Registration Practices Statement

< REGISTRATION AUTHORITY NAME >
Approved < DATE>
Version 1.00

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

This document is the < REGISTRATION AUTHORITY NAME > (<RAN>) Registration Practices Statement (RPS). The RPS outlines the procedures that the community members of <RAN> follow to comply with the CA Profile. If any inconsistency exists between this RPS and the IGTF CLASSIC CA being utilized (the CA), Grid Certificate Practice Statement (CPS), the CA CPS takes precedence.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the <RAN> Registration Practices Statement and was approved by the <RAN>, <CA>, and <any relevant PMA(s)>.

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

The CA is a certification authority (CA) that issues high quality and highly trusted digital certificates in accordance with its CPS. As a CA, the CA performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

1.3.2 Registration Authorities

<RAN> is a Registration Authority (RA) responsible for the verification prior to the issuance of certificates issued under the CA's grid policy. <RAN> (or a third party Operator designated by the <RAN>) operates the RA on behalf of the community and is responsible for ensuring <RAN>'s compliance with this RPS and any associated CPS. <RAN> is obligated to abide by the CA's CPS and any industry standards that are applicable to <RAN>'s role in certificate issuance, management, and revocation.

1.3.3 Subscribers

Subscribers are the members of <RAN> and their associated researchers, students, employees, agents, and subcontractors who use the CA's certificates to conduct secure transactions and communications. Subscribers are not always the party identified in a certificate, such as in a host or device certificate, or robot certificate. The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the Subject of the certificate and the entity that contracted with the CA for the certificate's issuance. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

1.3.4 Relying Parties

Relying Parties are entities that act in reliance on a certificate and/or digital signature facilitated by <RAN>.

1.3.5 Other Participants

1.3.5.1 Trusted Agents

Individuals, including those who are affiliated with <RAN> member organizations are designated as "Trusted Agents" of the CA. Trusted Agents are authorized by <RAN> and the CA to gather documentation in relation to the issuance of a digital certificate. Trusted Agents act as <RAN>'s representative for the purpose of facilitating certificate issuance to the Trusted Agent's employees, contractors, agents, researchers, students, and affiliated entities. Administrators designated by the Trusted Agent organization are responsible for ensuring the Trusted Agent's compliance with this RPS and the respective CPS.

1.4 CERTIFICATE USAGE

A *digital certificate* (or *certificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key.

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate was issued.

1.4.1 Appropriate Certificate Uses

Certificates issued under this RPS will be primarily used for authentication and digital signatures as allowed under the Authentication Profile for Classic X.509 Public Key Certification Authorities with Secure Infrastructure (IGTF CLASSIC Profile) with object identifier 1.2.840.113612.5.2.2.1. <RAN> shall ensure that certificate usages are consistent with those specified in the CA CP and CPS.

1.4.2 Prohibited Certificate Uses

RA will inform Subscribers of the CA's prohibited use requirements.

1.5 PRACTICE STATEMENT ADMINISTRATION

1.5.1 Organization Administering the Document

This RPS is maintained by the <RAN> Operator, which can be contacted at:

____
____
____
____

The CA may be contacted at:
The CA Policy Authority
____
____
____
Tel: ____________________
Eml: ____________________

Contact Person
____
____
____
____

1.5.2 Person Determining RPS Suitability

The <RAN> Operator and the CA or relevant authority are responsible for determining the suitability and applicability of this RPS.

1.5.3 RPS Approval Procedures

The <RAN> Operator and the CA or relevant authority approve this RPS and any amendments. Amendments are made by either updating the entire RPS or by publishing an addendum. Any amendments to the RPS must continue to satisfy IGTF requirements.

NOTE: The CA may require additional controls over and above this RPS in order to meet the CAs CPS.

1.6 DEFINITIONS AND ACRONYMS

“Affiliated Organization” means an organization that has an organizational affiliation with a Subscriber and that approves or otherwise allows such affiliation to be represented in a certificate.

“Applicant” means an entity applying for a certificate.

“Application Software Vendor” means a software developer whose software displays or uses the CA certificates and distributes the CA’s root certificates.

“Key Pair” means a Private Key and associated Public Key.

“OCSP Responder” means an online software application operated under the authority of the CA and connected to its repository for processing certificate status requests.

“Private Key” means the key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

“Public Key” means the key of a key pair that may be publicly disclosed without impacting the integrity of or security of communications and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

“Relying Party” means an entity that relies upon either the information contained within a certificate or a time-stamp token.

“Subscriber” means either entity identified as the subject in the certificate or the entity that is receiving the CA’s time-stamping services.

“Subscriber Agreement” means an agreement that governs the issuance and use of a certificate that the Applicant must read and accept before receiving a certificate.

Abbreviations:

CA	Certificate Authority or Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	The CA Policy Authority
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

This RPS is provided by the <RAN> Operator to Trusted Agents and other interested participants upon receipt of a written request. All other repository responsibilities are the domain of the CA.

