authorities%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?cACertificate;binary,crossCertificatePair;binary
CRL Distribution Points[48]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://eca.orc.com/CRLs/ORCECA<UNIQUE CA>.crl

10.9 Group/Role Signature Certificate

ORC ECA does not currently support Group/Role certificates.

10.10 Group/Role Encryption Certificate

ORC ECA does not currently support Group/Role certificates.

[47] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[48] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

10.11 Content Signing PIV-I Certificate

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256WithRSAEncryption
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	6 years or less from date of issue
Subject Distinguished Name	<cn=Descriptive CMS Name>, <ou=CMS Operations Company Name > or Unaffiliated, ou=ORC, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha256WithRSAEncryption
Authority key identifier[49]	c=no; octet string
Subject key identifier[50]	c=no; octet string
key usage	c=yes; digitalSignature
Extended key usage	c=yes; id-fpki-pivi-content-signing; {2.16.840.1.101.3.8.7}
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 8}
Policy Mapping	Not Present
subject Alternative Name	Not Present
Issuer Alternative Name	Not Present
Subject Directory Attributes[51]	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://eva.orc.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eca.orc.com/caCerts/<UNIQUE CA>.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://eca-ds.orc.com/cn%3dORC%20ECA%20<UNIQUE CA>%2cou%3dCertification%20Authorities%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?cACertificate;binary,crossCertificatePair;binary

[49] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[50] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[51] Before July 1, 2007, if citizenship is not known, the subjectDirectoryAttributes extension shall be omitted. After July 1, 2007, citizenship information is required and the subjectDirectoryAttributes extension shall be populated with this information.

Field	Certificate Value
CRL Distribution Points[52]	c=no; always present, [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://eca.orc.com/CRLs/ORCECA<UNIQUE CA>.crl

10.12 OCSP Responder Self-Signed Certificate

Note: This profile is for relying parties that choose to deploy an OCSP responder.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Issuer Distinguished Name	cn=<OCSP Responder Name>, <ou=Company Name>, ou=ECA, o=U.S. Government, c=US
Validity Period	1, 2, or 3 years from date of issue in Generalized Time format
Subject Distinguished Name	cn=<OCSP Responder Name>, <ou=Company Name>, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} or Algorithm OID: ecPublicKey { 1 2 840 10045 2 1} Parameters: namedCurve P-256 { 1 2 840 10045 3 1 7 } SubjectPublic Key: Uncompressed EC Point
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Extensions	Not Present

10.13 OCSP Responder Certificate

Note: This profile is used only for CSAs

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>,ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	1 month from date of issue in UTCT format

[52] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Field	Value
Subject Distinguished Name	cn=http://eva.orc.com, ou=ORC, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} or Algorithm OID: ecPublicKey { 1 2 840 10045 2 1} Parameters: namedCurve P-256 { 1 2 840 10045 3 1 7 } SubjectPublic Key: Uncompressed EC Point
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA CA's public key information)
Subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the OCSP Responder public key information)
Key usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}, {2 16 840 1 101 3 2 1 12 3}
Subject Alternative Name	http URL for the OCSP Responder
Authority Information Access	C=no; always present, [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://eva.orc.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eca.orc.com/caCerts/<UNIQUE CA>.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://eca-ds.orc.com/cn%3dORC%20ECA%20<UNIQUE CA>%2cou%3dCertification%20Authorities%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?cACertificate;binary,crossCertificatePair;binary
No Check Id-pkix-ocsp-nocheck; {1.3.6.1.5.5.7.48.1.5}	c=no; NULL

10.14 ECA Root CA CRL

NOT CONTAINED IN THIS CPS, REFER TO US GOVERNMENT ECA CP.

10.15 Subordinate CA CRL

Field	Subordinate CA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }

Field	Subordinate CA CRL Value
Issuer Distinguished Name	cn=ORC ECA <UNIQUE NAME #>,ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 7 days
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
CRL extensions	
CRL Number	Integer
Authority Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA public key information)
CRL entry extensions	
Invalidity Date	present when received
Reason Code	Always Present; Will not include certificateHols

10.16 OCSP Request Format

OCSP requests are not required to be signed. The OCSP Responder will not check the signature on the request. See RFC2560 for detailed syntax. The following table lists which fields are required by the ORC CSA OCSP Responder.

