UAE National Root Certification Authority

Certificate Policy

V 1.4

December 2019

Signature Page

Telecommunication Regulatory Authority	Date

Document History

Document Version	Document Date	Revision Details
DRAFT	April 14, 2014	First draft of the CP
1.0	February 1, 2016	Draft update based on CA operations contractor engaged
1.1	January 3, 2017	TRA Management
1.2	January 2, 2018	Annual Review only – no updates
1.3	December 31, 2018	Annual Review only – no updates
1.4	December 31, 2019	Annual Review only – no updates

References

RFC 3647	Internet X.509 Public Key Infrastructure - Certificate Policies and Certification Practices Framework
RFC 5280	Internet X.509 Public Key Infrastructure - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 6960	Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol – OCSP
UAE Information Assurance Standards	The UAE Information Assurance Standards v1.0
UAE National PKI Certificate Policy	UAE National PKI Certificate Policy v1.0
Secure Communication Policy	UAE National PKI Secure Communication Policy - v1.00
UAE Digital Certificate Interoperability Guidelines	TBD
Business Continuity Management Plan	TBD

Contents

1 Introduction

The UAE has established a national Public Key Infrastructure (PKI) program with the mission to provide standardized Certification Authority (CA) services that enable interoperability and trust across governmental entities, businesses and individuals.

The national PKI program was established with the following strategic objectives:

- Establish and operate national trust anchors
- Obtain international recognition for the national root CAs
- Increase the uptake of digital certificates as enablers of electronic transactions
- Establish a governance model that enables control while promoting innovation
- Encourage collaboration of all stakeholders to improve the national CA ecosystem
- Improve the UAE legal environment to enable the national CA program services

This Certificate Policy (hereinafter, CP) defines the responsibilities of Certification Authorities, Subscribers and Relying Parties that should be adhered to when issuing, managing, and using digital certificates as part of the UAE National PKI.

A PKI that applies this CP may provide some or all of the following PKI management services:

- Key management (generation and storage)
- Certificate generation, modification, re-key, and distribution
- Key escrow and recovery of private keys associated with encryption certificates
- Certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP) response generation and distribution
- Repository management of certificate related items
- System management functions (e.g., security audit, configuration management, archive.)
- Timestamping services

The security of these services is ensured by defining requirements on PKI activities, including the following:

- Subscriber identification and authorization verification.
- Control of computer and cryptographic systems.
- Operation of computer and cryptographic systems.
- Usage and protections of keys and public key certificates by Subscribers and Relying Parties.
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met.

The Telecommunication Regulatory Authority (TRA) is established to set public policies governing the operation of all components of the National Public Key Infrastructure (PKI) and manage the operational components (Examples include Certification Authorities, Registration Authorities, repositories among others.) of the National PKI. The TRA serves the interest of UAE government entities, private organizations, and citizens and residents as Relying Parties within the National PKI.

Any use of or reference to this CP outside the purview of the Telecommunication Regulatory Authority is completely at the using party's risk. An Entity shall not assert the OIDs defined in this CP in any certificates an Issuing CA produces, except in accordance with the policies and uses cases defined herein.

This CP is consistent with the Internet Engineering Task Force (IETF PKIX) [RFC 3647], Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, with regard to format and content recommendations.

The terms and provisions of this CP shall be interpreted under and governed by applicable UAE laws and regulations.

The UAE National PKI conforms to the current version of the guidelines adopted by the Certification Authority/Browser Forum ("CAB Forum") when issuing publicly trusted certificates, including the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") and the Guidelines for Extended Validation Certificates ("EV Guidelines") both of which are published at https://www.cabforum.org. With regard to SSL/TLS Server Certificates or Code Signing Certificates, if any inconsistency exists between this CP and the Baseline Requirements or the EV Guidelines, then the EV Guidelines take precedence for EV Certificates and the Baseline Requirements take precedence for publicly trusted SSL certificates. Time-stamping services are provided according to IETF RFC 3161 and other technical standards.

1.1 Overview

The UAE National PKI Certificate Policy (UAE PKI CP) is the national policy under which Certification Authorities within the public administration are established and operated as part of the UAE National PKI.

This CP defines the creation and management of Version 3 X.509 public key certificates for multiple use cases covered within the UAE National PKI. Such applications include, but are not limited to, electronic mail, transmission of unclassified and classified information, signature of electronic documents, contract formation signatures, and authentication of infrastructure components such as web servers, firewalls, and directories.

The UAE PKI CP (this CP) is only one of several documents that govern the UAE National PKI. Other important documents include Certification Practice Statements, registration authority agreements and practice statements, subscriber agreements, relying party agreements, customer agreements, privacy policies, and memoranda of agreement. The TRA may publish additional certificate policies or certification practice statements as necessary to describe other related service offerings. These supplemental policies and statements may be made available to applicable users or relying parties on a need to know basis.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CP is divided into nine parts that cover the security controls and practices and procedures for certificate or time-stamping services within the scope of the UAE National PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement "Not applicable" or "No stipulation".

This CP does not define a particular implementation of PKI, nor the plans for future implementations of future Certificate Policies. This document will be reviewed and updated as described in Section 1.5, based on operational experience, changing threats, and further analysis. The latest CP document is available at: http://ca.darkmatter.ae/CPS.

1.2 Document Name and Identification

This document is referred to as the UAE PKI CP, recognized under the following identifications:

- Title: UAE Public Key Infrastructure Certificate Policy
- Version: 1.1
- Object identifier (OID): 2.16.784.1.1.7.35.2.0.1.1.1

The OID for the UAE National PKI is joint-iso-ccitt (2) country (16) UAE (784) UAE-government (1) federal government (1) federal authorities (7) Agency (35) UAE National PKI (2). The OID arcs for the various certificates and documents described in this CP are assigned under this arc as follows:

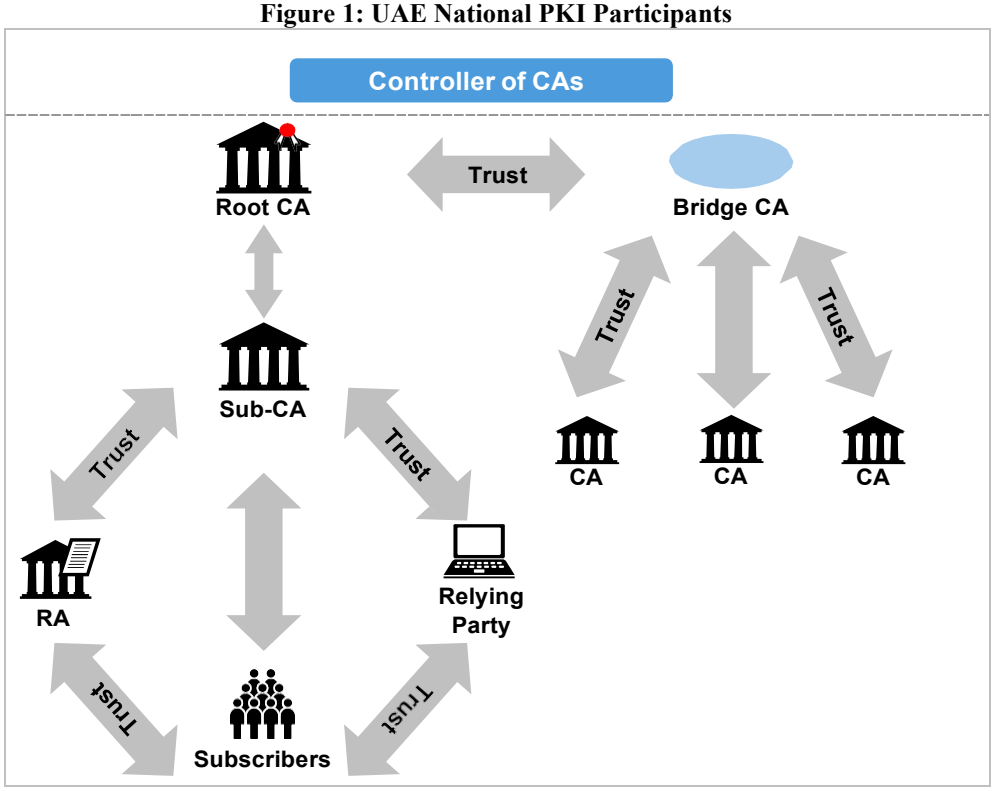
Object Description	Object Identifier (OID)
Certification Policy Documents	2.16.784.1.1.7.35.2.0.1
This CP document	2.16.784.1.1.7.35.2.0.1.1.1
Certificate Profiles	2.16.784.1.1.7.35.2.2
TLS Certificates	2.16.784.1.1.7.35.2.2.1
UAE EV TLS Certificates	2.16.784.1.1.7.35.2.2.1.1
UAE OV TLS Certificates	2.16.784.1.1.7.35.2.2.1.2
Client Certificates	2.16.784.1.1.7.35.2.2.2
UAE Authentication Certificate	2.16.784.1.1.7.35.2.2.2.1
UAE SMIME Dual Use	2.16.784.1.1.7.35.2.2.2.2
UAE SMIME Digital Signature	2.16.784.1.1.7.35.2.2.2.3
UAE SMIME Encryption	2.16.784.1.1.7.35.2.2.2.4
UAE SMIME Escrow Encryption	2.16.784.1.1.7.35.2.2.2.5
UAE Device	2.16.784.1.1.7.35.2.2.2.6
Object Signing Certificates	2.16.784.1.1.7.35.2.2.3
UAE Code Signing	2.16.784.1.1.7.35.2.2.3.1
UAE EV Code Signing	2.16.784.1.1.7.35.2.2.3.2
UAE Document Signing	2.16.784.1.1.7.35.2.2.3.3

Certain certificates in the UAE National PKI may be issued using alternate hierarchies under Root CAs, which are automatically trusted in browsers and other commonly used software (Please see Annex C for a description of additional policy identifiers that may be employed to facilitate this option). For these certificates, this CP should be read in conjunction with the relevant CP/CPS of the Public Trust Partner (available at https://ca.darkmatter.ae/iCPS).