2.1 REPOSITORIES

Not Applicable.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

Not Applicable.

2.3 TIME OR FREQUENCY OF PUBLICATION

Not Applicable.

2.4 ACCESS CONTROLS ON REPOSITORIES

Not Applicable.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards for subjectName. The RA will provide name elements pertaining to subscribers in accordance with the CA's CPS.

3.1.2 Need for Names to be Meaningful

Certificates use unique distinguished names to identify both the subject and issuer of the certificate. The name elements provided by the RA will be sufficient for the CA to uniquely identify the subscriber.

3.1.3 Anonymity or Pseudonymity of Subscribers

<RAN> does not provide anonymous <or pseudonymous> name elements.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names are interpreted using X.500 standards. The RA shall ensure that name forms provided to the CA are in compliance with GFD.225.

3.1.5 Uniqueness of Names

Each subjectName element combination provided by the RA must be permanently associated with a single unique entity. Device/host certificates must include the FQDN of the host.

3.1.6 Recognition, Authentication, and Role of Trademarks

RAs must not knowingly approve Applicant requests for certificates with content that infringes on the intellectual property rights of other entities.

3.2 INITIAL IDENTITY VALIDATION

The RA must ensure that approved certificate requests are bound to vetting of the corresponding Applicant's identity.

3.2.1 Method to Prove Possession of Private Key

RAs that collect and process CSRs must do so in a secure manner that reliably ensures the CSR was generated by the Applicant. An Applicant must submit a CSR to establish that it holds the Private Key corresponding to the Public Key in the certificate request. A PKCS#10 format or Signed Public Key and Challenge (SPKAC) is recommended.

3.2.2 Authentication of Organization Identity

There is no current standard for representing Organizational association in Grid Certificates. However, if there is a local requirement for Organizational association, then the RA must verify that: the Applicant's information is verified by having the appropriate Trusted Agent's Administrator verify that (i) the certificate information is correct, (ii) the applicant is authorized to request the certificate, and (iii) the organization information in the certificate request is correct (including the name of the Organization being a meaningful representation of the same).

3.2.3 Authentication of Individual Identity

Either the <RAN> or a Trusted Agent must verify the identity of the Applicant by examining a valid government-issued photo-identification or equivalent document of the applicant during a face-to-face meeting. If an identification document is used, sufficient information about the applicant's identity must be recorded and archived in order to ensure that identity of the individual can be confirmed at a later date.

3.2.4 Non-verified Subscriber Information

The subjectName, subjectAlternativeNames and Public Key association to Applicants MUST be verified by the RA, other elements of the certificate are not guaranteed to be verified by the RA.

3.2.5 Validation of Authority

<RAN> verifies that the Applicant is authorized to request certificates on behalf of themselves or their organization. Trusted Agents are responsible for validating individuals in an organization who are authorized to obtain host certificates for a specific FQDN, and are required to confirm this authority prior to requesting a certificate. The Trusted Agent requesting issuance of a device/host certificate must retain contact information for each device's registered owner and request revocation if the device's sponsor's authorization to use the FQDN in the certificate or the device is known to be terminated.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Certificates authorized by a <RAN> have a validity period of at most 400 days. <RAN> may rekey/renew certificates prior to their expiration date for additional 400 day periods up to a maximum of five years. Applicant may prove identity by demonstrating control of existing private key or else, they must undergo same identity proofing for a new certificate. <RAN> or a Trusted Agent revalidates the certificate information at least once every five years.

3.3.2 Identification and Authentication for Re-key After Revocation

<RAN> must not authorize rekey of a certificate if it was revoked for any reason other than for renewal or update actions. <RAN> must re-verify the information in these certificates using the initial registration process.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The <RAN> Operator must authenticate all revocation requests. The <RAN> Operator may authenticate revocation requests using the Certificate's Public Key, even if the associated Private Key is compromised.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

<RAN> may accept certificate applications from Trusted Agents and other authorized individuals. <RAN> may not provide certificates to any entity that is not eligible or is outside of the <RAN> constituency.

4.1.2 Enrollment Process and Responsibilities

Trusted Agents verify the identity of a certificate applicant prior to authorizing the issuance of a certificate. Trusted Agents and the <RAN> Operator use protected communication to interact with the CA's certificate issuing systems.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

The applicant is verified in accordance with Section 3.2. The <RAN> Operator shall protect all sensitive information obtained from the Applicant in compliance with the Privacy Plan identified in 9.2.4.

4.2.2 Approval or Rejection of Certificate Applications

The <RAN> Operator shall reject any certificate application that it considers inadequately verified. The <RAN> Operator shall also reject a certificate application if issuing the certificate could damage or diminish the CA's reputation or business. Rejected Applicants may re-apply. Subscribers are required to check the data listed in the certificate for accuracy prior to using the certificate.

If some or all of the documentation used to support the application is in a language other than English, an employee of the <RAN> Operator skilled in such language and having the appropriate training, experience, and judgment in confirming organizational identification and authorization performs the final cross-correlation and due diligence. <RAN> may also rely on a translation of the relevant portions of the documentation by a qualified translator.