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

10.17 OCSP Response Format

See RFC2560 for detailed syntax. The following table lists which fields are populated by an 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[53], thisUpdate, nextUpdate[54],

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

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

Field	Expected Value
Extension	
Nonce	Will be present if nonce extension is present in the request
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256WithRSAEncryption or ecdsa-with-SHA256 { 1 2 840 10045 4 3 2 }
Signature	Present
Certificates	Applicable certificates issued to the OCSP Responder

11 Identity Proofing Outside the United States

All identity proofing for U.S citizens and non-U.S. citizens located outside the U.S. must be carried out in accordance with this CPS and the ECA CP Version 4.3.

Identity proofing for non-U.S. citizens located inside the U.S. must be carried out in accordance with Section 3 of this CPS and ECA CP Version 4.3.

In all cases, except where noted below, Subscribers will perform initial registration, key generation, and perform all other functions in the same manner as U.S. citizens located within the U.S. as described in Section 3.2.3.1 of this CPS.

11.1 Identity Proofing by U.S. Consular Officers

U.S. citizens located outside the U.S. can use the notary services provided by U.S. consular offices, JAG officers and embassies for identity proofing purposes under this CPS. Non-U.S. citizens of those countries identified in Section 11.1.3 below may also use these services for identity proofing when identity proofing is performed in one of these countries. Non-U.S. citizens who are not citizens of the countries identified in Section 11.1.3 below must either comply with the requirements of Section 11.2 to obtain their identity proofing, or they must be located in the U.S. and must follow the procedures in Section 3.2.3.1 of this CPS. ORC will not issue certificates to foreign nationals proscribed by U.S. laws and regulations.

11.1.1 Procedures for Identity Proofing by U.S. Consular Officers and JAG Officers

Consular officers and US DoD JAG officers may act as a Notary public for the purpose of performing identity proofing for ORC ECA certificate Subscribers. Subscribers will take the 4 page printed request forms along with 2 photo identity documents (one of which must be a current valid passport) and proof of organizational affiliation to a US Consular Officer. The US Consular Officer will verify the subscriber's identity in accordance with Section 3.2.3.1 of this CPS and notarize the forms.

Locations of U.S. consular offices and embassies may be found at:

• http://travel.state.gov/travel/tips/embassies/embassies_1214.html

See also 22 CFR 92.1-92.35.Consular officers are required to establish the identity of persons executing notarized statements. See 22 CFR 92.31 (c) which says: "(c) Satisfactory identification of grantor(s). The notarizing officer must be certain of the identity of the parties making an

acknowledgment. If he is not personally acquainted with the parties, he should require from each some evidence of identity, such as a passport, police identity card, or the like. The laws of some States and Territories require that the identity of an acknowledger be proved by the oath of one or more “credible witnesses", and that a statement regarding the proving of identity in this manner be included in the certificate of acknowledgment. Mere introduction of a person not known to the notarizing officer, without further proof of identity, is not considered adequate identification for acknowledgment purposes."

11.1.2 ECA Requirements

In addition to meeting all other requirements of this CPS, including identity proofing using a Notary Public, all certificates issued based on identity proofing performed by a U.S. consular officer will assert the country of citizenship of the Subscriber. ORC will verify that the documentation received contains the seal of a consular officer from one of the countries identified in Section 11.1.3. ORC will also verify that the Subscriber presented a passport as one of the identity documents and for proof of citizenship.

11.1.3 Participating Countries

As listed by the ECA CP Version 4.3, the ORC ECA recognizes the following participating countries:

Australia
Canada
New Zealand
United Kingdom

11.2 Identity Proofing by Authorized DoD Employees

Non-U.S. citizens who are not citizens of the countries identified in Section 11.1.3 above must either comply with the requirements of this section (11.2) to obtain their identity proofing, or they must be located in the U.S. and must follow the procedures in Section 3.2 of this CPS.