1.3 PKI Participants

In the UAE, five types of entities fill the roles of participants within the UAE National Public Key Infrastructure. The parties mentioned hereunder are collectively called PKI participants and include Certification Authorities, Registration Authorities, Subscribers, Relying Parties, and Controller of Certification Authorities as illustrated in Figure 1. The following sections introduce the PKI participants involved in issuing and maintaining key management certificates. More details on specific roles within the PKI participants are described in detail in Section 5.2.

Figure 1: UAE National PKI Participants



All communications among the participants within the PKI regarding any phase of the life cycle of certificates should be in compliance with the UAE PKI Secure Communication Policy.

1.3.1 Certification Authorities

Within a PKI, a Certification Authority (CA) is a trusted entity that performs functions associated with Public Key certificate life cycle events, including receiving certificate requests, issuing, revoking and renewing a certificate, and validating the certificates it issues.

A subordinate CA is an entity that is issued a CA Certificate by a Root CA (or possibly another subordinate CA) where the Private Key associated with that subordinate CA Certificate is authorized only to be used in accordance with, and operated within infrastructure maintained in accordance with the policies specified by the issuing CA. For ease of reference herein, all CAs issuing certificates in accordance with this CP are hereafter referred to as "Issuing CAs."

1.3.2 Registration Authorities

The Registration Authority (RA) is an entity that has been delegated the responsibility by a CA to establish enrollment procedures for certificate applicants, perform identification and authentication of certificate applicants, deliver the certificates, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA.

An Issuing CA shall monitor each RA's compliance with this Policy, the CPS, and if applicable, any Registration Practices Statement (RPS) under which the RA operates. An Issuing CA that relies on a variety of RAs or Identity Management (IDM) systems to support various communities of interest may submit an RPS for each RA or IDM to the TRA for approval. The RPS must contain details necessary for the TRA to determine how the RA achieves compliance with this Policy. Necessary details include how the RA's process or IDM establishes the identities of applicants, how the integrity and authenticity of such identifying information is securely maintained and managed, and how changes and updates to such information are communicated to the Issuing CA.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate or who assumes responsibility for the operation of the device or service named in the certificate, who asserts that it uses its key and certificate in accordance with the Certificate Policy asserted in the certificate, and who does not itself issue certificates. CAs are sometimes technically considered "Subscribers" in a PKI when for instance the Root CA in this PKI issues certificates to these CAs for cross-certification.

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 Issuing CA for the certificate's issuance. Prior to verification of identity and issuance of a certificate, a Subscriber is an Applicant. However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information. Therefore, the UAE National PKI Root CAs (NRCA) does not issue certificates directly to Subscribers, except for specific tests with written approval of the controller (Refer to 1.3.5).

1.3.4 Relying Parties

A Relying Party uses a Subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber among other PKI functions. The Relying Party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate to determine the suitability of the certificate for a particular use. More details on validation services are described in Section 4.10.

This document makes no assumptions or limitations regarding the identity of Relying Parties. Relying Parties are not required to have an established relationship with the UAE National PKI Root CAs and are outside the scope of this document.

1.3.5 Controller of Certifying Authorities

The Controller of Certifying Authorities is the custodian of the National CA program and is responsible for setting regulations and guidelines, and monitoring CA activity to ensure adherence to the National CA Program's strategic objectives.

The Controller of Certifying Authorities has the following responsibilities:

- Establishing and maintaining Certificate Policies utilized by authorized PKIs through the function of the TRA.
- Overseeing CA core business activities to ensure compliance to overarching standards for the National CA Program.
- Reviewing public and commercial CAs license applications.
- Issuing licenses to approved public CAs applications.
- Developing national regulations and guidelines for Certificate Practice Statements for Sub-CAs and Bridge CAs through the function of the TRA.
- Ensuring appropriate policy governance through the function of the TRA.
- Performing audits on all CAs operating in the National CA program and issuing corrective orders to those not abiding by required standards.
- Revoking licenses from CAs and Bridge CAs that are no longer fit to operate.

The Telecommunications Regulatory Authority (TRA) is the Controller of Certification Authorities operating under this document. The TRA operates under the direction of the Controller of Certifying Authorities.

1.4 Certificate Usage

A digital certificate (or certificate) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital certificate potentially allows an entity taking part in an electronic transaction to

prove its identity to other participants in such transactions, depending on the data included in the certificate. A time stamp token (TST) cryptographically binds a representation of data to a particular time stamp, thus establishing evidence that the data existed at a certain point in time.

1.4.1 Appropriate Certificate Uses

Certificates issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the certificate. The sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. Organizations must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each organization for each application and is not controlled by the CP.

1.4.2 Prohibited Certificate Uses

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 issued.

Public Trust Issuing CAs in the UAE National PKI must not be used for Man in the Middle (MITM) purposes or for the traffic management of domain names or IP addresses that the Subject entity does not own or control

1.5 Policy Administration

1.5.1 Organization Administering the Document

The TRA within the Controller of Certifying Authorities is responsible for the development, publishing and amendment of this document.

1.5.2 Contact Person

Questions regarding this document shall be directed to:

Telecommunication Regulatory Authority

Abu Dhabi

Phone:

9712777 2229

Email: info@TRA.gov.ae

1.5.3 Person Determining CPS Suitability for the Policy

The Controller of Certifying Authorities via the TRA is responsible for asserting whether a CPS conforms to this CP.

The determination of suitability is based on an independent compliance auditor's results and recommendations.

1.5.4 CPS Approval Procedures

The Issuing CA submits its CPS and the results of a compliance audit to the TRA of the Controller of Certification Authorities for approval.

The Controller of Certifying Authorities via the TRA accepts or rejects the CA CPS and accompanying compliance audit. If rejected, the CA is tasked to resolve the identified discrepancies.

When the resolutions are documented, a compliance audit will be conducted and the results resubmitted to the TRA of the Controller of Certification Authorities for review and approval.

1.6 Definitions and Acronyms

Refer to Annex A and Annex B.

2 Publication and Repository Responsibilities

2.1 Repositories

All CAs that issue publicly trusted certificates under this Policy are obligated to post all corresponding publicly trusted CA certificates and cross-certificates issued by or to the CA and corresponding CRLs or other applicable status information issued by the publicly trusted CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid publicly trusted certificates issued by that CA. Private trust certificates will be published in accordance with the stipulation of the corresponding CPS. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

The publicly accessible repository system used to provide information regarding publicly trusted certificates and cross-certificates and their corresponding status information shall be designed and implemented so as to provide high availability 24 hours a day, 7 days a week.

2.2.2 Publication of CA Information

This CP shall be publicly available. The CPS of publicly trusted CA's will also be published. There is no requirement to publish a CPS for private trust CAs; a CPS summary however shall either be publicly available or available upon request.

2.3 Time or Frequency of Publication

An updated version of this CP will be made publicly available within thirty (30) days of the incorporation of changes. A corresponding CPS update (where required to be published), shall be made available thirty (30) days after an update. Issuing CAs shall publish CA certificates and revocation data as soon as possible after issuance.

2.4 Access Controls on Repositories

Information published in a repository is public information. The Issuing CA shall provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories. The CA shall protect information not intended for public dissemination or modification.

Publicly trusted CA certificates and CRLs in the repository shall be publicly available through the Internet. The CPS shall detail what information in the repository shall be exempt from automatic availability, and under which conditions the restricted information may be made available.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The CA shall assign a Distinguished Name (DN) to each Subscriber that complies with ITU X.500 standards. Subscriber certificates may contain any name type appropriate to the certificate application.

3.1.2 Need for Names to be Meaningful

Names used in certificates shall not be ambiguous and must represent an identifier for the Subscriber. Names should be meaningful enough, irrespective of whether the entity is a person, machine, or organization.

CA certificates that assert the UAE National PKI Certificate Policy shall not include a personal name, but rather shall identify the subject as a CA and include the name-space for which the CA is authoritative.

When applicable, Issuing CAs shall ensure that each User Principal Name (UPN) is unique and accurately reflects organizational structures.

3.1.3 Anonymity or Pseudonymity of Subscribers

Issuing CAs may issue end-entity anonymous or pseudonymous certificates provided that (i) such certificates are not prohibited by applicable policy (e.g. for certificate type, assurance level, or certificate profile) and (ii) name space uniqueness is preserved.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.500 standards and ASN.1 syntax. Rules for interpreting e-mail addresses are specified in [RFC 2822] see also [RFC 2253] and [RFC 2616] for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

The CA shall ensure that created names uniquely identify the Subscribers of that CA. The names should conform to X.500 standard for name uniqueness.

3.1.6 Recognition, Authentication, and Role of Trademarks

The CA shall not knowingly use trademarks in names unless the subject has the rights to use that name. However, the CA is not obligated to research trademarks or resolve trademark disputes. Issuing CAs may reject any application or require revocation of any certificate that is part of a trademark dispute.

3.2 Initial Identity Validation

An Issuing CA may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. The Issuing CA may refuse to issue a certificate solely at its discretion.

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession and control of the private key, which corresponds to the public key in the certificate request. The CA shall ensure that any mechanism or procedure used ties the private key to the identity being asserted by the Subscriber.

3.2.2 Authentication of Organization Identity

Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing CA certificates, the CA or RA shall verify the information, in addition to the authenticity of the representative to act in the name of the CA.

For Subscriber organization certificates, the CA shall verify the existence of the organization by verifying the identity and address of the organization, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

Issuing CAs and RAs shall identify high risk certificate requests and shall conduct additional verification activity and take additional precautions as are reasonably necessary to ensure that high risks requests are properly verified.