4.2.3 Time to Process Certificate Applications

<RAN> confirms certificate application information and requests issuance of the digital certificate within a reasonable time frame, usually not more than two business days after receiving all necessary details and documents from the Applicant.

4.3 CERTIFICATE ISSUANCE

4.3.1 Actions during Certificate Issuance

The <RAN> Operator shall verify the source of a certificate request and the identity of the Applicant in a secure manner prior to issuing a certificate.

4.3.2 Notification to Subscriber of Issuance of Certificate

The <RAN> Operator may deliver certificates in any secure manner within a reasonable time after issuance. If there is an issue preventing the approval of the certificate request, the <RAN> shall notify the Applicant in a reasonable time.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

No Stipulation.

4.4.2 Publication of the Certificate

If the <RAN> delivers issued certificates, the <RAN> may use any reliable method to deliver issued certificates in accordance with any applicable stipulations of the Privacy Plan described in Section 9.2.4.

4.4.3 Notification of Certificate Issuance to Other Entities

No Stipulation.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers are required to protect their Private Keys from unauthorized use or disclosure, must discontinue using a Private Key after the expiration of all associated certificates or revocation of any associated certificates, and use Private Keys only as specified in the key usage extension.

4.5.2 Relying Party Public Key and Certificate Usage

No Stipulation.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

The <RAN> Operator may renew a certificate if:

1. the associated private key has not reached the end of its permissible lifetime,
2. the Subscriber name and attributes are unchanged,
3. the associated private key remains un compromised, and
4. re-verification of the Subscriber's identity is not required under Section 3.3.1.

4.6.2 Who May Request Renewal

Trusted Agents or an authorized representative of a Subscriber may request renewal of the Subscriber's certificates to the <RAN>.

4.6.3 Processing Certificate Renewal Requests

No additional verification (besides proof of possession of original private key) is required if the certificate subject information has not changed and less than five years have passed since the certificate's information was verified. Otherwise, the same identification verification requirements for initial request are required. A Trusted Agent must represent that the renewal request is authentic, compliant to these requirements, and still authorized by the appropriate entities.

4.6.4 Notification of New Certificate Issuance to Subscriber

The <RAN> Operator shall use contact information provided by the Subscriber to notify the Subscriber of the certificate's issuance. If there is an issue preventing the approval of the certificate request, the <RAN> shall notify the Applicant in a reasonable time.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No Stipulation.

4.6.6 Publication of the Renewal Certificate

If the <RAN> delivers issued certificates, the <RAN> may use any reasonably reliable method to deliver issued certificates in accordance with any applicable stipulations of the Privacy Plan described in Section 9.2.4.

4.6.7 Notification of Certificate Issuance to Other Entities

No Stipulation.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Rekey

Re-keying a certificate consists of creating a new certificate with a new public key with associated private key, and new serial number while keeping the subject information the same. The new certificate may have a different validity period, key identifiers, CRL and OCSP distributions, and a different signing key. After re-keying a certificate, <RAN> may revoke the old certificate but may not further re-key, renew, or modify the old certificate.

4.7.2 Who May Request Certificate Rekey

A Trusted Agent or the certificate subject may request certificate rekey.

4.7.3 Processing Certificate Rekey Requests

No additional verification (besides proof of possession of original private key) is required if the certificate subject information has not changed and less than five years have passed since the certificate's information was verified. Otherwise, the same identification verification requirements for initial request are required. A Trusted Agent must represent that the rekeying request is authentic, compliant to these requirements, and still authorized by the appropriate entities.

4.7.4 Notification of Certificate Rekey to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate

No stipulation.

4.7.6 Publication of the Issued Certificate

Rekeyed certificates are published by delivering them to Subscribers.

4.7.7 Notification of Certificate Issuance to Other Entities

No stipulation.

4.8 CERTIFICATE MODIFICATION

4.8.1 Who May Request Certificate Modification

Not applicable.

4.8.2 Processing Certificate Modification Requests

Not applicable.

4.8.3 Notification of Certificate Modification to Subscriber

Not applicable.

4.8.4 Conduct Constituting Acceptance of a Modified Certificate

Not applicable.

4.8.5 Publication of the Modified Certificate

Not applicable.

4.8.6 Notification of Certificate Modification to Other Entities

Not applicable.

4.9 *CERTIFICATE REVOCATION AND SUSPENSION*

4.9.1 Circumstances for Revocation

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. Prior to revoking a certificate, <RAN> shall verify the identity and authority of the entity requesting revocation. <RAN> must request revocation of a certificate if any of the following occur:

1. The Subscriber requested revocation of its certificate;
2. The Subscriber did not authorize the original certificate request;
3. Either the Private Key associated with the certificate or the Private Key used to sign the certificate was compromised;
4. The Subscriber breached a material obligation under the CP, the CPS, or the relevant Subscriber Agreement;
5. The Subscriber's or <RAN>'s obligations under the CP or CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
6. The certificate was not issued in accordance with the CP, CPS, or applicable industry standards;
7. <RAN> received a lawful and binding order from a government or regulatory body to revoke the certificate;
8. <RAN>'s right to manage certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);
9. Any information appearing in the Certificate was or became inaccurate or misleading; or
10. The binding between the subject and the subject's public key in the certificate is no longer valid.