To facilitate certificate issuance to these individuals, the processes indicated in ECA CP Section 11, version 4.3 may be used when a DoD employee who interacts regularly with the certificate Subscriber is available and can be authorized to assist with the required identity proofing. The data recipient must authenticate all data exchanges that are part of this process and the process used for this authentication must be commensurate with the strength of the certificate being issued. Identity proofing is subject to

compliance audit requirements as outlined in Section 8 of the ECA CP Version 4.3.

11.2.1 Process for Authorizing Issuance of ECA Certificates when identity Proofing is Performed by Authorized DoD Employees Outside the U.S.

Subscribers requiring issuance of ORC ECA issued certificates and their sponsoring DoD Components must ensure that all requirements for authorization, as delineated in the ECA CP Version 4.3 , are followed. The steps to be followed by any DoD Component or Program sponsoring Subscribers for ECA certificates are as follows:

- Ensure that a formal agreement, such as a Memorandum of Understanding (MOU), exists between the DoD and the foreign government, which requires the need for information exchange with local nationals in that country or with citizens of that country to accomplish the goals of the agreement.
- Submit a formal request in a digitally signed email to their DoD Component PKI POC, requesting participation in the program, and including the following:
  - A statement of the requirement to exchange information,
  - Information about the agreement(s) that exist, and,
  - A statement that the DoD Program Sponsor will follow the procedures outlined in Section 11 of the ECA CP for performing identity proofing.
- Provide the list of sponsored Subscribers and countries to the DoD PKI ECA Liaison Officer and DoD Component PKI POC in a digitally signed email. The Program Sponsor will either have personal knowledge of the sponsored Subscribers or will obtain this information in an authenticated manner from an authorized local representative. This list must be on file with the DoD PKI ECA Liaison Officer. The DoD PKI ECA Liaison Officer and DoD Component PKI POC may vet the list.
- Coordinate in an authenticated manner with the DoD PKI ECA Liaison Officer and DoD PKI Component POC to ensure there are authorized DoD Employees who can support the identity proofing of sponsored Subscribers.

The DoD Component PKI POC must complete the following steps:

- Agree to follow the procedures outlined in Section 11 of the ECA CP for performing identity proofing.
- Coordinate with the DoD PKI ECA Liaison Officer to identify and establish authorized DoD Employees

- Each authorized DoD employee must:
  - Be a U.S. citizen,
  - Have a SECRET or higher clearance granted by the U.S.,
  - Have a Common Access Card (CAC) containing an identity certificate issued by the DoD PKI,
  - Be authorized to perform identity proofing for a specified set of countries, and,
  - Review the procedures in Section 11.2.2 for performing identity proofing of non-U.S. Citizens and submit a digitally signed statement to the DoD PKI ECA Liaison Officer, acknowledging the DoD employee's roles and responsibilities. [Note: Familiarity with passports and all other approved proof of citizenship documents in the country must be one of the enumerated responsibilities.]
- Provide the list of authorized DoD employees to the DoD PKI ECA Liaison Officer in a digitally signed email. This list must contain the CAC signature certificate subject distinguished name for each authorized DoD employee and state which employees are authorized to perform identity proofing for which foreign countries. The DoD Component must keep this list current and must, at a minimum, provide an updated list quarterly.
- Validate the program, the Program Sponsor, and the authority of the Program Sponsor POC to speak for the program.
- Decide whether or not to approve requests from validated Program Sponsors.
- Provide a list of approved program sponsors and a POC for each program to the DoD PKI ECA Liaison Officer in an authenticated manner

The DoD PKI ECA Liaison Officer must complete the following steps:

- Maintain a list of current DoD Component PKI POCs,
- Maintain a list of authorized DoD Employees for each country,
- Provide the list of authorized DoD Employees to approved Program Sponsors in a digitally signed email,
- Maintain the list of approved Subscribers, including vetting the list of countries and Subscribers,
- Provide the list of approved Subscribers to the authorized DoD Employees in a digitally signed email, and;

Provide the list of authorized DoD Employees, along with their certificate information, to ORC in a digitally signed email.

