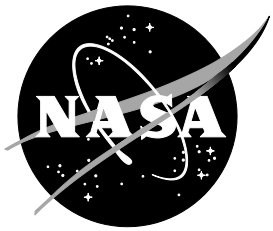


National Aeronautics and Space Administration
George C. Marshall Space Flight Center
NASA Enterprise Competency Center
Huntsville, Alabama 35812

NASA Operational Certificate Authority Registration Practice Statement

Version 3.0

January 2015

National Aeronautics and Space Administration
George C. Marshall Space Flight Center
Huntsville, Alabama 35812

This page is intentionally blank.

Signature:

_____ _____

NASA ICAM Program Executive Date

Signature:

_____ _____

Treasury Program Management Authority Date

This page is intentionally blank

Revision History

Document Version	Document Date	Revision Details	Initials	Section
1.0	**9/2009**	Original SSP CPS		
1.2	**1/2010**	Revision to Adopt changes into the NASA Registration practice statement	**SJL**	**ALL**
2.0	**9/2010**	Revised document for review by NASA and Treasury	**SJL**	**ALL**
2.1	**4/2011**	Final revision after 10/2010 audit findings 2/2011	**SJL**	**ALL**
2.2	**6/2011**	Revision to document to update changes to NOCA	**SJL**	**ALL**
2.3	**11/2011**	Revision to document transition of PKI Operations to NEACC	**TWB**	**ALL**
2.4	**07/2012**	Rewrite of document based on FY 2011 Treasury audit review	**TDW**	**ALL**
2.5	**08/2013**	Revise RPS based on FY 2012 Treasury audit findings	**TDW**	**ALL**
3.0	**01/2015**	Revised based on FY 2013 Treasury audit findings	**TDW**	**5, 7, and 8**

Preface

The registration process is the first step in establishing trust in the end entity certificates of a Certification Authority (CA). This process binds the authenticated identity of a person or device to a digital certificate signed by the CA. Registration Authorities (RA) within the National Aeronautics and Space Administration (NASA) include Security Officers (SO), Super RAs, RAs, and Trusted Agents (TA). These roles shall follow this Registration Practice Statement (RPS) to ensure the accuracy and trustworthiness of the CAs, and its end entity certificates.

This page is intentionally blank

Table of Contents

1 INTRODUCTION

The National Aeronautics and Space Administration (NASA) entered into an Agreement with the US Treasury to have the US Treasury as the Shared Service Provider (SSP) for the operation of the NASA Certification Authority (CA), referred to as the NASA Operational Certification Authority (NOCA). Under this Agreement, NASA retains responsibility for the operation of the Registration Authorities (RAs).

This document assumes an understanding of Public Key Infrastructure (PKI) concepts and technology and a familiarity with NASA PKI. It describes the practices for the RAs that operate under the NOCA. This document's focus is on the responsibilities and procedures for the RAs, is a component of the overall PKI policies and procedures, and is designed to comply with the X.509 Certificate Practice Statement for Department of Treasury Subordinate Certificate Authorities (CPS).

To obtain information concerning the underlying policies for this RPS, consult the "*X.509 Certificate Policy for the U.S. Federal PKI Common Policy*."

2 REGISTRATION PRACTICE STATEMENT (RPS)

2.1 Purpose

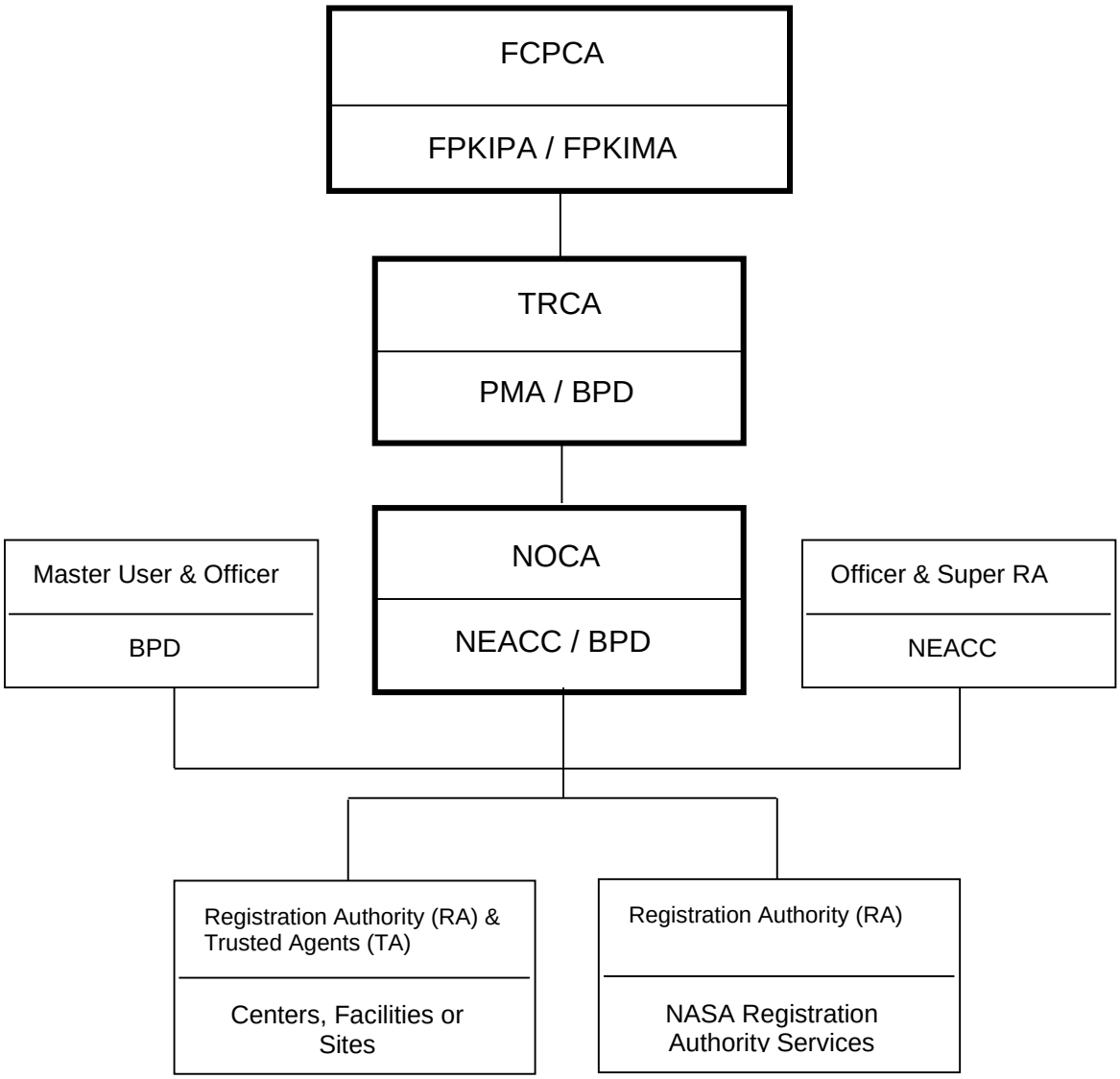
The "*X.509 Certificate Practice Statement for Department of Treasury Subordinate Certificate Authorities*" states the practices that shall be followed by the NASA RPS to comply with the established assurance that can be placed in the certificates it issues. The term "Registration Authority" as used in this document, refers to NASA's registration infrastructure setup to perform the registration authority and life-cycle management of all certificates issued from the NOCA.