4.9.2 Who Can Request Revocation

Subscribers are required to request revocation within one working day after detecting a loss or compromise of the Private Key or if the certificate data is no longer valid. <RAN> may accept revocation requests from entities other than the subscriber. <RAN> may require entities to verify their identity prior to accepting a revocation request. Entities submitting certificate revocation requests should list their identity and explain the reason for requesting revocation.

4.9.3 Procedure for Revocation Request

<RAN> logs each revocation request and submits a copy of the request to the CA. <RAN> will request revocation of certificate if the revocation request originated from the subscriber. If a third party requested revocation, <RAN> will investigate the request before requesting revocation of the certificate. Factors considered in revoking a certificate include the nature of the problem, the number of complaints received, and the entity making the request.

If appropriate, <RAN> may forward complaints to law enforcement.

4.9.4 Revocation Request Grace Period

Revocation grace period is one working day, which is the amount of time Subscribers have to make their request after the activating event. For non-subscribers activating events, the RAN must respond to the request within one working day.

4.9.5 Time within which RA Processes the Revocation Request

The <RAN> Operator processes certificate revocation requests as soon as practically possible, but no later than one working day.

4.9.6 Revocation Checking Requirement for Relying Parties

As specified in the CA CP and CPS.

4.9.7 CRL Issuance Frequency

As specified in the CA CP and CPS.

4.9.8 Maximum Latency for CRLs

As specified in the CA CP and CPS.

4.9.9 On-line Revocation/Status Checking Availability

As specified in the CA CP and CPS.

4.9.10 On-line Revocation Checking Requirements

As specified in the CA CP and CPS.

4.9.11 Other Forms of Revocation Advertisements Available

As specified in the CA CP and CPS.

4.9.12 Special Requirements Related to Key Compromise

As specified in the CA CP and CPS.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

As specified in the CA CP and CPS.

4.10.2 Service Availability

As specified in the CA CP and CPS.

4.10.3 Optional Features

As specified in the CA CP and CPS.

4.11 END OF SUBSCRIPTION

A Subscriber’s subscription service ends if its certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy Practices

<RAN> does not provide key escrow services.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

As specified in the CA CP and CPS.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

This Section covers physical controls applicable to <RAN> systems used to provide RA services.

5.1.1 Site Location and Construction

The <RAN> Operator shall implement a security policy that is designed to detect, deter, and prevent unauthorized access to <RAN>'s operations.

5.1.2 Physical Access

The <RAN> Operator shall protect its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering.

5.1.3 Power and Air Conditioning

The <RAN> must ensure that power and air conditioning resources are sufficient to meet its RA obligations.

5.1.4 Water Exposures

As specified in the CA CP and CPS. The <RAN> must ensure that equipment, critical resources are protected from water related exposure.

5.1.5 Fire Prevention and Protection

The <RAN> must ensure that fire prevention and protection resources are sufficient to allow it to meet its RA obligations.

5.1.6 Media Storage

The <RAN> Operator shall protect <RAN>'s media from accidental damage and unauthorized physical access.

5.1.7 Waste Disposal

The <RAN> Operator shall securely destroy all outdated or unnecessary copies of printed sensitive information before disposal. The <RAN> Operator shall securely destroy all electronic media used in the RA operations.

5.1.8 Off-site Backup

The <RAN> Operator shall maintain at least one full backup and make regular backup copies of any information necessary to recover from a system failure. Such backups must be stored securely in an appropriate off-site location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Personnel acting in Trusted Roles include <RAN>'s system administration personnel and personnel involved with identity vetting and the issuance and revocation of certificates.

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for each Role

<RAN> shall require users accessing RA systems to authenticate first.

5.2.4 Roles Requiring Separation of Duties

<RAN> must comply with CP/CPS requirements for multi-person controls (if any) specified.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

<RAN>'s practices shall provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements

Trusted Agents and/or <RAN> shall provide periodic skills training to all personnel involved in PKI operations. The training relates to the person's job functions and covers:

1. basic Public Key Infrastructure (PKI) knowledge,
2. software versions used by <RAN>,
3. authentication and verification policies and procedures,
4. disaster recovery and business continuity procedures,
5. common threats to the validation process, including phishing and other social engineering tactics, and
6. applicable industry and government guidelines.

<RAN> shall maintain records of who received training and what level of training was completed. <RAN> shall provide these records to the CA upon request.

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Independent Contractor Requirements

No stipulation.