11.2.2 Identity Proofing Procedures to Be Used by Authorized DoD Employees for ECA Certificates

Once DoD employees have been authorized using the process identified in Section 11.2.1 of the ECA CP version 4.3, they must adhere to the requirements of the ECA CP and the following requirements for performing identity proofing of non-U.S. citizens applying for ORC ECA issued certificates:

- The authorized DoD employee must have a copy of the list of individuals of the country who are authorized to receive certificates, which will include assertion of their citizenship. The authorized DoD employee must authenticate the list and may only accept it if the source is the ECA Liaison Officer.
- The authorized DoD employee must have the list of approved proof of citizenship documents and be able to recognize legitimate versions of identity documentation that will be provided by the Subscriber.
- The Subscriber must appear, in person, before the authorized DoD employee. The authorized DoD employee must verify that the Subscriber is on the list of individuals.
- The Subscriber must present two forms of identification, at least one of which must be a proof of citizenship, either a passport or another document from the approved list, and both of which forms of identification must be recognized as legitimate identity documents by the authorized DoD employee.
- The Subscriber and the authorized DoD employee must exchange sufficient information for the ECA vendor to ensure that the binding of the identity proofing to the certificate request is unambiguous and accurate. This information (e.g., certificate request number, certificate request password) may vary among ECAs, but must be specifically defined by the ECA in its CPS as part of its certificate request process.
- The Subscriber must sign a copy of the ECA's subscriber agreement form in the presence of the authorized DoD employee.
- The authorized DoD employee must also sign the ECA's subscriber agreement form. The authorized DoD employee must retain a copy and provide a copy of the signed form to the Subscriber. DoD Components may choose to maintain subscriber agreements in a centralized location, in which case the DoD Component PKI POC must provide the authorized DoD employees with instructions for transferring the forms to the centralized location.

- The authorized DoD employee must send an email that is digitally signed with the employee's CAC signature certificate to the ECA, containing:
  - The name of the Subscriber,
  - A statement that the authorized DoD employee has performed identity proofing for this Subscriber in accordance with the ECA CP,
  - The citizenship of the Subscriber, and,
  - The information binding the identity proofing to the certificate request for the Subscriber.

11.2.3 ECA Requirements

In addition to adhering to all other requirements of this CPS, the ORC ECA will adhere to the following requirements when accepting identity proofing performed by authorized DOD employees:

- The ORC ECA specifies in this CPS the information exchanged among the ECA, the Subscriber, and the authorized DoD employee to ensure that the binding of the identity proofing to the certificate request is unambiguous and accurate.
- The ORC ECA will obtain in an authenticated manner the list of authorized DoD employees from the DoD PKI ECA Liaison Officer.
- The ORC ECA will receive, prior to each certificate issuance, an email digitally signed by a CAC-based signature certificate of the authorized DoD employee, asserting that the identity proofing has taken place. This email must contain information sufficient to accurately and unambiguously match the individual's identity proofing with the pending certificate request. The ORC ECA will verify the signature on the email, including full certification path validation, as described in [RFC 3280]. The ORC ECA will verify that the certificate is a CAC based signature certificate by viewing the Certificate Policies and verifying that the OID 2.16.840.1.101.2.1.11.9 (id-us-dod-mediumHardware) is present in the certificate. ORC will use the mail client to examine the signing certificate and compare it to the data included in the listing of Approved DoD Employees sent out by the DISA ECA Program office. The ORC ECA will also verify that the signer of the email is on the list of authorized DoD employees. All emails are archived according to the retention policy described in Section 5.5.
- The ORC ECA will provide a copy of the ECA subscriber agreement to all Subscribers.