2.2 Scope

The reader shall have undertaken the RA training as well as being familiar with basic PKI concepts such as public-private key cryptography, digital signature, signature verification, encryption, decryption, certification authority, PKI directory, certificate revocation lists and certificate verification.

The RPS establishes the processes used by the RA in performance of their duties in the issuance and management of certificates. This RPS applies to certificates issued to devices, federal employees, contractors, and other personnel affiliated with NASA. The NOCA does not issue certificates to other CAs.

2.3 NASA PKI Structure



2.4 Suitability of the NOCA RPS

The Treasury PMA will determine suitability of this RPS with the Treasury CPS. The NASA Program Executive will determine suitability of this RPS with NASA.

2.5 RPS Administration

The NASA ICAM Program Executive and the ICAM PKI Functional Service Owner are responsible for review and acceptance of any changes to this RPS in accordance with the policies set forth by the FPKIPA. This document is administered and maintained by the NASA Enterprise Application Competency Center (NEACC) ICAM PKI Team in the Office of the Chief Information Officer of the George C. Marshall Space Flight Center (MSFC).

3 CERTIFICATES

3.1 Types of Certificates Issued

The NOCA only issues end entity certificates but does not issue CA certificates.

Certificate Types

- **Non-PIV Human – Software Certificates:** Are used by human subscribers for verifying digital signatures and encrypting email and documents.
    - Key usage: Digital Signature, Non-repudiation, Key Encipherment
    - Extended Key Usage: N/A
    - Entrust cryptographic module protects certificate keys

- RA Smartcard Certificates: Are used by RAs for performing RA operations with certain PKI tools.
    - Key usage: Digital Signature, Non-repudiation, Key Encipherment
    - Extended Key Usage: N/A
    - FIPS 140 Validated Hardware Token
    - Some tools use the RA's PIV card for authentication

- **PIV Human – Smartcard Based Certificates:** Are used by human subscribers for Smart Card Based PIV Authentication, Digital Signature, Key Encipherment, Card Authentication
    - Key usage: Digital Signature, Non-repudiation, Key Encipherment
    - Extended Key Usage: Client Authentication
    - NASA only uses FIPS 201 compliant cryptographic modules for Personal Identity Verification (PIV)

- **Non-Person Entity (NPE) Certificates:** Are dual usage single key pair certificates used to support device authentication, secure mailing lists and secure communications via SSL.
    - Key Usage: Digital Signature, Key Encipherment
    - Extended Key Usage: Server Authentication, Client Authentication

Characteristics for Each Certificate Type

Number of certificates issued for each certificate type: The Non-PIV Human Software type is a set of 2 certificates, each restricted to a single use, i.e., one for digital signature verification and one for encryption. Other certificate types involve the issuance of a single certificate.

Intended use of each certificate: Intended uses for certificates are digital signature verification, authentication and encryption. Some certificate types are intended for single use, while others are intended for multiple uses.

Type of cryptographic module required to protect the private keys: A cryptographic module is designed to protect a Human Subscriber's or Device's private keys. Cryptographic modules can be implemented in software or in hardware, e.g., a Smart Card or cryptographic accelerator board for a server or application. Cryptographic modules used by the federal government must be certified as meeting the requirements stated in Federal Information Processing Standard (FIPS) 140-2. There are several levels specified in FIPS 140-2 with Level 1 being the lowest, Level 2 more secure, Level 3 even more secure, etc.

Public key cryptographic algorithm and key size: The required public key cryptographic algorithm, e.g. Rivest Shamir Adleman (RSA) and key size, e.g., 2048 bit hashing algorithm, e.g., Secure Hashing Algorithm (SHA-2) used for encryption and digital signature are identified for each certificate type.

Key Usage Period: The private key usage period sets the upper limit on the private key's use, after which a new key pair must be generated and a new certificate issued if the Human Subscriber or Device is to continue to use their PKI service. The public key usage period determines the expiration date for the certificate. After that date, Relying Parties will no longer be able to validate the certificate.

4 TRUSTED ROLES AND RESPONSIBILITIES

4.1 NASA Operational Certification Authority

The NOCA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. The NOCA is responsible for:

a. The certificate manufacturing process,
b. Publication of certificates,
c. Revocation of certificates,
d. Generation and destruction of CA signing keys, and
e. Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under the Federal CP and Treasury CP are performed in accordance with the requirements, representations, and warranties of those CPs.

As the Shared Service Provider (SSP), the U.S. Treasury, Bureau of Public Debt (BPD) is responsible for operation of the NASA CA, NOCA, creation and maintenance of the CPS and oversight of the CA policy. The NOCA will issue certificates under "*X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*" and the "*X.509 Certificate Policy For The US Treasury PKI*". These certificates contain registered certificate policy object identifiers (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose.

As the Contracting Federal Agency NASA is responsible for maintenance of the CA and RA component software, Identification and management of the authoritative data source used to create digital credentials, managing the PKI branch of the NASA Enterprise Directory, and management operation and technical controls over the RA, in compliance with Federal CP, CPS and this RPS.

The Treasury PMA designates individuals as PKI Trusted Roles. Only Trusted Roles may perform administrative type responsibilities on the NOCA. All NASA personnel requesting Trusted Roles shall use the NASA Access Management System (NAMS) for approval before being assigned PKI Administrative Roles.