5.3.8 Documentation Supplied to Personnel

<RAN> shall provide personnel in trusted roles the documentation necessary to perform their duties, including a copy of this RPS.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

<RAN> computer systems used to request certificates shall require identification and authentication at system logon using a unique identity and corresponding credential. The <RAN> Operator shall enable all essential event auditing capabilities of its operations in order to record the essential events below. If an application cannot automatically record an event, the <RAN> Operator shall use a manual procedure to satisfy these requirements. For each event, the <RAN> Operator shall record the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. The <RAN> Operator shall make these event records available to the CA and the CA's auditors as proof of <RAN>'s practices.

Auditable Event
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
Successful and unsuccessful attempts to assume a role in <RAN>'s systems
The value of maximum number of authentication attempts to <RAN>'s systems is changed
Maximum number of authentication attempts to <RAN> system's occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
All security-relevant messages that are received by remote access to <RAN>'s systems
Verification activities
Logon attempts to the CA's API through <RAN>'s interface
All certificate compromise notification requests
Known or suspected violations of physical security related to <RAN>'s RA systems
Firewall and router activities related to RA systems
Software error conditions related to <RAN>'s RA activities
Network attacks (suspected or confirmed) related to <RAN>'s RA activities
Violations of the CPS or RPS

5.4.2 Frequency of Processing Log

The <RAN> Operator shall periodically review the logs generated by <RAN>'s systems, make system and file integrity checks, and conduct a vulnerability assessment. During these checks, the <RAN> Operator shall check whether anyone has tampered with the log and scan for anomalies or specific conditions, including any evidence of malicious activity. The <RAN> Operator shall investigate any anomalies or irregularities found in the logs. The <RAN> Operator shall make these logs available to the CA upon request.

5.4.3 Retention Period for Audit Log

The <RAN> Operator shall retain audit logs on-site until after they are reviewed.

5.4.4 Protection of Audit Log

<RAN> Operator systems used in the RA function must retain all generated audit log information until after it is copied by a system administrator. The <RAN> Operator shall configure its RA systems to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period.

5.4.5 Audit Log Backup Procedures

The <RAN> Operator shall make backup copies of its audit logs on a monthly basis.

5.4.6 Audit Collection System (internal vs. external)

Automatic audit processes on RA systems must begin on system startup and end at system shutdown. <RAN> shall promptly notify the CA if the integrity of the system or confidentiality of the information protected by a system is at risk.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

<RAN> shall perform routine risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of its RA systems. <RAN> shall routinely assess the sufficiency of its risk control policies, procedures, information systems, technology, and other arrangements.

5.5 RECORDS ARCHIVAL

<RAN> personnel acting in Trusted Roles or their Trusted Agents, shall comply with all record retention policies that apply by law. <RAN> shall include sufficient detail in all archived records to show that a certificate was issued in accordance with the CPS.

5.5.1 Types of Records Archived

<RAN> personnel acting in Trusted Roles or their Trusted Agents must retain the following information and provide copies of such information upon request to the CA:

1. Contractual obligations and other agreements regarding certificates, including agreements with applicants specifying the terms of certificate use,
2. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2,

<RAN> retains the following information and provides such information to the CA upon request:

1. Certificate and revocation requests,
2. Changes to <RAN>'s audit parameters,
3. Attempts to delete or modify <RAN>'s audit logs,
4. Approval or rejection of a certificate status change request,
5. Certificate compromise notifications,
6. Remedial action taken as a result of violations of physical security, and
7. Violations of the RPS or the CPS by <RAN>, a Trusted Agent, or Subscriber.

5.5.2 Retention Period for Archive

<RAN> shall retain archived data for as long as there are valid certificates whose issuance was based on the archived data (or make arrangements to transfer to the CA if RA's role terminates before all certificates are no longer valid).

5.5.3 Protection of Archive

<RAN> shall store archive records in a manner that prevents unauthorized modification, substitution, or destruction. <RAN> shall maintain any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If the <RAN> Operator needs to transfer any media to a different archive site or equipment, the <RAN> Operator shall maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives must occur in a secure manner.

5.5.4 Archive Backup Procedures

<RAN> shall create an archive disk of the data listed in section 5.5.1 annually and stores it securely for the duration of the retention period.

5.5.5 Requirements for Time-stamping of Records

The <RAN> Operator shall automatically time-stamp archived records with system time (non-cryptographic method) as they are created. The <RAN> Operator shall synchronize its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

<RAN> shall stamp and record information collected during the identity verification process, including IP addresses associated with applicant submissions and screen shots provided by verification information sources where applicable.

5.5.6 Archive Collection System (internal or external)

The <RAN> operator is responsible for collecting and archiving information related to <RAN>'s RA operations.

5.5.7 Procedures to Obtain and Verify Archive Information

The <RAN> Operator may establish procedures that allow parties to obtain archived information. The <RAN> Operator shall make archived information available to the CA after receiving a written request from the CA.

5.6 KEY CHANGEOVER

Not applicable.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The <RAN> Operator shall promptly notify the CA if a disaster causes <RAN>'s RA operations to become inoperative.