- The ORC ECA will provide the email address that authorized DoD employees must use when sending to the ECA the confirmation that identity proofing has taken place.
- The ORC ECA will assert the country of citizenship of the Subscriber for all certificates issued based on identity proofing performed by an authorized DoD employee.

11.2.4 Participating Countries

The ORC ECA will accept certificate requests for all qualified foreign nationals in all countries, except countries or entities or nationals proscribed by law and regulation at the time of application. Relevant laws and regulations include:

Department of State International Traffic in Arms Regulations (ITAR) Proscribed List (22 C.F.R. Section 126.1)

Department of Commerce Export Administration Regulations (EAR), 15 C.F.R. Section 730 et seq., including specifically, but not limited to, Parts 736, 738, 740, 744 Spir, and 746. See http://www.access.gpo.gov/bis/ear/ear_data.html

Department of the Treasury regulations issued pursuant to the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. Ch.35, Sec. 1701 et seq. or other laws identifying prohibited countries or people or entities, including the Office of Foreign Assets Control (OFAC) Listing of Specially Designated Nationals and Blocked Persons (SDN List) and OFAC Country Sanctions Programs. For more information, see specifically http://www.treas.gov/offices/enforcement/ofac/index.shtml and http://www.treas.gov/offices/enforcement/lists/

11.3 Identity Proofing by ECA Registration Authority or Trusted Agent

U.S. citizens located outside the U.S. requiring Medium/ medium SHA-256 software, Medium Token/ medium token SHA-256, and Medium Hardware/ medium hardware SHA-256 Assurance certificates may have identity verification performed by an ECA Registration Authority (RA) or Trusted Agent (TA) who is located outside the U.S. All requirements specified in this CP for an ECA RA and TA will apply. Non-U.S. citizens of the countries listed in this CPS may also use an ECA RA or TA for identity proofing when identity proofing is performed in one of these countries. Note that the RA must be a U.S. citizen. TA must be a U.S. citizen unless the identity

proofing is carried out in one of the countries listed in this CPS. In that case, the TA must either be a U.S. citizen or a citizen of the country where the identity proofing is performed.

11.3.1 Procedures for Identity Proofing by ECA RA or TA

The RA or TA will meet the CP requirements specified in this CPS for in-person authentication of Subscribers. When identity proofing is performed by an RA or TA, Subscribers must present a current valid passport for proof of citizenship and as one of the documents proving identity. As a second photo ID, the Subscriber may provide a driver's license or other photo ID issued by a government authority in their country of citizenship, or issued by a government entity within the U. S.

11.3.2 ECA Requirements

In addition to meeting all other requirements of this CPS, all certificates issued based on identity proofing performed by an RA or TA must assert the country of citizenship of the Subscriber. The RA or TA must also verify that the Subscriber presented a passport as one of the identity documents and for proof of citizenship.

12 PIV-INTEROPERABLE SMART CARD DEFINITION

To support technical interoperability of PIV-I cards with Federal Agency PIV implementations, certificates asserting any of the PIV-I policies must comply with the technical specifications used for Federal Agency issued PIV cards. Hardware tokens used for Medium Hardware PIV-I and Card Authentication PIV-I certificates and the systems used to create them shall meet all of the following requirements.

- To ensure interoperability with Federal systems, PIV-I Cards shall use a smart card platform that is on GSA's Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS201-2] Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).
- When Card Management System is used for PIV-I issuance, the Card Management Master Key shall conform to NIST SP 800-78.
- PIV-I Cards shall conform to NIST Special Publication 800-73, Interfaces for Personal Identity Verification [SP800-73], ensuring that PIV-I UUID requirements are met.
- PIV-I Cards shall contain an authentication certificate that conforms to the Medium Hardware PIV-I policy and the profile specified in Section 10.
- PIV-I Cards shall contain a card authentication certificate that conforms to the Card Authentication PIV-I policy, [SP800-73], and the profile specified in Section 10.
- PIV-I Cards shall contain an electronic representation (as specified in [SP800-73] and NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification [SP800-76] of the Cardholder Facial Image printed on the card.
- PIV-I Cards shall contain an electronic representation (as specified in [SP800-76] of the fingerprint images collected during card registration.
- PIV-I Cards shall contain signature and encryption certificates that conform to the Medium Hardware PIV-I policy and the profile specified in Section 10.
- PIV-I Cards shall be visually distinguishable from Federal PIV Cards to ensure no suggestion of attempting to create a fraudulent Federal PIV Card. At a minimum, images or logos on a PIV-I Card shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS201-2].
- The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card:
    - Cardholder facial image;
    - Cardholder full name;