NASA Policy Management Authority

The NASA Policy Management Authority (PMA) is responsible for:

a. NASA PKI Policy,
b. Maintenance, approval, and compliance of the NASA Registration Practice Statement (RPS),
c. Maintaining critical policy documentation,
d. Representing NASA at federal meetings involving policy issues that have bearing on NASA's PKI program,
e. Defining training requirements for PKI Trusted Roles,
f. Approving NAMS applications for all PKI Administrator Roles.

Security Officers

The NOCA designates at least one security officer who is verified and registered by the Treasury PMA. Other security officers may be designated to help with the operation of the NOCA. Security officers can either be affiliated with the Treasury SSP or with NASA.

The primary responsibilities of the NASA security officer are:

a. Register and verify other security officers and Registration Authorities

b. Create and maintain security profiles,

c. Modify and provide Treasury any new certificate specifications,

d. Create and maintain device certificates essential to the operation of the CA, i.e. Online Certificate Status Protocol (OCSP) signature certificates.

e. Perform emergency certificate maintenance tasks,

f. Perform subscriber registration functions in the absence of a "Super" Registration Authority or Registration Authority

"Super" Registration Authorities and Registration Authorities

NASA designates individuals as "Super" Registration Authorities (SRAs) and registration authorities (RAs). The SRAs are highly experienced employees that assist the Center RAs with problems and issues that surface in the course of performing their RA duties. Typical SRA duties include:

a. Training RAs on the performance of their duties and on the use of PKI related hardware and software.
b. Provisioning new RAs (i.e., providing the required access to perform RA duties).
c. Terminating RA accounts when the RA leaves or is reassigned.
d. Assisting with RA duties when an RA is out or unavailable.

RAs collect and verify each subscriber's identity and information that is to be entered into the subscriber's public key certificate. The RA is responsible for:

a. Determining eligibility to receive certificates;

b. Performing in person identification and authentication when issuing new Certificates or Key Recoveries for Encryption, Signing.

c. Verifying the accuracy of information to be included in certificates;

d. Approving and executing the issuance of the certificates from the NOCA;

e. Approving and executing the revocation, updates, and re-key of certificates.

a. Using Entrust certificate management tools to issue NOCA certificates.

b. Securely delivering activation codes to the sponsor to be used to generate digital credentials on devices;

As the SSP hosting provider, Treasury does not use or manage SRAs, or RAs for NASA. NASA is responsible for the selection and training of SRAs and RAs.

Card Management System (CMS) Registration Authority

The CMS registration authority is the registration authority associated with the Card Management System. The CMS RA issues PIV Human – Smartcard Based Certificates as described in section 3.1.1 of this document. Trusted Agents (Enrollment Officers and Supervisors) utilize the CMS to issue PIV certificates with keys generated on approved cryptographic hardware tokens.

Trusted Agents

The NASA PMA approves individuals as trusted agents. A trusted agent satisfies all the trustworthiness requirements for an RA and performs identity proofing and/or distributes authorization codes as a proxy for the RA.

As the SSP hosting provider, Treasury does not use or manage trusted agents for NASA.

Subscribers

A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. Subscribers are limited to Federal employees, contractors, affiliated personnel, and devices operated by or on behalf of NASA.

Applicant

An applicant is a prospective Subscriber seeking issuance of a certificate.

4.2 Other Participants

NASA Enterprise Directory (NED) Administrators

As part of the certificate management services, the NASA Enterprise Directory (NED) is the Repository Administrator. NASA maintains the directory repository that houses the certificates and Certificate Revocation List (CRL). This includes, but is not limited to, creating and maintaining the directory information tree structure, providing operational backup scripts/schemes to the Backup Operators and Monitoring Operators, completing directory recovery tasks, etc.

PKI Sponsors

A PKI Sponsor fills the role of a Subscriber for non-human system components that are named as public key certificate subjects. The PKI Sponsor must be an active subscriber in the NASA PKI system. The PKI Sponsor works with the SRAs, RAs or security officers to register components (SSL certificates, software code, domain controllers, routers, firewalls, etc.) in

accordance with this RPS and is responsible for meeting the obligations of Subscribers as defined throughout this document.

5 IDENTIFICATION AND AUTHENTICATION

5.1 Naming

Types of Names

Base Distinguished Name

There can be multiple types of names in the certificate by which the subject is known, such as directory name, a unique user ID, email name, hostname and/or DNS name. The NOCA generates and signs certificates that contain an X.500 DN. To ensure the NOCA does not overlap X.500 naming in use by any organization, the NOCA issues certificates that are subordinate to the following Distinguished Name (DN):

"ou=NASA, o=U.S. Government, c=US"

Distinguished Name of the CA

The NOCA has the following DN:

"ou=NASA Operational CA, ou=Certification Authorities, ou=NASA, o=U.S. Government, c=US"

This name is inserted as the Issuer of every certificate issued by the NOCA, regardless of namespace utilized for the Subscriber or device.

Distinguished Names of Employees

Employees shall have a DN of the following form:

The Common Name (CN) is unique across the NOCA directory. It is comprised of the first name, middle initial, last name, and generational information if applicable. An Agency Unique Identifier (AUID) attribute shall be included in the form of a multi-valued Relative Distinguished Name (RDN) to ensure uniqueness. The result would have the following DN:

For People branch:

"uid=[AUID] + cn=[FirstName LastName OptionalGenerationQualifier], ou=People, ou=NASA, o=U.S. Government, c=US"

For PIV branch:

"uid=[AUID] + cn=[FirstName LastName OptionalGenerationQualifier], ou=PIV, ou=NASA, o=U.S. Government, c=US"

Distinguished Names of Affiliates

Federal Contractors and other affiliated persons shall have the text "(affiliate)" appended to the CN. An Agency Unique Identifier (AUID) attribute shall be included in the form of a multi-

valued Relative Distinguished Name (RDN) to ensure uniqueness. The result would have the following DN:

For People branch:

"cn=[FirstName LastName OptionalGenerationQualifier] (affiliate) + uid=[AUID], ou=People, ou=NASA, o=U.S. Government, c=US"

For PIV branch:

"cn=[FirstName LastName OptionalGenerationQualifier] (affiliate) + uid=[AUID], ou=PIV, ou=NASA, o=U.S. Government, c=US"

Distinguished Names of Devices

Devices shall have a DN of the following form:

"cn=[DeviceName], ou=Services, ou=NASA, o=U.S. Government, c=US"

The CN shall be a descriptive name for the device. If the device is a fully described Internet domain name, then the CN is optional and will contain the fully qualified domain name.