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

The <RAN> Operator shall reestablish RA operations as quickly as possible after a disaster or data corruption.

5.7.3 Entity Private Key Compromise Procedures

Not applicable.

5.7.4 Business Continuity Capabilities after a Disaster

The <RAN> Operator shall implement data backup and recovery procedures. The <RAN> Operator shall develop a Business Continuity Management Program (BCMP) that is reviewed, tested, and updated annually.

5.8 RA TERMINATION

Before <RAN> terminates RA activities, the <RAN> Operator shall:

1. Provide notice and information about the termination by sending notice by email to its customers and by posting such information on <RAN>'s web site; and
2. Transfer all certificate responsibilities to the CA.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

Subscriber public keys must be generated in a secure manner that is appropriate for the certificate type.

6.1.2 Private Key Delivery to Subscriber

If <RAN> generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. <RAN> may deliver keys via secure channels or on a hardware cryptographic module. In all cases:

1. <RAN> may not retain a copy of the Subscriber's Private Key after delivery,
2. <RAN> must protect the private key from activation, compromise, or modification during the delivery process,
3. The Subscriber must acknowledge receipt of the private key(s), and
4. <RAN> must deliver the Private Key in a way that ensures that the correct hardware cryptographic modules and activation data are provided to the correct Subscribers, including:
    a. For hardware cryptographic modules, maintaining accountability for the location and state of the module until the Subscriber accepts possession of it and

b. For electronic delivery of private keys, encrypting key material using a cryptographic algorithm and key size at least as strong as the private key. <RAN> will deliver activation data using a separate secure channel.

If a hardware cryptographic module is provided by the <RAN>, the <RAN> shall maintain a record of the Subscriber's acknowledgement of receipt of the module containing the Subscriber's Key Pair. <RAN> provides or retains a copy of this record for auditing by the CA.

6.1.3 Public Key Delivery to Certificate Issuer

The public key is delivered to the Issuer either by the <RAN> or the subscriber in a CSR as part of the certificate request process. The signature on the CSR is authenticated prior to issuing the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

As specified in the CA CP and CPS.

6.1.5 Key Sizes

As specified in the CA CP and CPS.

6.1.6 Public Key Parameters Generation and Quality Checking

As specified in the CA CP and CPS.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

As specified in the CA CP and CPS.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

Certificate Subscribers must protect their Private Keys in accordance with the applicable Guidelines on Private Key Protection, including the use of strong pass phrases to protect private keys.

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

As specified in the CA CP and CPS.

6.2.3 Private Key Escrow

<RAN> does not provide key escrow services.

6.2.4 Private Key Backup

<RAN> does not backup keys.

6.2.5 Private Key Archival

<RAN> does not archive Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All keys must be managed in accordance with the Private Key Protection Guidelines.

6.2.7 Private Key Storage on Cryptographic Module

Keys requiring storage on cryptographic modules must be managed in accordance with the Private Key Protection Guidelines.

6.2.8 Method of Activating Private Keys

Subscribers are solely responsible for protecting their Private Keys in accordance with the Private Key Protection Guidelines.

6.2.9 Method of Deactivating Private Keys
Subscribers should deactivate their Private Keys when not in use.

6.2.10 Method of Destroying Private Keys
Subscribers should destroy their Private Keys if the Private Key is no longer needed.

6.2.11 Cryptographic Module Rating
See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival
As specified in the CA CP and CPS..

6.3.2 Certificate Operational Periods and Key Pair Usage Periods
<RAN> certificates have a maximum validity period in accordance with the profile being used (e.g. Classic, SLCS, etc.) per the applicable CPS.

6.4 ACTIVATION DATA
As specified in the CA CP and CPS.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements
The <RAN> Operator shall secure <RAN>'s systems and authenticate and protect communications between its systems and trusted roles. <RAN>'s servers must be secured and hardened using industry best practices. The <RAN> Operator shall document how their systems are secured against intrusions and compromise.

6.5.2 Computer Security Rating
As specified in the CA CP and CPS.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls
The <RAN> Operator shall control and monitor the acquisition and development of <RAN>'s RA systems. The <RAN> Operator shall only install software on RA systems that is necessary to <RAN>'s operation.

The <RAN> systems shall be procured in a way that does not disclose its intended purpose, thereby minimizing the exposure to risk of tampering.

Software developed in-house or by consultants will be developed using a documented development methodology in a controlled environment. Quality assurance is maintained throughout the process through testing and documentation of the results thereof.

6.6.2 Security Management Controls
The <RAN> Operator has mechanisms in place to control and monitor the security-related configurations of its RA systems, including change control and data entries that are processed, logged and tracked for any security-related changes. When loading software onto a RA system, the <RAN> Operator verifies that the software is the correct version and is supplied by the vendor per <RAN>'s specified configuration.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The <RAN> Operator shall document and control the configuration of its network systems, including any upgrades or modifications made. The <RAN> Operator shall configure its firewalls and boundary control devices to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of its RA services.