    - Organizational Affiliation, if exists; otherwise the issuer of the card; and
    - Card expiration date.
- PIV-I Cards shall have an expiration date not to exceed 3 years after issuance date.
- Expiration of the PIV-I Card shall not be later than expiration of Content Signing PIV-I certificate used to sign the content on the card.
- The digital signature certificate that is used to sign objects on the PIV-I Card (e.g., CHUID, Security Object) shall contain the Content Signing PIV-I policy OID, and shall conform to the profile in Section 10.
- The Content Signing PIV-I certificate and corresponding private key shall be managed within a trusted CMS.
- At issuance, the RA shall activate and release 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.
- To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card diversified keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card diversified key. Card diversified keys shall meet the algorithm and key size requirements stated in NIST Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification [SP800-78]. At a minimum, the Secure Channel specification version 02 with three key 3DES along with a plan to transition to AES shall be implemented

13 References

The following documents contain information that provides background, examples, or details about the contents of this policy.

Number	Title	Date
ABADSG	Digital Signature Guidelines	1 Aug 1996
ECA CP	US Government Certificate Policy for External Certification Authorities	4 Jan 2012
ECA KRP	US Government Key Recovery Policy for External Certification Authorities	4 June 2002
FIPS112	Password Usage	5 May 1985
FIPS140	Security Requirements for Cryptographic Modules	25 May 2001
FIPS186-3	Digital Signature Standard	June 2009
FIPS 201-2	Personal Identity Verification (PIV) of Federal Employees and Contractors	9 July 2012
FOIA	5 U.S.C. 552, Freedom of Information Act As Amended By Public Law No. 104-231, 110 Stat. 3048	1996
FPKI-E	Federal PKI Certificate and CRL Profile	12 Oct 2005
FWPP	U.S. Government Firewall Protection Profile for Medium Robustness Environments	25 July 2007
IDSPP	Intrusion Detection System Protection Profile	4 Feb 2002
ISO9594-8	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework	1997
NS4009	NSTISSI 4009, National Information Assurance Glossary	26 Apr 2010
ORC KRPS	Operational Research Consultants Key Recovery Practices Statement	17 Dec 2006
ORC SSP	Operational Research Consultants Systems Security Plan	13 Sep 2013
PKCS-1	PKCS #1 v2.1: RSA Cryptography Standard	14 June 2002
PKCS-11	PKCS #11 v2.20 Cryptographic Token Interface Standard	June 2004
PKCS-12	PKCS #12 v1.1 Public-Key Cryptography Standard - Personal Information Exchange Syntax Standard	27 Oct 2012
RFC2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP	June 1999
RFC 2822	Internet Message Format	Apr 2001
RFC 3647	Certificate Policy and Certification Practices Framework	Nov 2003
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace	July 2005
RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocols	Sep 2005
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP	Jun 2013
SDN702	SDN.702, Abstract Syntax for Utilization with Common Security Profile (CSP), Version 3 X.509 Certificates and Version 2 CRLs	31 July 1997
SP 800-73	Interfaces for Personal Identity Verification	Apr 2005
SP 800-76	Biometric Data Specification for Personal Identity Verification	Jan 2007