3.2.3 Authentication of Individual Identity

The CA or RA shall ensure that the Subscriber's identity information is verified in accordance with the procedures detailed in the corresponding CPS or RPS that meet the minimum required detailed in the table below.

Certificate Type	Identity Verification
SSL Server Certificates and Object Signing Certificates (issued to an Individual)	The Applicant shall submit a legible copy of at least one currently valid government-issued photo ID (passport or Emirates ID). If the Issuing CA or RA requires further assurance, the Applicant shall provide additional forms of identification, including non-photo and non-governmental forms of identification such as recent utility bills, financial account statements, Applicant credit card, additional ID credential, or equivalent document type. The Issuing CA or RA shall confirm that the Applicant is able to receive communication by telephone, postal mail/courier, or fax. If the Issuing CA or RA cannot verify the Applicant's identity using the procedures described above, then the Issuing CA or RA shall obtain a Declaration of Identity*

	witnessed and signed by a Registration Authority, trusted agent, notary, lawyer, accountant, or any entity certified by a State or National Government as authorized to confirm identities.
EV SSL Certificates issued to a Sole Proprietor	As specified in the CA-Browser Forum EV Guidelines (See annex C)
Authentication Certificates	The entity controlling the secure location represents that the certificate holder has authorization to access the physical location or logical resource.
Grid Certificates	Either the RA responsible for the grid community or a trusted agent must obtain a copy of the Applicant's photo ID or a similar identity document during a face-to-face meeting with the Applicant or a trusted agent must attest that the Applicant is personally known to the trusted agent. If an identification document is used, the RA must retain sufficient information about the Applicant's identity in order to verify the Applicant at a later date.
Level 1 Client - Personal	Applicant's control over an email address (or any of the identity verification methods listed for a higher level client certificate).
Level 1 Client - Enterprise	Any one of the following: 1. In-person appearance before an RA or trusted agent with presentment of an identity credential (e.g., driver's license or birth certificate). 2. Using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as: - the ability to place or receive calls from a given number; or - the ability to obtain mail sent to a known physical address. 3. Through information derived from an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, employer, or retail company). Acceptable information includes: - the ability to obtain mail at the billing address used in the business relationship; or - verification of information established in previous transactions (e.g., previous order number); or - the ability to place calls from or receive phone calls at a phone number used in previous business transactions. 4. Any method required to verify identity for issuance of a Level 2, 3, or 4 Client Certificate
Level 2 Client	This level of assurance requires that the Issuing CA or RA verify that the asserted name matches: (a) a government-issued photo-ID (either a passport of Emirates ID); (b) the individual's date of birth; and (c) a current address or personal telephone number. The Issuing CA or RA shall verify the Applicant's identity using one of the following four (4) methods: 1. In-person proofing before an RA or trusted agent with presentment of a government-issued photo ID, examined for authenticity and validity. An entity certified by a State or National Government as authorized to confirm identities

	may perform in-person authentication on behalf of the RA, provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data. 2. Remotely verifying information provided by applicant (including name, date of birth, and current address or telephone number) using (i) a government-issued photo ID and (ii) one additional form of ID such as another government-issued ID, an employee or student ID card number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the applicant's residence. The Issuing CA or RA may confirm an address by issuing the credentials in a manner that confirms the address of record and may confirm a telephone number by recording the applicant's voice during a communication after associating the telephone number with the applicant in records that are available to the Issuing CA or RA. 3. If the Issuing CA or RA has a current, ongoing relationship with the Applicant, the Issuing CA or RA may verify identity using an exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo ID, and (b) the ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret. 4. Any of the methods required to verify identity for issuance of a Level 3 or 4 Client Certificate.
Level 3 Client	In-person proofing before an RA, trusted agent, or an entity certified, either by a local Emirate or the Federal Government, that is authorized to confirm identities (provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner and that the RA is not relieved of its responsibility to verify the presented data). The Applicant shall provide at least one Federal Government-issued Picture I.D., an Emirates ID, or two Non-Federal Government I.D.s, one of which must be a photo I.D. (e.g., driver's license). The Issuing CA or RA shall examine the credentials for authenticity and validity. For each Level 3 Client Certificate issued, the Issuing CA or the RA shall review and record a Declaration of Identity which shall be signed by the applicant and the person performing the in-person identification. The Issuing CA or RA shall verify the provided information (name, date of birth, and current address) to ensure legitimacy and may verify it electronically by a record check with the specified issuing authority or through similar databases to establish the existence of such records with matching name and reference numbers and to corroborate date of birth, current address of record, and other personal information sufficient to ensure a unique identity. A trust relationship between an RA or trusted agent and the applicant notice of assurance sent to the address of record. If the photo ID does not confirm the Applicant's address of record, then the certificate shall be issued in a manner that confirms the address of record. For all Level 3 Client Certificates, the identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance. that is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement provided that (1) it meets the thoroughness and rigor of in-person proofing described

	above, (2) supporting ID proofing artifacts exist to substantiate the antecedent relationship, and (3) mechanisms are in place that bind the individual to the asserted identity. If the photo ID is valid and confirms the address of record for the Applicant, then the certificate may be approved for issuance with notice of issuance sent to the address of record. If the photo ID does not confirm the Applicant's address of record, then the certificate shall be issued in a manner that confirms the address of record. For all Level 3 Client Certificates, the identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance.
Level 4 Client e.g. Emirates Identity Authority (EIDA)	In-person proofing before an RA, trusted agent, or an entity certified, either by a local Emirate or the Federal Government, that is authorized to confirm identities (provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner and that the RA is not relieved of its responsibility to verify the presented data). The Application shall supply (i) one Federal Government-issued Picture I.D., an Emirates ID, or two Non-Federal Government I.D.s, one of which must be a photo I.D. (e.g., driver's license) and (ii) the contemporaneous collection of at least one biometric (e.g. photograph or fingerprints) to ensure that the Applicant cannot repudiate the application. The Issuing CA or RA shall examine the credentials for authenticity and validity. For each Level 4 Client Certificate issued, the Issuing CA or the RA shall review and record a Declaration of Identity* that is signed by the applicant and the person performing the in-person identification. For all Level 4 Client Certificates the use of an in-person antecedent is not applicable and the Applicant shall establish his or her identity no more than 30 days prior to initial certificate issuance. Issuing CAs and RAs shall issue Level 4 Client Certificates in a manner that confirms the Applicant's address of record.

The CA or RA may accept authentication of a Subscriber's identity attested to and documented by a trusted agent to support identity proofing of remote Subscribers.

At a minimum, authentication procedures for individual Subscribers must include the following:

1. The identity of the person performing the identity verification;
2. A signed declaration by that person that he or she verified the identity of the applicant;
3. The date and time of the verification; and
4. A declaration of identity signed by the applicant.

If an Applicant cannot participate in face-to-face registration, a trusted person who already has a certificate of the same type applied for by the Applicant may represent the Applicant during the validation process. The trusted person must present their certificate and the Applicant's information to the person performing the face-to-face registration.

3.2.3.1 Authentication for Role-based Client Certificates

An Issuing CA may issue certificates that identify a specific role that the Subscriber holds, provided that the role identifies a specific individual within an organization (e.g., Chief Information Officer is a unique individual whereas Program Analyst is not). These role-based certificates are used when nonrepudiation is desired. The Issuing CA may only issue role-based certificates to Subscribers who first obtain an individual

Subscriber certificate that is at the same or higher assurance level as the requested role-based certificate. An Issuing CA may issue certificates with the same role to multiple Subscribers. However, the Issuing CA shall require that each certificate have a unique key pair. Individuals may not share their issued role-based certificates and are required to protect the role-based certificate in the same manner as individual certificates.

The Issuing CA or an RA shall verify the identity of the individual requesting a role-based certificate (i.e. the sponsor) in accordance with Section 3.2.3 and record the information identified in Section 3.2.3 for a sponsor associated with the role before issuing a role-based certificate. The sponsor must hold an individual certificate in his/her own name issued by the same CA at the same or higher assurance level as the role-based certificate.

IGTF Certificates are not issued as role-based certificates.

3.2.3.2 Authentication for Group Client Certificates

If several entities are acting in one capacity and non-repudiation is not necessary, the Issuing CA may issue a certificate corresponding to a Private Key shared by multiple Subscribers. The Issuing CA or RA shall record the information identified in Section 3.2.3 for a sponsor from the Information Systems Security Office or equivalent before issuing a group certificate.

In addition, the Issuing CA or the RA shall:

1. Require that the Information Systems Security Office, or equivalent, be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to the private key, and account for the time period during which each Subscriber had control of the key,
2. Not include a subjectName DN in the certificate that could imply that the subject is a single individual,
3. Require that the sponsor provide and continuously update a list of individuals who hold the shared private key, and
4. Ensure that the procedures for issuing group certificates comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

Interoperable Global Trust Federation (IGTF) Certificates are not issued as group certificates.

3.2.3.3 Authentication of Devices with Human Sponsors

An Issuing CA may issue a Level 1, 2, 3 or 4 Client or Federated Device Certificate for use on a computing or network device, provided that the entity owning the device is listed as the subject. In such cases, the device must have a human sponsor who provides:

1. Equipment identification (e.g., serial number) or service name (e.g., DNS name),
2. Equipment public keys,
3. Equipment authorizations and attributes (if any are to be included in the certificate), and
4. Contact information.

If the certificate's sponsor changes, the new sponsor shall review the status of each device to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

The Issuing CA shall verify all registration information in accordance with the requested certificate type. Acceptable methods for performing this authentication and integrity checking include:

1. Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested)
2. In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.