All RA equipment is configured with a minimum number of services and all unused network ports and services are disabled. The <RAN> Operator shall allow the CA to review its network configuration upon request.

6.8 TIME-STAMPING

The system time on computers operating the RA process are updated regularly using a reliable time source to synchronize system clocks .

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

As specified in the CA CP and CPS.

7.1.2 Certificate Extensions

As specified in the CA CP and CPS.

7.1.3 Algorithm Object Identifiers

As specified in the CA CP and CPS.

7.1.4 Name Forms

As specified in the CA CP and CPS.

7.1.5 Name Constraints

As specified in the CA CP and CPS.

7.1.6 Certificate Policy Object Identifier

The OIDs used by <RAN> are set forth in the CA's Certificate Profiles document.

7.1.7 Usage of Policy Constraints Extension

As specified in the CA CP and CPS.

7.1.8 Policy Qualifiers Syntax and Semantics

As specified in the CA CP and CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

As specified in the CA CP and CPS.

7.2 CRL PROFILE

As specified in the CA CP and CPS.

7.3 OCSP PROFILE

As specified in the CA CP and CPS.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

<RAN> accepts audits by the CA on the basis of this RPS and the applicable CP and CPS.
Audits of <RAN>'s validation process are conducted using a randomly selected sample of certificates.
<RAN> audits its Trusted Agent's validation process on an annual basis using a randomly selected sample of certificates.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The CA personnel are responsible for auditing <RAN>'s compliance with this RPS and the applicable CP and CPS. <RAN> personnel are responsible for auditing Trusted Agents.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

<RAN> is an RA of the CA. Trusted Agents are members of <RAN>'s organizational group.

8.4 TOPICS COVERED BY ASSESSMENT

Audits of <RAN> cover <RAN>'s systems and validation process. Audits may also include a Trusted Agent's procedure for performing the certificate validation required under this RPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If any audit discovers any material noncompliance with applicable law, this RPS, the CPS, the CP, or any other contractual obligations related to <RAN>'s services (to the extent such information is audited), then (1) the CA will document the discrepancy, (2) the CA will promptly notify the <RAN> Operator, (3) the <RAN> Operator will develop and implement a plan to rectify the noncompliance; and (4) the CA notifies the applicable PMA(s). If <RAN>'s audit of a Trusted Agent discovers any material noncompliance by a Trusted Agent with this RPS, then <RAN> will (1) document the discrepancy, (2) promptly notify the CA, and (3) develop and implement a plan to rectify the non-compliance, and (4) the CA will inform the applicable PMA(s) in its periodic audit reports.

8.6 COMMUNICATION OF RESULTS

The results of an audit are reported to the CA's policy authority and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results.

8.7 SELF-AUDITS

The <RAN> Operator performs regular self-audits to ensure that <RAN> and the Trusted Agents are in compliance with this RPS. To the extent possible, the <RAN> Operator may conduct these audits electronically by requesting a copy via a secure channel of the documentation relied on in issuing the certificate.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

As specified in the CA CP and CPS.

9.2 FINANCIAL RESPONSIBILITY

As specified in the CA CP and CPS.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

The <RAN> Operator shall protect the following as confidential information using a reasonable degree of care:

1. Information and data used to access the CA's systems;
2. Business continuity, incident response, contingency, and disaster recovery plans;

3. Information held by <RAN> as confidential information in accordance with Section 9.4;
4. Audit logs and archive records; and
5. Transaction records, financial audit records, and external or internal audit trail records and any audit reports.

9.3.2 Information Not Within the Scope of Confidential Information

Information not listed as confidential is considered public information. Published certificate and revocation data is considered public information.

9.3.3 Responsibility to Protect Confidential Information

The <RAN> Operator shall contractually obligate its employees, trusted agents, and contractors to protect confidential information. The <RAN> Operator shall ensure that employees, trusted agents and contractors, receive training on how to handle confidential information.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The <RAN> Operator follows the confidentiality policy that is publicly available e.g. on its website, when handling personal information. Personal information is only disclosed when required by law or when requested by the subject of the personal information e.g. as agreed to under subscriber agreements. This may also apply to information considered confidential by organizational entities. The <RAN> Operator will disclose necessary information related to the issuance or use of a certificate to the CA upon request.

9.4.2 Information Treated as Private

The <RAN> Operator shall treat all personal information about an individual as private, unless that information is publicly available in the contents of a certificate or CRL . This may also apply to information considered confidential by organizational entities serviced by the <RAN>. The <RAN> Operator shall protect private information using appropriate safeguards and a reasonable degree of care, including encrypting private information when in transit to and from <RAN>'s RA systems.

9.4.3 Information Not Deemed Private

Private information does not include certificates, CRLs and other forms of validation responses such as OCSP or CT.

9.4.4 Responsibility to Protect Private Information

The <RAN> Operator shall handle information considered private in strict confidence and shall meet the requirements of all applicable laws concerning the protection of data considered confidential. All sensitive information is securely stored and protected against unintended disclosure.