Distinguished Names of Mailing Lists

Mailing lists shall have a DN of the following form:

"cn=[MailingListName], ou=Services, ou=NASA, o=U.S. Government, c=US"

The CN shall be a descriptive name for the mailing list.

Distinguished Names of Cards

Certificates issued under the id-fpki-common-cardAuth shall have a DN of the following form where FASC-N is the FASC-N on the subject's PIV card:

"serialNumber=[FASC-N], ou=PIV, ou=NASA, o=U.S. Government, c=US"

Certificates issued under id-fpki-common-cardAuth shall contain a subject alternative name extension that has a value that includes the piv FASC-N name type. The value for this name will be the FASC-N. No other name will be included in the subject alternative extension of the certificate.

Certificates issued under id-fpki-common-cardAuth are not published in the LDAP or HTTP repository.

Need for Names to Be Meaningful

Subject names used in certificates shall identify the person or object in which they are assigned in a meaningful way. When X.500 based DNs are used, the common name represents the

Subscriber in a way that is easily understandable for humans. For individuals the legal name will be used. For equipment, this may be a model name and serial number, a server's fully qualified host name, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

The NOCA does not use the CN attribute to describe itself. The NOCA uses the Organizational Unit (OU) attribute to provide a meaningful name to relying parties and subscribers.

The subject name in NOCA certificates matches the issuer name in certificates issued by the subject, as required by RFC 3280.

Uniqueness of Names

The NASA RA shall ensure Distinguished Name (DN) uniqueness within the X.500 name space. The unique user ID and serialNumber attributes are used to ensure that no two individuals are assigned the same DN, and potentially the same electronic identity or credential. The RA shall investigate and, if necessary, recommend the correction of any name duplications brought to their attention. The RA shall coordinate with and defer to the NASA PMA where appropriate.

5.2 Initial Identity Validation

Certificate applicants shall submit requests for certificates via the NAMS and/or the NASA Identity Management System (IDMS). To complete certificate enrollment the applicant must have an active identity in the NASA IDMS with a valid Photo Biometric on file.

Method to Prove Possession of Private Key

In the case where a subscriber generates its own signature keys, the NOCA must require the subscriber to prove possession of the corresponding private key. This is done by the subscriber using its private key to sign a value and providing that value to the NOCA, using the PKIX-CMP (RFC-2510).

In the case where key generation is performed under the CA or RA's direct control, the NOCA does not require proof of possession.

NASA shall authenticate the identity of any organization that appears as a component of the subject name appearing in the certificate before processing the certificate application. The CA software requires that all such organizations be pre-defined before issuing subscriber certificates belonging to that organization.

Authentication of Human Subscribers (NON-PIV)

All subscribers requesting a certificate shall submit a NAMS request that is routed to their Supervisor for approval, and then to the RA for provisioning. As part of the NAMS workflow and approval process, the subscriber must click a radio button acknowledging that (s)he has read and accepted the terms and conditions in the NOCA Subscriber Agreement. A link to the Subscriber Agreement is provided in the acknowledgement statement.

The RA shall ensure that the Applicant's identity is verified prior to certificate issuance. The applicant must provide a current active PIV/CAC Card that is either issued by or registered with NASA or two forms of government identification with one of them containing a biometric

(picture). If the applicant submits the required forms digitally signed using a PIV card, it is an acceptable mechanism of authentication. Once completed, the NOCA will ensure that the Applicant's identity information and public key are properly bound.

Where it is not possible for applicants to appear in person before the RA, a trusted agent may serve as proxy for the RA. The requirement for recording a biometric of the applicant may be satisfied by comparing a passport-style photograph with the biometric information recorded in the NASA **IDMS. The trusted agent will verify the photographs against the appearance of the applicant and th**e biometrics on the presented credentials against those recorded in the NASA IDMS. The Trusted Agent shall follow the same identity proofing process as required for the RA (noted above). This information shall be sent to the RA in a secure manner (i.e., digitally signed electronic means, via registered mail, or in person).

To ensure these requirements are met, the RA or TA shall fill out NASA Form (NF) 1824 (see Appendix D) and provide the applicant a copy of the NOCA Subscriber Agreement (see Appendix E). The RA or TA shall have the applicant review the NF1824 for accuracy and read the Subscriber Agreement. Both the RA or TA and the applicant shall sign NF1824.

In-Person Antecedent

In instances where a user cannot appear in person before the RA or TA (e.g., a NASA employee or affiliate who is not near a NASA Center), Federal and Treasury PKI policy allows that a trust relationship between the RA or TA and the applicant, based on an in-person antecedent (i.e., previous in-person identity verification), will suffice as meeting the in-person identity-proofing requirement provided the in-person verification occurred within the previous 9 years.

Since Federal Common Policy promotes strict in-person identity verification, the antecedent in-person verification is only allowed under certain circumstances. Before applying the antecedent policy, the RA shall obtain approval from the Agency NOCA Security Officer. If the Security Officer is not available, the RA shall contact their Center PKI Point of Contact for approval. The Security Officer or PKI POC shall make the final determination of whether the antecedent in-person verification is justified. Once approved, the RA or TA shall confirm the applicant has an active identity in the Identity Management System. The RA or TA shall verify the applicant's identity by contacting them via their verified business phone number, and asking security questions from the applicant's Launchpad security questions list.

Authentication of Human Subscribers for Group Certificates

Normally, a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers.

In addition to the authentication of the sponsor, the following procedures shall be performed for members of the group:

1. The Information Systems Security Office or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.

2. The subjectName DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form;
3. The list of those holding the shared private key must be provided to, and retained by, the applicable CA or its designated representative; and
4. The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

Delivery of Activation Codes

If the applicant answers all questions correctly, the RA or TA can provide the PKI codes. If the applicant fails to authenticate, they shall report in person before the RA or TA to obtain their PKI codes. The RA or TA shall deliver the applicant their one time activation codes (i.e. reference number and authorization code) out of band via separate communications channels.