3.2.4 Non-Verified Subscriber Information

Issuing CAs are not required to confirm that the common name in a Level 1 - Personal Client Certificate is the legal name of the Subscriber. Any other non-verified information included in a certificate shall be designated as such in the certificate. No unverified information shall be included in any Level 2, Level, 3, Level 4, Object Signing, or EV certificate.

3.2.5 Validation of Authority

The Issuing CA or RA shall verify the authorization of a certificate request as follows:

Certificate Type	Verification
DV SSL, OV SSL and Device Certificates	An authorized contact listed with the Domain Name Registrar, a person with control over the domain name, or through communication with the applicant using a reliable method per Section 11.2.3 of the Baseline Requirements.
EV SSL	In accordance with the EV Guidelines.
Object Signing Certificates	An authoritative source within the organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a reliable means of communication
Level 1 Client - Personal	An individual has control over the email address listed in the certificate.
Level 1 Client - Enterprise	A person who has technical or administrative control over the domain name and verifying the requester's control over the email address listed in the certificate.
IGTF Certificates	Pursuant to the relevant requirements by the accreditation authority.
Levels 2, 3 and 4 Client	Individuals affiliated with the organization who confirm the applicant's authority to obtain a certificate indicating the affiliation and who agree to request revocation of the certificate when that affiliation ends.

Certificates that contain explicit or implicit organization affiliations shall be issued only after ascertaining the Subscriber has the authorizations to act on behalf of the organization in the implied capacity. Examples of these include group and role certificates, and CA and RA certificates.

3.2.6 Criteria for Interoperation

The Certificate and CRL Profile, and this CP shall form a basis for assessing interoperability within the UAE National PKI.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

An Issuing CA may allow Subscribers of SSL and Code Signing Certificates to authenticate themselves over a TLS/SSL session with username and password. Each Subscriber shall reestablish its identity using the initial registration processes of section 3.2 according to the following table:

Certificate Type	Routine Re-Key Authentication	Re-Verification Required
OV SSL Certificates	Username and password	At least every 39 months
EV SSL Certificates	Username and password	According to the EV Guidelines
Subscriber EV Code Signing Certificates	Username and password	At least every 39 months
Signing Authority EV Code Signing Certificates	Username and password	At least every 123 months
Timestamp EV Code Signing Certificates	Username and password	At least every 123 months
Object Signing Certificates	Username and password	At least every six years
Level 1 Client Certificates	Username and password	At least every nine years
Level 2 Client Certificates	Shared secret (PIN/password) meeting NIST 800-63 Level 2 entropy requirements (Table A.2)	At least every nine years
Level 3 and 4 Client Certs	Current signature key only	At least every nine years
IGTF Certificates	Username and password, RA attestation after comparison of identity documents, re-authenticate through an approved IdM, or through associated private key	At least every 13 months. However, certificates associated with a private key restricted solely to a hardware token may be rekeyed or renewed for a period of up to 5 years

The Issuing CA shall not re-key a certificate without additional authentication if doing so would allow the Subscriber to use the certificate beyond the limits described above.

For re-key of any CA certificate or Subscriber issued under this certificate policy, identity may be established through use of current signature key as long as the validity period of the new certificate does not extend beyond the periodic in-person authentication requirements.

3.3.2 Identification and Authentication for Re-Key after Revocation

In the event of certificate revocation (for reasons other than as the result of a routine certificate renewal, update, or modification action), issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.2.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated by the Issuing CA or the RA that would be responsible for approving the certificate's issuance. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The Certificate application process must provide sufficient information before the certificate issuance to:

- Establish the applicant's authorization to obtain a certificate;
- Establish and record identity of the applicant;
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required; and
- Verify any role or authorization information requested for inclusion in the certificate.

4.1.1 Who can Submit a Certificate Application

A certificate application may be submitted to the CA by the Subscriber, or an RA on behalf of the Subscriber.

No individual or entity listed on a government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the United Arab Emirates may be accepted as an applicant for a certificate.

4.1.2 Enrollment Process and Responsibilities

Entities and Subscribers applying for certification are responsible for providing accurate information on their certificate applications.

The Issuing CA is responsible for ensuring that the identity of each Certificate Applicant is verified in accordance with this CP and the applicable CPS prior to the issuance of a certificate.

All communication among PKI Authorities supporting the certificate application and issuance process is authenticated and protected from modification. Any electronic transmission of shared secrets and personally identifiable information shall be protected. Where electronic communication is used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used.

4.2 Certificate Application Processing

Information in certificate applications must be verified as accurate before certificates are issued.
Procedures to verify information in certificate applications shall be specified in the applicable CPS or RPS.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the Subscriber shall be done by the CA, or a RA on behalf of the Subscriber. The Issuing CA shall ensure that all communication between the Issuing CA and an RA regarding certificate issuance or changes in the status of a certificate are made using secure and auditable methods. If databases or other sources are used to confirm sensitive or confidential attributes of an individual subscriber, then that sensitive information shall be protected and securely exchanged in a

confidential and tamper-evident manner, protected from unauthorized access, and tracked using an auditable chain of custody.

4.2.2 Approval or Rejection of Certificate Applications

The certificate application may be rejected for various reasons such as inaccurate information, or any reasonable basis, including if the certificate could damage the Issuing CA's business or reputation. The Issuing CA shall reject any certificate application that cannot be verified. At their sole discretion, the CA or RA may work with appropriate parties to resolve certificate application issues.

A certificate application shall not be considered accepted until the CA has accepted the application and decided to issue a certificate. Issuing CAs and RAs shall follow industry standards when approving and issuing certificates. The Issuing CA or RA shall contractually require subscribers to verify the information in a certificate prior to using the certificate.

4.2.3 Time to Process Certificate Applications

All parties involved in certificate application processing shall use reasonable efforts to ensure that certificate applications are processed in a timely manner. Identity shall be established no more than 30 days before initial issuance of Level 3 and Level 4 Certificates.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Upon receiving the request, the CA or RA should:

- Verify the identity of the requester as specified in Section 3.2
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1
- Sign and issue the certificate if all certificate requirements have been met
- Make the certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged their obligations as described in Section 9.6.3

The Issuing CA and any RA shall protect databases under its control and that are used to confirm Subscriber identity information from unauthorized modification or use. All authorization and other attribute information received from a prospective Subscriber shall be verified before inclusion in a certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs shall inform the Subscriber of the creation of a certificate and may use any reliable mechanism to make the certificate available to the Subscriber. For device certificates, the CA shall issue the certificate according to the certificate requesting protocol used by the device and, if the protocol does not provide inherent notification, also notify the authorized organizational representative of the issuance.

4.4 Certificate Acceptance

The CA makes available to the Subscriber its responsibilities through the Subscriber Agreement and the Subscriber accepts this agreement through any effective use of its private key.

4.4.1 Conduct Constituting Certificate Acceptance

A certificate is deemed as accepted by the Subscriber if the certificate is used or the Subscriber failed to object to the certificate or its contents within a reasonable time.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

During the validity period, the intended scope of usage for a private key is specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

The Subscriber shall not use the signature private key after the associated certificate has been revoked or has expired. The Subscriber may continue to use the decryption private key solely to decrypt previously encrypted information after the associated certificate has been revoked or has expired.

4.5.2 Relying Party Public Key and Certificate Usage

The relying parties shall rely upon a public key in a certificate only when it is used for the purposes indicated by the key usage extension and the Extended key usage extension, if either of those extensions is present, and also if the relying party has verified with the CA that the certificate is still valid.

A Relying Party should use discretion when relying on a certificate and should consider the totality of the circumstances and risk of loss prior to relying on a certificate. Relying on a digital signature or certificate that has not been processed in accordance with applicable standards may result in risks to the Relying Party. The Relying Party is solely responsible for such risks. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate.

4.6 Certificate Renewal

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. The old certificate should be revoked.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key.

CA Certificates may be renewed so long as the aggregated lifetime of the public key does not exceed the certificate lifetime.

4.6.2 Who May Request Renewal

For all CAs operating under this Policy, the corresponding operating authority may request renewal of its own certificate. Only a Subscriber or their authorized representative may request renewal of the Subscriber's certificates.

4.6.3 Processing Certificate Renewal Requests

The Issuing CA may require reconfirmation or verification of the information in a certificate prior to renewal. For renewal requests, digital signatures should be validated before electronic renewal requests are processed. Alternatively, renewal requests may be processed using the same process used for initial certificate issuance.

4.6.4 Notification of New Certificate Issuance to Subscriber

CAs shall inform the Subscriber of the renewal of a certificate and make the new certificate available to the Subscriber.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

For certificate acceptance, the same conditions apply for a renewed certificate as for a new certificate (Refer to Section 4.4.1).

4.6.6 Publication of the Renewal Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-Key

Re-keying a certificate means that a new certificate is created that has the same characteristics and abiding by the same certificate policies as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key), may specify different CRL and/or OCSP distribution points, have a different serial number, and it may be assigned a different validity period.

After certificate re-key, the old certificate should be revoked. After re-keying a Client Certificate, the Issuing CA may not re-key, renew, or modify the old certificate.

4.7.1 Circumstance for Certificate Re-Key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtain new keys. Examples of circumstances requiring certificate re-key include: expiration, loss or compromise.

Subscribers requesting Client Certificate re-key should identify themselves using their current signature key as permitted by Section 3.3.1 to establish proof of control of existing private key. Subscribers of other types of certificates shall identify and authenticate themselves as stated in the applicable CPS.

4.7.2 Who May Request Certification of a New Public Key

The Issuing CA may initiate certificate re-key at the request of the certificate subject, an RA, or in its own discretion.

4.7.3 Processing Certificate Re-Keying Requests

For re-keying requests, digital signatures should be validated before electronic re-key requests are processed. Alternatively, re-keying requests may be processed using the same process used for initial certificate issuance (see Section 3.3.1).