9.4.5 Notice and Consent to Use Private Information

Information that is not included in a certificate that is provided during the application or identity verification process is considered confidential. Unless otherwise stated in the CPS or RPS, a party shall only use information considered confidential after obtaining the subject's express written consent. All Subscribers must consent to the global transfer and publication of any personal data contained in a certificate.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

<RAN> may disclose private information, without notice, when required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual property rights

As specified in the CA CP and CPS.

9.6 Representations and warranties

9.6.1 CA Representations and Warranties

The CA offers the warranties described in its CPS.

9.6.2 RA Representations and Warranties

<RAN> represents that:

1. <RAN>'s certificate issuance and management services conform to this RPS, and to the CA CP and CPS,
2. Information provided by the <RAN> Operator does not contain any false or misleading information,
3. Translations performed by the <RAN> Operator are an accurate translation of the original information, and
4. All certificates requested by the <RAN> Operator meet the requirements of the this RPS, and of the CA CPS.

9.6.3 Subscriber Representations and Warranties

Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to represent to the CA, Application Software Vendors, and Relying Parties that, for each certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide adequate, accurate and relevant information when communicating with the <RAN> Operator,
3. Confirm the accuracy of the certificate data prior to using the certificate,
4. Promptly cease using a certificate and notify the <RAN> Operator if (i) any information that was submitted to the <RAN> Operator or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate,
5. Ensure that individuals using certificates on behalf of an organization have received security training appropriate to the certificate,
6. Use the certificate only for authorized and legal purposes, consistent with the certificate purpose, the CPS, any applicable CP, and the relevant Subscriber Agreement, including only installing SSL certificates on servers accessible at the domain listed in the certificate,
7. Abide by the Subscriber Agreement, the CPS, and this RPS when requesting or using a Certificate,
8. Any further stipulations required by the relevant CP/CPS.

9.6.4 Relying Party Representations and Warranties

As specified in the CA CP and CPS.

9.6.5 Representations and Warranties of Other Participants

As specified in the CA CP and CPS.

9.7 Disclaimers of warranties

The products and services provided under this RPS may be modified or discontinued as set forth in a contract between <RAN> and the CA.

9.8 Limitations of liability

NOTHING HEREIN LIMITS LIABILTY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM the <RAN>'S NEGLIGENCE OR (II) FRAUD COMMITTED BY the <RAN>. EXCEPT AS STATED

ABOVE, ANY ENTITY USING the <RAN> SERVICE WAIVES ALL LIABILITY OF the <RAN> RELATED TO SUCH USE.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether the <RAN> failed to follow any provision of this RPS, or (v) whether any provision of this RPS was proven ineffective. The disclaimers and limitations on liabilities in this RPS are fundamental terms to the use of the <RAN> services.

1.1. INDEMNITIES

9.8.1 Indemnification by <RAN>

<RAN>'s indemnification obligations are set forth in a contract between <RAN> and the CA.

9.8.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber is contractually obligated (e.g. via an online click-through agreement) to indemnify the CA, <RAN> and any cross-signed entities, and their respective partners, directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, the CPS, the RPS, or applicable law; (iii) the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the certificate or Private Key.

9.8.3 Indemnification by Relying Parties

As specified in the CA CP and CPS.

9.9 TERM AND TERMINATION

9.9.1 Term

This RPS and any amendments to the RPS are effective when approved by the CA and the <RAN> Operator and remain in effect until replaced with a newer version.

9.9.2 Termination

This RPS and any amendments remain in effect until replaced by a newer version.

9.9.3 Effect of Termination and Survival

The <RAN> Operator shall communicate the conditions and effect of this RPS's termination in a manner mutually agreed to by the CA and the <RAN> Operator. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination.

9.10 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Notice requirements are set forth in the agreement between the parties.

9.11 AMENDMENTS

9.11.1 Procedure for Amendment

This RPS is reviewed annually. Amendments are made by mutual agreement between the CA and the <RAN> Operator, and may require ratification by the appropriate PMA.

9.11.2 Notification Mechanism and Period

Notices of amendments may be provided to the appropriate PMA but are not provided to any other third party.

9.11.3 Circumstances under which OID Must Be Changed

As specified in the CA CP and CPS.

9.12 DISPUTE RESOLUTION PROVISIONS

As specified in the CA CP and CPS.

9.13 GOVERNING LAW

The laws of the CA's local domicile state or territory govern the interpretation, construction, and enforcement of this RPS and all proceedings related to the CA's and <RAN>'s products and services, including tort claims, without regard to any conflicts of law principles. The courts of the relevant state or territory have non-exclusive venue and jurisdiction over any proceedings related to the RPS or any of the CA and <RAN>'s products or services.

9.14 COMPLIANCE WITH APPLICABLE LAW

As specified in the CA CP and CPS.

9.15 MISCELLANEOUS PROVISIONS

As specified in the CA CP and CPS.

9.16 OTHER PROVISIONS

As specified in the CA CP and CPS.