If using an electronic means to deliver one component of the code, it will be the reference number. For example, the reference number can be delivered via the applicant's email provided the applicant has a nasa.gov email address. The authorization code can then be delivered via telephone, voice mail, or first class mail.

The RA or TA shall email the applicant a copy of the Subscriber Agreement and NF1824. The applicant shall read the Subscriber Agreement and sign NF 1824 (either handwritten or digitally) and return the document either electronically (scanned to .pdf format) or by first class mail to the RA or TA. If the applicant fails to sign NF 1824, the certificate shall be revoked. The RA or TA shall complete and sign NF1824. The RA shall retain the completed form in a locked cabinet or drawer.

Authentication of Human Subscribers (PIV)

In addition to the requirements for Authentication of Human Subscribers (Non-PIV) (Section 5.2.2) the TA verifies the photo on the smartcard is of the person receiving the new smartcard. A biometric match of the fingerprint or photo is then performed in the CMS to unlock the smartcard for logical and physical use.

Authentication of Devices

A current Subscriber shall represent an Applicant that is a device or process (Ex. Firewalls, Routers, Web Servers, etc.). The Subscriber shall maintain operational control of, and responsibility for, certificates issued to the device or process along with the associated private keys. The Sponsor shall be responsible for providing the following registration information:

1. Equipment identification;

2. Equipment authorizations and attributes (if any are to be included in the certificate), and;

3. Contact information to enable the NOCA, SRA or RA to communicate with the Subscriber when required.

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested.

Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

1. Verification of digitally signed messages sent from the Subscriber (using certificates of equivalent or greater assurance than that being requested).

2. In person registration by the Subscriber, with the identity of the PKI sponsor confirmed in accordance with the requirements of Section 5.2.2.

6 PERSONNEL CONTROLS

6.1 Trusted Roles

A Trusted Role is one whose incumbent performs functions essential in establishing the basis of trust.

6.2 Qualifications, Experience, and Clearance Requirements

Security Officers, SRAs, RAs, and Trusted Agents all perform functions that can introduce serious security breaches if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible, or the integrity of the NOCA will be weakened. All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity.

NASA management is responsible for screening all employees with Trusted Roles to ensure a level of trust comparable with the duties of the individual. NASA complies with the OPM human resource guidelines for a standard security background check on its employees and/or contractors fulfilling trusted roles. NASA management shall ensure that appropriate background investigations are conducted on NASA and contractor personnel assigned to sensitive positions.

Individuals assigned Trusted Roles shall meet the following requirements:

a. Be a U.S. citizen;
b. Be a NASA employee or NASA contractor;
c. Have a background investigation and
d. Assigned a level of confidence of 50 (Position of Public Trust) or higher.

In addition to the listed requirements, the Security Officer shall have a Top Secret security clearance.

6.3 Background Check Procedures

NASA SRAs, RAs, and Trusted Agents shall have a favorable adjudication of MBI results.

The NASA Account Management System shall contain background check requirements for persons filling the Security Officer, RA, SRA, or TA roles.

6.4 Training Requirements

All trusted personnel attend focused training before performing their duties. In addition to technical training, trusted personnel receive training with regard to data handling to ensure confidential information, records and applications are handled in compliance with the Privacy Act.

NAMS holds documentation identifying all trusted personnel who received SMA training and the date that training was completed.

All individuals in Trusted Roles shall receive:

- Initial SMA / WebSMA Training
- Annual Refresher Training
- Additional Training as needed (Application Upgrades, New procedures, etc.)

6.5 Sanctions for Unauthorized Actions

All personnel who have access to data on any NOCA computers/networks are responsible for the data and are bound by applicable laws, rules, and Treasury, BPD, and NASA directives.

Specific sanctions are not mandated for each incident of non-compliance with the rules. Depending upon the number of occurrences, purpose (unintentional vs. intentional) and severity of the violation, at the discretion of administration and through due process of the law, consequences may include suspension or revocation of access privileges.

7 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

7.1 Physical Controls

Identification and Authentication for Each Role

PKI Administrators shall use smart card login to authenticate themselves into SMA, and Web SMA. For Web SMA, RAs shall use their PIV Badge for login. For SMA, RAs shall use a special Smart Token for login. The RA's SMA software will be hosted on a desktop or laptop computer running Microsoft Windows, and configured with computer and physical security controls that meet the following requirements:

- System must meet NASA-STD-2804 and NASA-STD-2805 requirements for hardware and software.
- System must meet the Federal Desktop Core Configuration (FDCC) requirements.
- 2 Smart Card Readers
- Entrust Security Manager Administration 9.2 or later installed.
- ActivClient Middleware must be installed.

No cameras or mirrors shall be installed next to or behind an RA computer in such a way that would allow monitoring of keystrokes from any viewing angle. To prevent visual eavesdropping, an antireflective filter may be required.

The *Entrust* profile associated with each RA's certificate shall be stored on a NASA issued smartcard. The profiles used by RAs shall have a one-to-one correspondence with their users; i.e., no two RAs may share a password or profile at any time.

Information Logging

RA and TA actions shall be recorded through the NAMS PKI Users and PKI Administrator workflows. Specific RA actions shall also be recorded by the NOCA. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used.

Hardcopy reports generated by the RA office shall be stored sequentially in a three-ring binder and stored in a secure location when not in use. They shall be dated and categorized according to

point of origin (i.e., who created the report). If the reports are electronic, they shall be encrypted and stored on the RA computer, or encrypted on shared/removable media.

Informational Updates

RAs are responsible for relaying PKI news/updates to their Center and respective PKI users. RAs must post any NASA PKI changes or alerts in an accessible, highly visible area, or distribute them by e-mail.

To communicate with NASA PKI Technical Support, as well as local Center personnel, RAs must have access to a telephone and e-mail software during business hours. RAs must also have access to this RPS and the following documents:

- X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework
- NASA PKI Registration Authority (RA) Operations Guide for Entrust SMA
- NASA PKI Registration Authority (RA) Operations Guide for Entrust WebSMA
- NASA PKI Website https://pki.nasa.gov

Archival

Electronic archival is provided by NAMS. In instances where paper forms are collected, documents and forms provided to the RA must be archived for a minimum of 10 years and 6 months from the date of their creation. If the original media cannot retain the data for this required period, you must transfer the archived data to newer media technologies available during the time of transfer.