4.7.4 Notification of New Certificate Issuance to Subscriber

CAs shall inform the Subscriber of the renewal of a certificate and may use any reliable mechanism to make the new certificate available to the Subscriber.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

A certificate is deemed as accepted by the Subscriber if the certificate is used or the Subscriber failed to object to the certificate or its contents within a reasonable time frame.

The Subscriber has a responsibility to verify the accuracy of the issued certificate.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Certificate modification consists of creating new certificates with subject or extension information (e.g., non-essential parts of names or email address) that differs from the old certificate. The new certificate may have the same or different subject public key.

After certificate modification, the old certificate is revoked.

4.8.1 Circumstance for Certificate Modification

A CA may modify a CA or Online Certificate Status Protocol (OCSP) responder certificate whose characteristics have changed (e.g. assert new policy OID). The new certificate may have the same or a different subject public key.

A CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., name change due to marriage). The new certificate shall have the same or a different subject public key. After modifying a client certificate, the Issuing CA may not re-key, renew, or modify the old certificate.

4.8.2 Who May Request Certificate Modification

The Subscriber or RA may request the modification of a Subscriber certificate together with evidences for the correctness of the required modification.

4.8.3 Processing Certificate Modification Requests

For modification requests, digital signatures should be validated before electronic modification requests are processed. Alternatively, modification requests may be processed using the same process used for initial certificate issuance.

After receiving a request for modification, the Issuing CA shall verify any information that will change in the modified certificate. The Issuing CA may issue the modified certificate only after completing the verification process on all modified information. The validity period of a modified certificate must not extend beyond the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

CAs shall inform the Subscriber of the issuance of a modified certificate and may use any reasonable means to make the new certificate available to the Subscriber.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

A certificate is deemed as accepted by the Subscriber if the certificate is used or the Subscriber failed to object to the certificate or its contents within a reasonable time frame.

The Subscriber has a responsibility to verify the accuracy of the issued certificate.

4.8.6 Publication of the Modified Certificate by the CA

As specified in Section 2.1, all modified CA certificates shall be published in repositories.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

CAs operating under this policy shall issue status information (e.g. CRLs or OCSP) covering all unexpired certificates issued under this Policy with exception for OCSP responder certificates.

4.9.1 Circumstances for Revocation

Certificates shall be revoked if at least one of the following circumstances is known to exist:

- The Subscriber requested revocation of its certificate.
- The Subscriber did not authorize the original certificate request and did not retroactively grant authorization.
- A certificate contains information that is not valid or no longer valid, including if Applicant has lost its rights to a trademark or the domain name listed in the certificate.
- The certificate was not issued in accordance with the CP, CPS, or applicable industry standards.
- The certificate has been illegally extended.
- The certificate can no longer guarantee that a signature verification key can be assigned to a specific person.
- The private key of the Subscriber has been changed, lost, stolen, made public or otherwise compromised or misused.
- The Subscriber is no longer entitled to hold the certificate (Refer to 1.3.3).

- Either the Subscriber's or the Issuing CA'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.
- The CA does not comply with imposed requirements.
- The Issuing CA received a lawful and binding order from a government or regulatory body to revoke the certificate.
- The Subscriber or the cross-certified CA breached a material obligation under the CP, the CPS, or the relevant agreement.
- The certificate in question is no longer needed.
- The used algorithms and key sizes are not considered secure any more, or if the technical content or format of the Certificate presents an unacceptable security risk to application software vendors, Relying Parties, or others.
- The Issuing CA ceased operations and did not arrange for another certificate authority to provide revocation support for the certificate.
- The Subscriber was added as a denied party or prohibited person to a blacklist, or is operating from a destination prohibited under UAE law.
- For code-signing certificates, the certificate was used to sign, publish, or distribute malware or other harmful content, including any code that is downloaded onto a user's system without their consent.

The Issuing CA shall revoke a certificate if the binding between the subject and the subject's public key in the certificate is no longer valid or if an associated Private Key is compromised.

If a certificate expresses an organizational affiliation, the Issuing CA or the RA shall require the Affiliated Organization to inform it if the subscriber affiliation changes. If the Affiliated Organization no longer authorizes the affiliation of a Subscriber, then the Issuing CA shall revoke any certificates issued to that Subscriber containing the organizational affiliation. If an Affiliated Organization terminates its relationship with the Issuing CA or RA such that it no longer provides affiliation information, the Issuing CA shall revoke all certificates affiliated with that Affiliated Organization.

An Issuing CA or cross-certified entity shall request revocation of its cross-certificate if it no longer meets the stipulations of this or other asserted policies, as indicated by the policy OIDs in certificates or those listed in the policy mapping extension of the cross-certificate.

4.9.2 Who can Request Revocation

The Issuing CA or RA shall accept revocation requests from authenticated and authorized parties, such as the certificate Subscriber and the Affiliated Organization named in a certificate. The Issuing CA or RA may establish procedures that allow other entities to request certificate revocation for fraud or misuse. The Issuing CA shall revoke a certificate if it receives sufficient evidence of compromise of loss of the Private Key. The Issuing CA may revoke a certificate of its own volition without reason, even if no other entity has requested revocation. A legally recognized representative of either party to a cross-signed CA certificate may request revocation.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The Issuing CA or RA shall authenticate and log each revocation request. The Issuing CA will always revoke a certificate if the request is authenticated as originating from the Subscriber or the Affiliated Organization listed in the certificate. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, the Issuing CA or RA shall investigate the alleged basis for the revocation request.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this Policy; Subscribers and authorized PKI entities shall request the revocation of a certificate as soon as the need for revocation comes to their attention. Issuing CAs and RAs are required to report the suspected compromise of their CA or RA private key and request revocation to both the policy authority and operating authority of the superior issuing CA (e.g., cross- signing CA, Root CA, etc.) immediately upon discovery. Subscribers shall request revocation as soon as possible (within one day after detection) if the Private Key corresponding to the Certificate is lost or compromised or if the Certificate data is no longer valid.

4.9.5 Time Within which CA Must Process the Revocation Request

An Issuing CA shall revoke a certificate within one hour of receiving appropriate instruction from the TRA. An Issuing CA shall revoke the CA certificate of a subordinate or cross-signed CA as soon as practical after receiving proper notice that the subordinate or cross-signed CA has been compromised. If an Issuing CA or the TRA determines that immediate revocation is not practical, because the potential risks of revocation outweigh the risks caused by the compromise, then the Issuing CA and the TRA shall jointly determine the appropriate process to follow in order to promptly revoke the subordinate or cross-signed CA certificate. In all cases the TRA is the ultimate authority for making this decision.

The Issuing CA shall revoke other certificates as quickly as practical after validating the revocation request. The Issuing CA shall process revocation requests as follows:

1. Before the next CRL is published, if the request is received two or more hours before regular periodic CRL issuance,
2. By publishing it in the CRL following the next CRL, if the request is received within two hours of the regularly scheduled next CRL issuance, and
3. Regardless, within 18 hours after receipt.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on the information listed in a certificate, a Relying Party is recommended to confirm the validity of each certificate in the certificate path in accordance with IETF PKIX standards, including checks for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each certificate in the chain..

4.9.7 CRL Issuance Frequency (if applicable)

CRLs shall be issued periodically per the CPS, even if there are no changes to be made, to ensure timeliness of information.

Certificate status information shall be published no later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote operation.

4.9.8 Maximum Latency for CRLs (if applicable)

CRLs shall be published within 4 hours of generation (and no later than 18 hours after notification of compromise). Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

4.9.9 On-Line Revocation/Status Checking Availability

Where on-line status checking is supported, the Issuing CA shall ensure that the certificate status information distributed meets or exceeds the requirements for CRL issuance and latency stated in sections 4.9.5, 4.9.7 and 4.9.8.

4.9.10 On-Line Revocation Checking Requirements

Relying party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs. A relying party shall confirm the validity of a certificate via CRL or OCSP in accordance with section 4.9.6 prior to relying on the certificate.

4.9.11 Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA's approved CPS; and
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method meets the issuance and latency requirements for CRLs stated in sections 4.9.5, 4.9.7, and 4.9.8.

4.9.12 Special Requirements Re-Key Compromise

The Issuing CA or the RA shall use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects that its Private Key has been compromised. The Issuing CA must have the ability to transition any revocation reason to code to "key compromise". If a certificate is revoked because of compromise or suspected compromise, the Issuing CA shall issue a CRL within 18 hours after it receives notice of the compromise or suspected compromise.

4.9.13 Circumstances for Suspension

Certificate suspension is not recommended unless there is a narrowly defined use-case and the intended Relying Party interpretation of the suspension is clearly communicated. In that case, the following subsections must be completed.

4.9.14 Who can Request Suspension

For CA certificates, suspension is not permitted.

For Subscriber certificates, there is no stipulation.

4.9.15 Procedure for Suspension Request

No stipulation for end entity certificates.

4.9.16 Limits on Suspension Period

No stipulation for end entity certificates.

4.10 Certificate Status Services

There is no requirement to operate a certificate status service, but it is often perceived as more efficient and can provide more timely information if the service obtains status information more frequently than client applications.

4.10.1 Operational Characteristics

Issuing CAs shall make certificate status information available via CRL or OCSP. The Issuing CA shall list revoked certificates on the appropriate CRL where they remain until one additional CRL is published after the end of the certificate's validity period, except for EV Code Signing Certificates, which shall remain on the CRL for at least 365 days following the certificate's validity period.

4.10.2 Service Availability

If a certificate status service is offered, it will be operated 24x7 without interruption.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

The Issuing CA shall allow Subscribers to end their subscription to certificate services by having their certificate revoked or by allowing the certificate or applicable Subscriber Agreement to expire without renewal.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Subscriber keys may be escrowed to provide key recovery. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the Subscriber. Under no circumstances shall a Subscriber signature key be held in trust by a third party. CAs that support private key escrow for key management keys shall document their specific practices in their CPS.