14 Acronyms and Abbreviations

AES	Advanced Encryption Standard
AID	Application Identifier
APL	Approved Products List
ARA	Automated Registration Authority
BSM	Basic Security Module
CA	Certification Authority
CAA	Certificate Authority Administrator
CDR	Recordable CDROM
CDROM	Compact Disk, Read Only Memory
CM	Configuration Management
CMA	Certificate Management Authority
CMS	Card Management System
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRLDP	Certificate Revocation List Distribution Point
CSA	Certificate Status Authority (OCSP Responder)
CSAA	Code Signing Attribute Authority
CSOR	Computer Security Objects Registry
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
DN	Distinguished Name
DoD	Department of Defense
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
ECA	External Certification Authority
EE	End Entity
EPMA	ECA Policy Management Authority
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	(US) Federal Public Key Infrastructure
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
GSA	General Services Administration
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
I&A	Identification and Authentication

ID	Identity (also, a credential asserting an identity)
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standards
IT	Information Technology
JAG	Judge Advocate General
KEA	Key Exchange Algorithm
KED	Key Escrow Database
KRA	Key Recovery Authority
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over Secure Sockets Layer
LRA	Local Registration Authority
MCS	Mobile Code Signing
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ORC	Operational Research Consultants, Inc.
OU	Organizational Unit
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
POC	Point of Contact
POP	Proof of Possession
QUIC	Quantum Information and Computation
RA	Registration Authority
RAID	Redundant Array of Inexpensive Disks
RD	Road
RDN	Relative Distinguished Name
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)
SA	Systems Administrator
SBU	Sensitive But Unclassified
S/MIME	Secure Multipurpose Internet Mail Extensions
SNOC	Secure Network Operations Center
SCVP	Simple Certificate Validation Protocol
SDN	Secure Data Network
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer

TA	Trusted Agent
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
US	United States
USC	United States Code
USD	United States Dollar
UUID	Universally Unique Identifier
WWW	World Wide Web

15 Glossary

The primary source is NSTISSI 4009, National Information Systems Security Glossary; other sources were used if NSTISSI 4009 had no entry for the term, or if another source gave a definition more appropriate to PKI. If no reference is given, the definition is ad hoc.

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 IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
affiliated organization	An organization that has a relationship with a subscriber and sponsors that subscriber for obtaining a 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
archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by a CMA, 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"]
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]
Automated Registration Authority (ARA)	Card-issuing workstation/system specified for the issuance of Medium Token assurance, Medium Token SHA256 assurance and Medium Hardware assurance certificates.
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 person.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
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.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates. [ISO9594-8]
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
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]
certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
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.

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]
confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
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]
diversified key	A unique key for each card that is generated using the Master Key and the card identifying elements
dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services
encryption certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
External Policy Management Authority (EPMA)	Authority that oversees the creation and update of Certificate Policies, reviews Certification Practice Statements, reviews the results of CA audits for policy compliance, evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies.
firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Group/Role Manager	A person who is responsible for managing the Group/Role, including assigning individuals to the Group/Role membership and maintaining the list of Group/Role members and public key certificates issued to them.
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]
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	The retention of the private component of the key pair associated with a Subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
master key	The key required to unlock the Open Platform Key and allow changes to the contents of the card. Each card is shipped with a Manufacturer Master Key, which may optionally be changed for a Client Master Key as part of the card initialization step.
naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
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]
OCSP Responder	A trusted entity that provides on-line revocation status of certificates to Relying Parties. The OCSP Responder is either explicitly trusted by the Relying Party, or through the CA that issued the certificate whose revocation status is being sought.
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.

PKI Sponsor	Fills the role of a Subscriber for non-human system components or organizations that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this document.
PIVotal ID	ORC-branded card management system specified for the issuance of Medium Hardware PIV-I and Medium Card Authentication PIV-I assurance certificates on ECA PIV-I credentials
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of Subscriber data to Certification Authorities and does not sign or directly revoke certificates.
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.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received 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. [ABADSG]
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 trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG]
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.
server	A system entity that provides a service in response to requests from clients.
identity 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 signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG]. **Current Subscribers** possess valid ECA-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing 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.
technical non-repudiation	The contribution public key mechanisms make 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 a Certificate Management Authority in providing Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, 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.

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. [FIPS140]