Examples of archival data include:

- Certificate requests and approvals
- Revocation requests and approvals
- Key recovery requests and approvals
- Authentication of Subscriber's Identity data
- Documentation of receipt and acceptance of certificates
- Documentation of receipt of tokens

The RA facility must have a secure storage mechanism or be in a locked room where documents and completed forms can be retained. Annually, archived documentation (completed forms and logbooks) shall be moved from the RA work area to a permanent archival location that is secure and not under the RAs control (e.g., with the Center Information Security Officer or PKI POC, in a safe, locked room or locked cabinet).

Center PKI Logbook Storage Location

Center	Location	Accessible By	Locked Area
JSC	IT Security Building	Chief Information Security Officers	Yes
MSFC	Building 4200, Room 522D	PKI Privacy Lead	Yes
JPL	Badging Office Building 249	Personnel Security Group	Yes
HQ	Room 4H79	NASA HQ Chief Information Security Officer	Yes
LaRC	Building 1268 Room 2046	ICAM Subject Matter Expert (SME)	Yes
GSFC	Building 8 Room 041D	ICAM SME	Yes
GRC	Building 142 Room 183B	Network Operations, IT Security Operations, Data Center Facility Manager, Physical Security Supervisors	Yes
ARC	Building N-233, Room 166	ACES Security	Yes
AFRC	Building 4838, Room 264	ACES Field Technician	Yes
SSC	Building 3204, SSC Record Retention Facility	Controlled Facility – Employees must be granted access to building and room	Yes
KSC	M7-0355 room 1336A	Lead, Aerospace IT	Yes

8 ISSUING CERTIFICATES USING THE NOCA

8.1 Issuing the Certificate

The NASA RA shall perform the following steps when a certificate is issued to an applicant:

1. Establish the applicant's authorization based on the NASA IDMS for PIV. The NAMS workflow provides authorization for non-PIV and devices.
2. The RA authenticates the applicant according to the guidelines in section 5 of this document. The identity of the applicant and issuer is recorded within NAMS and/or NOCA Entrust Security Manager.
3. Verify role and / or authorization information requested for inclusion in the certificate.
4. The issuance of non-PIV/device authorization codes requires the approval of two different RA's.
5. The RA provides Authentication Codes to authenticated subscribers for device and non-PIV certificates. PIV certificates will be encoded in a FIPS 140-2 Level 2 hardware token secured by a biometric authentication.

The TA provides assistance as described in section 4.1of this document.

The RA shall encrypt and provide end user authentication information to the TA from the NASA IDMS. At a minimum, authentication information shall include the full name and photo from the NASA IDMS. The TA may access the activation codes via WebSMA, or if WebSMA access is not available, the RA shall pass the activation codes to the TA via signed and encrypted email.

Codes shall only be used once and are valid for 30 days. If the Sponsor allows the codes to expire, they will need to be reissued, as with the original codes, they must be distributed in a secure manner. In the event that the sponsor does not retrieve the credentials within 30 days, the entire vetting process must be performed again.

The RA or TA shall follow the guidance in section 5.2 Authentication of human subscribers. Once the subscriber is authenticated, the TA shall provide the subscriber the activation codes.

8.2 Certificate Acceptance

Conduct Constituting Certificate Acceptance

Before a Subscriber can make effective use of its private key, the Subscriber will be required to acknowledge his or her obligations with respect to protection of the private key and use of the certificate before being issued the certificate.

By applying via the NAMS process, the Subscriber will acknowledge that they have read and understood the NASA Subscriber Agreement. In the case of non-human components (router, firewalls, etc.), a NOCA PKI Sponsor will perform the functions of the Subscriber.

The Subscriber or Sponsor is deemed to have accepted the certificate at the time the NOCA issues the certificate. The publication of a certificate in an active state by the NOCA constitutes a complete and final acceptance of the certificate by the Subscriber or Sponsor.

8.3 Certificate Update

A certificate will be renewed or modified only if the public key has not reached the end of its validity period and the associated private key has not been compromised.

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number.

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

Circumstance for Certificate Modification

NOCA Security Officers, SRA and RAs will perform certificate modification for a subscriber whose characteristics have changed (e.g., name change due to marriage, email address, AUID). This new certificate will have a different subject public key.

Who May Request Certificate Modification

NOCA Security Officers, SRA and RAs will accept requests for certificate modifications from the following.

1. Subscribers with a currently valid certificate.
2. NASA Security Officers and RAs on behalf of a subscriber.
3. The human sponsor of a device certificate on behalf of the device.

Processing Certificate Modification Requests

Subscribers must provide proof of all subject information changes before the modified certificate is issued. For example, when an individual's name changes then proof of the name change must be provided in accordance with section 5.2. When the subscriber is using a managed certificate, the desktop client notifies them that a certificate update has occurred.

8.4 Key Recovery

Key recovery is performed whenever the Subscriber needs to recover the existing key and compromise has not occurred. Circumstances requiring Key Recovery are:

- Unusable Entrust Profile (epf)
- Damaged Token
- Forgotten PIN/Passwords
- New CA certificate

8.5 Key Update

When any fields are changed in a certificate, you should also update the certificate's key pair. This will ensure the changes are recognized immediately.

8.6 Certificate Revocation and Suspension

The NOCA periodically issues Certificate Status Information (CSI), CRLs and OCSP responses, covering all revoked certificates but does not support certificate suspension. CRLs are publicly published via Hypertext Transport Protocol (HTTP) and Lightweight Directory Access Protocol (LDAP).

The NOCA issues CRLs every 4 hours with an18 hour validity period. In the event of private key compromise or loss, the NOCA immediately publishes a CRL to the NOCA Repository.

The NOCA supports online status checking via OCSP [RFC 2560] for end entity certificates. The OCSP validation authority checks for CRL updates from the CA once every hour and have a validity period of 4 hours. The OCSP responder checks for new proofs once every 5 minutes.

Circumstances for Revocation

Multiple circumstances may arise that could result in certificate revocation. These circumstances may include, but are not limited to the following:

- A Subscriber violates the terms of this RPS, or any other agreement, regulation or law applicable to the certificate;
- A Subscriber is no longer affiliated with NASA;
- A private key has been compromised, lost, or stolen;
- A Subscriber asks for its certificate to be revoked;
- When the binding between the Subscriber and the Subscriber's public key contained within a certificate is no longer valid.