Subscribers and other authorized entities may request recovery of an escrowed Private Key. Entities escrowing Private Keys shall have personnel controls in place that prevent unauthorized access to Private Keys. Key recovery requests can only be made for one of the following reasons:

1. The Subscriber has lost or damaged the private key token,
2. The Subscriber is not available or is no longer part of the organization that contracted with the Issuing CA for Private Key escrow,

3. The Private Key is part of a required investigation or audit,
4. The requester has authorization from a competent legal authority to access the communication that is encrypted using the key,
5. If key recovery is required by law or governmental regulation, or
6. If the entity contracting with the Issuing CA for escrow of the Private Key indicates that key recovery is mission critical or mission essential.

An entity receiving Private Key escrow services shall:

1. Notify Subscribers that their Private Keys are escrowed,
2. Protect escrowed keys from unauthorized disclosure,
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys,
4. Release escrowed keys only for properly authenticated and authorized requests for recovery, and
5. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key-related information, or the facts concerning any key recovery request or process.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

CAs that support session key encapsulation and recovery shall identify the document describing the practices in the applicable CPS.

5 Facility, Management and Operational Controls

5.1 Physical Controls

CA equipment shall be dedicated to performing CA functions. RA equipment shall be operated to ensure that the equipment meets all physical controls at all times.

All CA and RA equipment, including cryptographic modules, shall be protected from theft, loss, and unauthorized access at all times.

5.1.1 Site Location and Construction

The Issuing CA shall perform its CA operations from a secure data center equipped with logical and physical controls that make the CA operations inaccessible to non-trusted personnel. The site location and construction, when combined with other physical security protection mechanisms such as guards, door locks, and intrusion sensors, shall provide robust protection against unauthorized access to CA equipment and records.

RAs must protect their equipment from unauthorized access in a manner that is appropriate to the level of threat to the RA, including protecting equipment from unauthorized access while the cryptographic module is installed and activated and implementing physical access controls to reduce the risk of equipment tampering, even when the cryptographic module is not installed and activated.

5.1.2 Physical Access

Each Issuing CA, RA, and all OCSP Responder equipment shall always be protected from unauthorized access and physical controls shall be implemented to reduce the risk of equipment tampering.

The Issuing CA shall manually or electronically monitor its systems for unauthorized access at all times, maintain an access log that is inspected periodically, and require two-person physical access to the CA hardware and systems. An Issuing CA shall deactivate, remove, and securely store its CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and must not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA equipment or private keys.

If the facility housing the CA equipment is ever left unattended, the Issuing CA's administrators shall verify that:

1. the CA is in a state appropriate to the current mode of operation,
2. the security containers are properly secured,
3. physical security systems (e.g., door locks, vent covers) are functioning properly, and
4. the area is secured against unauthorized access.

The Issuing CA shall make a person or group of persons explicitly responsible for making security checks. If a group of persons is responsible, the Issuing CA shall maintain a log that identifies who performed the security check. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Power and Air Conditioning

The CA shall have backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing CA certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on elevated floors).

5.1.5 Fire Prevention and Protection

Fire alarm systems and fire suppression mechanisms should be implemented to protect CA equipment against fire.

5.1.6 Media Storage

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Media that contains security audit and archive information for backup purposes shall be stored in a location separate from the CA primary operations facility.

5.1.7 Waste Disposal

Normal office waste shall be removed or destroyed in accordance with local policy. Media used to collect or transmit information discussed in Section 9.4 shall be destroyed prior to disposal, such that the information is unrecoverable.

5.1.8 Off-Site Backup

A system backup shall be made when a CA system is activated. If the CA system is operational for more than a week, backups shall be made at least once per week. Backups shall be stored offsite. Only the latest backup needs to be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

The data backup media shall be stored in a facility approved for storage of information of the same value of the information that will be protected by the certificates and associated private keys issued or managed using the equipment with a minimum requirement of transferring, handling, packaging, and storage of the information in a manner compliant with requirements for sensitive material.

5.2 Procedural Controls

5.2.1 Trusted Roles

CA and RA personnel acting in trusted roles include system administration personnel and personnel involved with identity vetting, the issuance and revocation of certificates, and the escrow and recovery of keys. Issuing CAs and RAs shall distribute the functions and duties performed by persons in trusted roles in a way that prevents one person from circumventing security measures or subverting the security and trustworthiness of the PKI. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of CA and RA operations. Senior management of the Issuing CA or the RA shall be responsible for appointing individuals to trusted roles. A list of such personnel shall be maintained and reviewed annually.

5.2.1.1 Administrator

The CA Administrator role shall be responsible for:

- Installing, configuring, and maintaining the CA systems;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates;
- Configuring CA audit parameters;
- Generating and backing up CA keys;
- Controlling and managing CA cryptographic modules;
- Managing system backups and recovery; and
- Changing recording media.

Administrators do not issue certificates to Subscribers.

5.2.1.2 Officer

The officer role is responsible for:

- Registering new Subscribers and requesting the issuance of certificates;
- Verifying the identity of Subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates;
- Requesting, approving and executing the revocation of certificates;
- Approving infrastructure certificates issued to support the operations of the CA;
- Approving revocation of certificates issued to CAs or to support the operations of the CA;
- Approving certificates issued to RAs and trusted agents;
- Authorizing RAs and trusted agents;
- Approving revocation of certificates issued to RAs; and
- Posting Certificates and CRLs.

5.2.1.3 Operator

The operator role is responsible for:

- Installing and configuring system hardware, including servers, routers, firewalls, and network configurations;
- Keeping systems updated with software patches and ensuring time services are accurate and synchronized;
- Maintaining and monitoring Intrusion Prevention services, malware protections, and responding to network related incidents or outages; and
- Any other maintenance activities needed for system stability and recoverability.

5.2.1.4 Security Auditor

The Auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA or RA is operating in accordance with the CPS or RPS.

5.2.2 Number of Persons Required per Task

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions and physical access to the CA system. The following tasks shall require two or more persons:

- Generation, activation, and backup of CA keys;
- Physical access to CA equipment; and
- Access to any copy of the CA cryptographic module.

5.2.3 Identification and Authentication for Each Role

Individuals shall identify and authenticate themselves before being permitted to perform any actions set forth above for that Trusted Role. On all accounts capable of directly causing certificate issuance, multi-factor authentication must be enforced.

5.2.4 Roles Requiring Separation of Duties

Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. The Issuing CA and RA may enforce separation of duties using CA equipment, procedurally, or by both means. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, and individuals serving as Auditors shall not perform or hold any other trusted role.

An individual that performs any trusted role shall only have one identity when accessing CA equipment.

5.3 Personnel Controls

Personnel Security plays a critical role in the CA facility's overall security system. Personnel Security shall be designed to prevent both unauthorized access to the CA facility and CA systems and compromise of sensitive CA operations by CA personnel.

5.3.1 Qualifications, Experience, and Clearance Requirements

Issuing CA and RA personnel and management who purport to act within the scope of this document shall be selected on the basis of loyalty, trustworthiness, and integrity. Any individual appointed to a trusted role shall meet the following:

- Be an employee or contractor of the CA and bound by terms of employment or contract;
- Be appointed in writing;
- Have successfully completed the appropriate training program;
- Have demonstrated the ability to perform the assigned duties;
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 5.2.1; and
- Have not been previously relieved of trusted role duties for reasons of negligence or non-performance of duties.

Managerial personnel involved in time-stamping operations must possess experience with information security and risk assessment and knowledge of time-stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures.

The Issuing CA or the RA shall ensure that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CP.

5.3.2 Background Check Procedures

Individuals fulfilling Trusted Roles shall pass an extensive background check conducted by the CA, or

A competent independent authority that has the authority to perform background investigations. The background check should include at least the following:

- Confirmation of previous employment;
- Confirmation of previous residence;
- Check of professional reference;
- Confirmation of the highest or most relevant educational degree obtained;

- Search of criminal records;
- Search of driver's license records; and
- Identification verification.

The Issuing CA or RA shall require each individual to appear in-person before a trusted agent whose responsibility it is verify identity. The trusted agent shall verify the identity of the individual using at least one form of government-issued photo identification. Checks of previous residences are over the past three years. All other checks are for the prior five years. The Issuing CA or RA shall verify the highest education degree obtained regardless of the date awarded and shall refresh all background checks at least every ten years.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA receive comprehensive trainings based on the assigned duties. Training shall be conducted in the following areas:

- Basic Public Key Infrastructure knowledge;
- CA security principles and mechanisms;
- All PKI software versions in use for the CA;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures;
- Common threats to validation processes, including phishing and other social engineering tactics; and
- The EV guidelines.

Issuing CAs shall maintain a record of who received training and what level of training was completed. Issuing CAs and RAs shall ensure that Validation Specialists have the minimum skills necessary to satisfactorily perform validation duties before they are granted validation privileges.

5.3.4 Retraining Frequency and Requirements

Personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. All individuals responsible for PKI Trusted Roles shall be made aware of changes in the CA and RA operation. Any significant change to the operations shall have a training plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions as documented in organization policy shall be taken against personnel who perform unauthorized actions involving the CA's systems, the certificate status verification systems, and the repository. Disciplinary actions may include measures up to and including

termination or agency and criminal sanctions, and shall be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

Contractor personnel filling trusted roles shall be subject to all requirements stipulated in this document. Independent contractors and consultants who have not completed or passed the background check procedures specified above shall be permitted access to the CA's secure facilities only to the extent they are escorted and directly supervised by a person holding trusted role at all times.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4 Audit Logging Procedures

Issuing CA and RA systems shall require identification and authentication at system logon. Important system actions shall be logged to establish the accountability of the operators who initiate such actions.

Audit log files shall be generated for all events relating to the security of the CAs and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.1 Types of Events Recorded

All essential security auditing capabilities of CA and RA operating system and applications shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- Date and time the event occurred;
- Type of event;
- Success or failure where applicable; and
- Identify of the user or system that caused the event or initiated the action.

All event records shall be available to auditors as proof of the CA or RA practices.

The audit records of the CA include:

SECURITY AUDIT

- Any changes to the audit parameters, e.g., audit frequency, type of event audited.
- Any attempt to delete or modify the audit logs.
- Obtaining a third-party time-stamp.

AUTHENTICATION TO SYSTEMS

- Successful and unsuccessful attempts to assume a role.
- The value of maximum number of authentication attempts is changed.
- Maximum number of authentication attempts occur during user login.

- An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts.
- An administrator changes the type of authenticator, e.g., from a password to a biometric.
- Attempts to set passwords.
- Attempts to modify passwords.
- Logon attempts to applications.
- Escalation of privilege.

LOCAL DATA ENTRY

- All security-relevant data that is entered in the system.

REMOTE DATA ENTRY

- All security-relevant messages that are received by the system.

DATA EXPORT AND OUTPUT

- All successful and unsuccessful requests for confidential and security-relevant information.

KEY GENERATION

- Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys).

PRIVATE KEY LOAD AND STORAGE

- The loading of component private Keys.
- All access to subscriber Private Keys retained within the CA for key recovery purposes.

TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE

- All changes to the trusted public keys, including additions and deletions.

SECRET KEY STORAGE

- The manual entry of secret keys used for authentication.

PRIVATE AND SECRET KEY EXPORT

- The export of private and secret keys (keys used for a single session or message are excluded).

CERTIFICATE REGISTRATION

- All certificate requests, including issuance, re-key, renewal, and revocation.
- Certificate issuance events.
- Verification activities.

CERTIFICATE REVOCATION

- All certificate revocation requests.

CERTIFICATE STATUS CHANGE APPROVAL

- The approval or rejection of a certificate status change request.

CA CONFIGURATION

- Installation of the operating system.
- Installation of the CA applications.
- Installing hardware cryptographic modules.
- Removing hardware cryptographic modules.
- Re-key of the CA applications.
- Destruction of cryptographic modules.
- System startup.
- Any security-relevant changes to the configuration of a CA system component.

ACCOUNT ADMINISTRATION

- Roles and users are added or deleted.
- The access control privileges of a user account or a role are modified.
- Appointment of an individual to a trusted role.
- Designation of personnel for multi-party control.

CERTIFICATE PROFILE MANAGEMENT

- All changes to the certificate profile.

REVOCATION PROFILE MANAGEMENT

- All changes to the revocation profile.

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT

- All changes to the certificate revocation list profile.

TIME STAMPING

- Clock synchronization.

MISCELLANEOUS

- Receipt of hardware / software.
- Backup or restoration of the internal CA database.
- File manipulation (e.g., creation, renaming, moving).
- Posting of any material to a repository.
- Access to the internal CA database.
- All certificate compromise notification requests.
- Loading hardware security modules (HSMs) with Certificates.
- Shipment of HSMs.
- Zeroizing HSMs.

CONFIGURATION CHANGES

- Hardware.
- Software.
- Operating System.
- Patches.
- Security Profiles.

PHYSICAL ACCESS / SITE SECURITY

- Personnel access to secure area housing CA component.
- Access to a CA component.
- Known or suspected violations of physical security.
- Firewall and router activities.

ANOMALIES

- System crashes and hardware failures.
- Software error conditions.
- Software check integrity failures.
- Receipt of improper messages.
- Misrouted messages.
- Network attacks (suspected or confirmed).
- Equipment failure.
- Electrical power outages.
- Uninterruptible Power Supply (UPS) failure.
- Obvious and significant network service or access failures.
- Violations of a CPS.
- Resetting Operating System clock.

5.4.2 Frequency of Processing Log

The audit log shall be reviewed at least once per month along with making system and file integrity checks, and performing a vulnerability assessment. The Issuing CA or RA may use automated tools to scan for anomalies or specific conditions. All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CA and RA since the last review shall be examined.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained on-site until after they are reviewed. A history of audit logs will be archived in accordance with Section 5.5 of this CP. The individual who removes audit logs from the CA or RA system shall be an official different from the individuals who, in combination, command the CA signature key.

5.4.4 Protection of Audit Log

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. Audit logs shall be protected to prevent alteration and detect tampering.

Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

The CA shall make regular backup copies of audit logs and audit log summaries and send a copy of the audit log off-site at least once every month.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system could be internal or external to the CA or RA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, the Issuing CA or RA shall consider suspending its operation until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this Policy.

5.4.8 Vulnerability Assessments

The CA 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 any certificate data or certificate issuance process. The Issuing CA shall also routinely assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the Issuing CA has in place to control such risks. The Issuing CA's auditors should review the security audit data checks for continuity and alert the appropriate personnel of any events, such as repeated failed

actions, requests for privileged information, attempted access of system files, and unauthenticated responses..

5.5 Records Archival

The Issuing CA shall comply with any record retention policies that apply by law. The Issuing CA shall include sufficient detail in archived records to show that a certificate was issued in accordance with the CPS.

5.5.1 Types of Records Archived

At a minimum, CA/RA shall record the following data for archive (where applicable):

- CA/RA accreditation
- Certificate policy versions
- Certification practice statement versions
- Other relevant national policies
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration
- Certificate and revocation requests
- Certificate compromise notifications
- Subscriber identity authentication data as per section 3.2.3
- Documentation of receipt and acceptance of certificates or tokens
- Subscriber agreements
- Issued certificates
- All CRLs issued and/or published
- All Audit logs
- Other data or applications to verify archive contents
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g. audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Key generation
- Export of Private Keys
- All access to Subscriber private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- Documentation of destruction of a cryptographic module
- Appointment of an individual to a trusted role
- Remedial action taken as a result of violations of physical security
- Violations of CP and CPS

5.5.2 Retention Period for Archive

Archive records must be kept for a minimum of 10 years without any loss of data. RAs may retain archived data for a shorter period of time if the practice is documented in a RPS or document retention policy and approved by the CA.

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive.

Archive media shall be stored in a safe, secure storage facility separate from the CA/RA in a manner that prevents unauthorized modification, substitution, or destruction of the contents. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

5.5.4 Archive Backup Procedures

The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

CA/RA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain and Verify Archive Information

The Issuing CA may archive data manually or automatically. If automatic archival is implemented, the Issuing CA shall synchronize its archived data on a periodic basis as defined in the CPS.

The Issuing CA may allow Subscribers to obtain a copy of their archived information. Otherwise, the Issuing CA shall restrict access to archive data to authorized personnel in accordance with the Issuing CA's internal security policy and shall not release any archived information except as allowed by law. The Issuing CA shall maintain, and provide upon receipt of a proper request by such authorized person, the procedures it follows to create, verify, package, transmit, and store archived information.

5.6 Key Changeover

To minimize risk from compromise of a CA’s private signing key, that key may be changed; from that time on, only the new key shall be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs, then the old key shall be retained and protected.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CA organizations shall have an Incident Response Plan and a Disaster Recovery Plan. The Issuing CA shall review, test, and update its Incident Response Plan and DR/BCP, and supporting procedures, at least annually.

If a hacking attempt or other form of potential compromise of a CA becomes known, it shall be investigated in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise the scope of potential damage shall be assessed in order to determine the most appropriate response.

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

The CA shall maintain backup copies of system, databases, and private keys in order to rebuild the CA capability in case of software and/or data corruption.

If a disaster causes the Issuing CA's operations to become inoperative, the Issuing CA shall, after ensuring the integrity of the CA systems, re-initiate its operations on replacement hardware using backup copies of its software, data, and Private Keys at a secure facility. The Issuing CA shall give priority to reestablishing the generation of certificate status information. If the Private Keys are destroyed, the Issuing CA shall reestablish operations as quickly as possible, giving priority to generating new key pairs.

5.7.3 Entity Private Key Compromise Procedures

If the Issuing CA suspects that a CA Private Key is comprised or lost then the Issuing CA shall follow its Incident Response Plan and immediately assess the situation, determine the degree and scope of the incident, and take appropriate action. Issuing CA personnel shall report the results of the investigation. The report must detail the cause of the compromise or loss and the measures should be taken to prevent a reoccurrence. If there is a compromise or loss, a superior CA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient manner. The superior CA shall notify any affiliated entities so that they may issue CRLs revoking cross-certificates issued to the Issuing CA and shall notify interested parties and make information available that can be used to identify which certificates are affected, unless doing so would breach the privacy of the Issuing CA's user or the security of the Issuing CA's services. The Issuing CA shall cease its CA operations until appropriate steps are taken to recover from the compromise and restore security.

If the CA is a Root-CA, the trusted self-signed certificate must be removed from Relying Party trust stores, and any new certificate distributed via secure out-of-band mechanisms. Root-CAs shall describe their approaches to reacting to a Root-CA key compromise in their CPSs.

5.7.4 Business Continuity Capabilities after a Disaster

CAs shall be required to maintain a Disaster Recovery Plan.

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations shall be re-established as quickly as possible, giving priority to the ability to revoke Subscriber's certificates. If the CA cannot re-establish revocation capabilities prior to date and time specified in the nextUpdate field in the currently published CRL issued by the CA, then the inoperative status of the CA shall be reported to the trust anchor managers and Superior CA. The trust anchor managers and Superior CA shall decide whether to declare the CA private signing key as compromised and re-establish the CA keys and certificates, or allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the CA shall request that its certificates be revoked. The CA installation shall then be completely rebuilt by re-establishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates. Finally, all Subscriber certificates will be re-issued. In such events, any Relying Parties who continue to use certificates signed with the destroyed private key do so at their own risk, and the risk of others to whom the data is forwarded, as no revocation information will be available (if the CRL signing key was destroyed).