Note: In the event of lost or stolen devices, the Center Incident Response Team (CIRT) shall notify the RA to deactivate and revoke certificates associated with lost/stolen devices (Per the IT Security Handbook).

Who Can Request Revocation

Within the NOCA PKI, the NOCA may summarily revoke certificates within its domain. Revocation requests are submitted via NAMS or the NASA IDMS by:

- the subscriber,
- authorized personnel acting on behalf of the subscriber,
- the sponsor of a NPE certificate,
- a Security Officer
- RA on behalf of NASA PMA

Procedure for Revocation Request

A request to revoke a certificate must identify the certificate to be revoked and explain the reason for revocation. This is accomplished via NAMS workflow approved by the NASA PMA and an RA verifies the request. The RA will authorize or deny the revocation request. If revocation is approved, the RA shall use Web SMA to both **deactivate and revoke** the certificate.

An electronic record is retained in the NOCA audit trail of any online (electronic) request.

The Subscriber will destroy, or return to NASA, any tokens associated with a revoked certificate prior to, or immediately upon, certificate revocation.

Revocation Request Grace Period

Subscribers and authorized parties shall submit revocation requests as defined in section 7.6.2 and/or notify the NASA help desk as soon as the need is identified.

8.7 End of Subscription

The NOCA does not require a subscriber to perform any action to end its subscription. If the subscriber's certificate expires and is not renewed, then the certificate and related public key will be archived. However, if the subscriber terminates his/her service with the NOCA, then the certificate and keys will be revoked and archived. Archiving of expired and revoked certificates and / or keys occurs on a periodic basis.

Appendix A: Bibliography

The following documents were used in part to develop this RPS:

CCP-PROF	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program, January 7, 2008. http://www.idmanagement.gov/fpkipa/documents/CertCRLprofileForCP.pdf
E-Auth	E-Authentication Guidance for Federal Agencies, M-04-04, December 16, 2003. http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
FIPS 140-2	Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-2	Digital Signature Standard (DSS), FIPS 186-3, June, 2009. http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
FIPS 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-1, March 2006. http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm
FBCACP	X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 2.24, February 25, 2011 http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf
FCPCACP	X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.16, September 23, 2011 http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf
GISRA	Government Information Security Reform http://www2.ed.gov/policy/gen/leg/gisra.doc
ISO9594-8	ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.509-200811-I!!PDF-E&type=items and http://www.itu.int/rec/dologin.asp?lang=e&id=T-REC-X.509-201102-I!Cor1!PDF-E&type=items

ITMRA	40 U.S.C. 1401, Information Technology Management Reform Act of 1996, Public Law 104-106 - Division E—Information Technology Management Reform (Clinger-Cohen Act) http://www.gpo.gov/fdsys/pkg/PLAW-104publ106/pdf/PLAW-104publ106.pdf
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://www.fas.org/irp/offdocs/nsd/nsd42.pdf (redacted version)
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997. (FOUO)
NS4009	NSTISSI 4009, National Information Systems Security Glossary, April 26, 2010. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
PACS	*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 30, 2004. http://159.142.162.84/documents/TIG_SCEPACS_v2.2.pdf
PKCS#1	Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003. http://www.ietf.org/rfc/rfc3447.txt
PKCS#12	PKCS 12 v1.0: Personal Information Exchange Syntax-June 24, 1999. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999. http://www.ietf.org/rfc/rfc2459.txt
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999. http://www.ietf.org/rfc/rfc2510.txt
RFC 2560	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, June 1999. http://www.ietf.org/rfc/rfc2560.txt
RFC 2822	Internet Message Format, Peter W. Resnick, April 2001. http://www.ietf.org/rfc/rfc2822.txt

RFC 3647 Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003. http://www.ietf.org/rfc/rfc3647.txt

SECAGSC Federal Public Key Infrastructure (FPKI) Security Controls Profile of Special Publication 800-53A Assessment Guidance for Security Controls in PKI Systems, Version 1.0, April 18, 2011. http://www.idmanagement.gov/fpkipa/documents/FPKI_Profile_SP80053A_PKI_Assessment_Guidance.pdf

SECPROF Federal Public Key Infrastructure (FPKI) Security Controls Profile of Special Publication 800-53 Security Controls for PKI Systems, Version 1.0, April 18, 2011 http://www.idmanagement.gov/fpkipa/documents/FPKI_Profile_SP80053_PKI_Security_Controls.pdf

SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems, NIST Special Publication 800-37 Rev 1, February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

SP 800-63 Electronic Authentication Guideline, NIST Special Publication 800-63 Version 1, Dec 2011 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

Appendix B: Acronyms and Abbreviations

BPD	The Bureau of the Public Debt
CA	Certification Authority
C&A	Certification and Accreditation
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm
FPKI OA	Federal Public Key Infrastructure Operational Authority
FIPS PUB	(US) Federal Information Processing Standards Publication
FPKI	Federal Public Key Infrastructure
FPKIA	Federal PKI Architecture
FPKIPA	Federal PKI Policy Authority
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
IDMS	Identity Management System
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector

NACI	National Agency Check with Inquiries
NAMS	NASA Account Management System
NARA	U.S. National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NEACC	NASA Enterprise Application Competency Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
MSFC	George C. Marshall Space Flight Center
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PKIX-CMP	Public Key Infrastructure X.509 – Certificate Management Protocol
PSS	Probabilistic Signature Scheme
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSASSA	RSA Signature Scheme with Appendix
SHA	Secure Hash Algorithm

S/MIME	Secure/Multipurpose Internet Mail Extensions
SP	Special Publication
SSL	Secure Sockets Layer
SSP-REP	Shared Service Provider Repository Service Requirements
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

Appendix C: Glossary

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the FPKIPA or comparable body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.

Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "certificate" refers to X.509 certificates that expressly reference the OID of this CP in the certificatePolicies extension.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a certification authority to perform certificate issuance and revocation.
Certification Authority Software	Key management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date.
Certificate Status Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status, and may also provide additional attribute information for the subject certificate.

Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two certification authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140-2]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity Certificate	A certificate in which the subject is not a CA.
FPKI Operational Authority (FPKI OA)	The Federal Public Key Infrastructure Operational Authority is the organization responsible for operating the Common Policy Root Certification Authority.

Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding the Federal PKI Architecture.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information Systems Security Officer (ISSO)	Person responsible to the Designated Approving Authority for ensuring the security of an information system throughout its life-cycle, from design through disposal. [NS4009]
Inside Threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be

	decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.
Modification (of 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.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI, OIDS are used to uniquely identify certificate policies and cryptographic algorithms.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring on-line).

Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	Fills the role of a subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of certificate policies, review certification practice statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.
Relying Party	A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this RPS; may also be referred to as a directory.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
RPS	Registration Practice Statement.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Structural Container	An organizational unit attribute included in a distinguished name solely to support local directory requirements, such as differentiation between human subscribers and devices.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.
Superior CA	In a hierarchical PKI, a CA that has certified the certificate signature key of another CA, and that constrains the activities of that CA. (See subordinate CA).

System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
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 CA in confirming 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 and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
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. [FIPS 140-2]

Appendix D: NASA Form 1824

National Aeronautics and Space Administration

Identity Validation for a Public Key Infrastructure (PKI) Account

(Federal PKI Common Policy and the X.509 Certificate Practice Statement for Department Of Treasury Subordinate Certificate Authorities)

SECTION I - ACCOUNT OWNER INFORMATION *(To be completed by the applicant)*

PRINTED NAME (Last, First, MI):	PRIMARY E-MAIL ADDRESS:		
CENTER:	TELEPHONE NUMBER:	BUILDING/ROOM:	EMPLOYER (EX. NASA, Company Name):

SECTION II - SIGNATURE

Conditions of Issuance

I acknowledge and declare that, prior to applying for, accepting or using the NASA Public Key Certificate, I have read and accepted the conditions in the NASA PKI Subscriber Agreement.

I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

ACCOUNT OWNERS SIGNATURE	DATE

SECTION III - I-9 IDENTITY VERIFICATION *(To be completed by PKI Registration Authority or Trusted Agent)*

For Official Use Only

Identity verification is required prior to approving a PKI Account Application. The employee may present one NASA PIV Badge or two acceptable documents found on the last page of *Form I-9, OMB No. 1615-0047, Employment Eligibility Verification*. The person who examines the documents must be the same person who signs Section IV.

NASA PIV BADGE NUMBER:	CARD UNIQUE IDENTIFIER (CUID):	BADGE EXPIRATION DATE:	
I-9 DOCUMENT TYPE:	ISSUER:	DOCUMENT ID:	EXPIRATION DATE *(If applicable)*:
I-9 DOCUMENT TYPE:	ISSUER:	DOCUMENT ID:	EXPIRATION DATE *(If applicable)*:

NAMS REQUEST NUMBER/COMMENTS:

Section IV - APPROVAL SIGNATURE *(To be completed by PKI Registration Authority or Trusted Agent)*

I have verified the applicant is an active NASA employee or affiliate. I have validated the applicant's biometrics against the I-9 documents recorded above.

I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

PRINTED NAME (Last, First, MI):	SIGNATURE OF APPROVING OFFICIAL:	DATE

NASA Form 1824 07/13 (1.0)

GRS 24.1(1)
Page 1 of 1

Appendix E: Subscriber Agreement

This Subscriber Agreement comes from NASA Procedural Requirements (NPR) 1600.4, *Identify and Credential Management*. The Agreement is applicable to the control and use of both PIV badges and PKI Certificates (PIV authentication certificates, encryption and signing certificates, and card authentication certificates).

Subscriber Agreement

NASA Public Key Infrastructure (PKI) Subscriber Agreement (HSPD-12 compliant badge) (version 1.0, August 2007):

YOU SHALL READ THIS NASA PKI SUBSCRIBER AGREEMENT BEFORE REQUESTING, ACCEPTING, OR USING A NASA HSPD-12 COMPLIANT BADGE. BY SUBMITTING A REQUEST FOR A NASA HSPD-12 COMPLIANT BADGE, YOU ACKNOWLEDGE YOUR ACCEPTANCE OF THE TERMS OF THIS SUBSCRIBER AGREEMENT.

By submitting a request for a NASA HSPD-12 compliant badge you agree to use the badge and any related NASA PKI certificate and services only in accordance with this Subscriber Agreement, including:

- Make true representation at all times regarding information in your HSPD-12 compliant badge request, related Public Key Certificate request, and other identification and authentication information related to a NASA PKI Certificate;

- Use your badge exclusively for authorized NASA business such as to gain access to NASA facilities and/or systems;

- Inform NASA within 24 hours of the loss of your badge;

- Take reasonable precautions to protect your badge from loss, disclosure, modification, or unauthorized use;

- Inform NASA within 48 hours of a change to any information included in your HSPD- 12 compliant badge request and related Public Key Certificate application;

- Return the badge to NASA upon expiration, demand by NASA, or when you no longer require the badge, for reasons including job transfer, extended leave, resignation, or termination of employment. NASA HSPD-12 compliant badge contains a NASA Public Key Certificate suitable for providing authentication.

Failure to abide by NASA certificate policies and practices may constitute grounds for revocation of certificate privileges, and may result in administrative action and/or criminal prosecution under the computer fraud and abuse act (18 U.S.C Sec. 1030 (c)). NASA reserves the right to refuse to issue a NASA Public Key Certificate. Additional information regarding

NASA Public Key Certificates is available at https://icam.nasa.gov/portal/server.pt/community/pki_operations.

This agreement shall be governed by and construed in accordance with United States Federal law. NASA badges and Public Key Certificates are deemed Government supplied equipment, and as such, all users are bound by U.S. Federal law governing the use of Government provided equipment.

If any provision of this Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, all other provisions shall remain in force. Further information, including HSPD-12 badge applicant rights and responsibilities, is available on the Agency Web site at http://hspd12.nasa.gov.

Account Access:

The following statement describes your responsibility for using the badge for logical access to NASA computer assets: Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording, and I will have no expectation of privacy in my use of and content on these systems and the computer equipment. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution. (NPR 2810.1A, 11.3.3.2)

Statement:
I hereby certify that the information provided by me is true and correct to the best of my knowledge and belief. I certify that I am the individual described in the NASA badge request. I agree to maintain control of the badge at all times once my fingerprint activates it and upon receipt and to abide by the agreements above. Once issued to me, I will immediately notify the Center Protective Services Office (Security) if I discover that it is not under my control due to misplacement, loss, or other cause.