5.8 CA or RA Termination

When a CA operating under this Policy terminates operations before all certificates have expired, Entities will be given as much advance notice as circumstances permit and shall transfer its responsibilities and records to any successor entities. If a qualified successor does not exist, the Issuing CA shall transfer all relevant records to a government supervisory or legal body.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA / RA Key Pair Generation

All publicly trusted CA keys must be generated using a FIPS-approved method or equivalent international standard. Publicly trusted Issuing CAs shall generate cryptographic keying material on a FIPS 140-2 level 3 validated cryptographic module using multiple individuals acting in trusted roles. CA and RA key pair generation must create a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

Multi-party control is required for CA key pair generation, as specified in section 6.2.2.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the Subscriber, CA, or RA. If the CA or RA generates Subscriber key pairs, the requirements for key pair delivery specified in section 6.1.2 must also be met.

If Subscriber hardware tokens are required, then signature keys must be generated on the hardware token to support source authentication.

6.1.2 Private Key Delivery to Subscriber

Key delivery only applies when the CA or RA generates the key pairs on behalf of the Subscriber. In this case, the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- The CA/RA shall not retain any copy of the signing key after delivery of the private signing key to the Subscriber. NOTE: when key escrow is desired, the CA or RA may retain a copy of the subscriber encryption key for escrow purposes.
- The private key(s) must be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct keys and activation data are provided to the correct Subscribers.

The CA / RA must maintain a record of the Subscriber acknowledgment of receipt of the key.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are not generated by the CA, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the Subscriber's verified identity to the public key. The certificate request process shall ensure that the Applicant possesses the Private Key associated with the Public Key presented for certification. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of a Root CA shall be provided to relying parties in a secure manner so that it is not vulnerable to modification or substitution. The Issuing CA may deliver its CA Public Keys to Relying Parties as (i) specified in a certificate validation or path discovery policy file, (ii) trust anchors in commercial browsers and operating system root store, and/or (iii) roots signed by other CAs.

The Issuing CA may distribute Public Keys that are part of an updated signature key pair as a self-signed certificate, as a new CA certificate, or in a key roll-over certificate. When a CA updates its signature key pair, the key rollover certificates may be signed with the CA's current private key; in this case secure distribution is inherent.

All accreditation authorities supporting UAE National PKI certificates and all application software providers are permitted to redistribute any Root Certificate that is issued under this CP.

6.1.5 Key Sizes

This CP requires use of RSA, DSA, or ECDSA signatures. Certificates issued under this Policy shall contain RSA or elliptic curve public keys.

Publicly trusted Root CA certificates shall contain subject public keys of at least 4096 bits for RSA/DSA, at least 256 bits for elliptic curve, and be signed with the corresponding private key. For Private trust Root CA certificates, public keys of at least 2048 bits for RSA/DSA and at least 256 bits for elliptic curve are required, and must be signed by the corresponding private key. The Issuing CA may require higher bit keys in its sole discretion.

Signatures on all certificates shall be generated using at least SHA-1. Publicly trusted CAs that generate certificates and CRLs under this policy should use at least SHA-256 hash algorithm when generating digital signatures.

ECDSA signatures on certificates and CRLs shall be generated using at least SHA-256, as appropriate for the key length. CAs that issue certificates signed with SHA-256 or greater must not issue certificates signed with SHA-1.

RSA signatures on CRLs that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. For example, public key parameters for use with algorithms defined in the Digital Signature Standard [FIPS 186-2] shall be generated and tested in accordance with [FIPS 186-2].

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

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

Public keys that are bound into Level 3 or Level 4 user certificates shall be used only for signing or encrypting, but not both. Level 1 and Level 2 certificates may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates must:

1. be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP,
2. never assert the non-repudiation key usage bit, and
3. not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CAs shall use a [FIPS 140] Level 3 or higher validated hardware cryptographic module for signing operations. RAs shall use a [FIPS 140] validated hardware cryptographic module for signing operations in accordance with the following table. The minimum level required for ALL certificates will be equivalent to the minimum level required for the highest level of certificate supported. Subscriber requirements are also detailed in the following table:

Assurance Level	Subscriber	Registration Authority
EV Code Signing	FIPS 140 L2 Hardware	FIPS 140 L2 Hardware
Code Signing	FIPS 140 L2 Hardware	FIPS 140 L2 Hardware
Level 1 Subscriber Certificate	N/A	FIPS 140 L1 Software
Level 2 Subscriber Certificate	FIPS 140 L1 Software	FIPS 140 L1 Software
Level 3 Subscriber Certificate	FIPS 140 L1 Software	FIPS 140 L2 Hardware
Level 4 Subscriber Certificate	FIPS 140 L2 Hardware	FIPS 140 L2 Hardware

The Issuing CA shall maintain any Card Management Master Key and perform diversification operations in a FIPS 140-2 Level 3 Cryptographic Module that conforms to [NIST SP 800-78]. The Issuing CA shall also require that card management be configured such that only the authorized CMS can manage issued cards.

For EV Code Signing Certificates, the Issuing CA shall ensure that the Private Key is properly generated, stored, and used in a cryptomodule that meets or exceeds the requirements of FIPS 140 level 2.

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

The Issuing CA shall ensure that multiple trusted personnel are required to act in order to access and use the Issuing CA's Private Keys, including any Private Key backups. Access to CA signing keys backed up for disaster recovery shall be under multiple trusted personnel control. The names of the parties used for multi-party control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

CA private signature keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.12.1. If a device has a separate key management key certificate, the key management private key may be

escrowed. The private key associated with a certificate that asserts a digital Signature key usage shall not be escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multiparty control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. Backup procedures shall be included in the CA's CPS.

6.2.4.2 Backup of Subscribers Private Signature Key

The Issuing CA may backup Level 1, Level 2, and Level 3 subscriber private signature keys, provided that the backup copies are held in Subscriber's control. The Issuing CA may not backup Level 4 subscriber private signature keys. Any subscriber key management keys may be backed up by the CA or RA. Backed up Subscriber private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the Subscriber's cryptographic module.

6.2.5 Private Key Archival

CA private signature keys shall not be archived. CAs that retain Subscriber private encryption keys for business continuity purposes shall archive such Subscriber private keys in accordance with section 5.5.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All CA keys shall be generated by a cryptographic module. CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4.1. At no time shall the CA private key exist in plaintext outside the cryptographic module.

In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; transport and re-activation must be effected under multi-party controls; private keys must never exist in plaintext form outside the cryptographic module boundary.

6.2.7 Private Key Storage on Cryptographic Module

The private key stored in the cryptographic module shall be protected from unauthorized access and use in accordance with the FIPS 140 requirements applicable for the module. Publicly trusted CA private keys must only be generated and stored protected by a FIPS 140 Level 3 module.

6.2.8 Method of Activating Private Key

Pass-phrases, PINs, biometric data, or other mechanisms of equivalent authentication robustness must be used to activate the private key in a cryptographic module in accordance with the specifications of the cryptographic module manufacturer. Subscribers are solely responsible for protecting their Private Keys.

At a minimum, Subscribers must authenticate themselves to the cryptographic module before activating their private keys. Entry of activation data shall be protected from disclosure by reasonable means.

6.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated and stored in in secure containers.

6.2.10 Method of Destroying Private Key

The Issuing CA shall use individuals in trusted roles to destroy CA, RA, and status server Private Keys when they are no longer needed. Subscribers shall either surrender their cryptographic module to CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked.

For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a “zeroize” command. Physical destruction of hardware should not be required.

6.2.11 Cryptographic Module Rating

Refer to Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificates and associated keys have maximum validity periods as detailed in the following table:

Type	**Private Key Use**	**Certificate Term**
Root CA	20 years	25 years
Issuing CA	10 years	15 years
Cross-certified CA	6 years	15 years
CRL or OCSP Signer	3 years	31 days
EV SSL	No Stipulation	27 Months
OV SSL	No Stipulation	42 months

EV Code Signing (Subscriber)	No Stipulation	39 months
EV Code Signing (Signature Authority)	No Stipulation	123 months
Time Stamp Authority	No Stipulation	123 months
Code Signing	No Stipulation	123 months
Client key management	36 months	36 months
Client (all other purposes)	42 months	42 months
IGTF 2048 bit RSA on Hardware	60 months	13 months
IGTF non-hardware	13 months	13 months

IGTF Issuing CAs must have a lifetime that is at least twice the maximum lifetime of any end entity certificate it issues.

The Issuing CA shall not issue a Subscriber certificate with an expiration date that is past the signing root's expiration date or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CA activation data may be user-selected (by each of the multiple parties holding that activation data) and providing it has sufficient strength to protect its Private Keys. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

RA and Subscriber activation data may be user-selected. The strength of the activation data shall meet or exceed the requirements for authentication mechanisms stipulated for appropriate module required to protect those key as specified in section 6.2.1 of this CP. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be:

1. memorized
2. biometric in nature, or

3. recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

The Issuing CA shall require personnel to not share their passwords with other individuals. The Issuing CA shall implement processes to temporarily lock access to secure CA processes if a certain number of failed log-in attempts occur.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

CA security controls will be implemented in accordance with recognized security standards (e.g. UAE Information Assurance Standards) to protect its information and information assets.

6.5.1 Specific Computer Security Technical Requirements

Access to information such as sensitive details about customer accounts, passwords, and ultimately, CA-related private keys must be carefully guarded, along with the machines hosting such information.

The CA shall authenticate and protect all communications between a trusted role and its CA system.

Information system account management features shall ensure that users access only that functionality permitted by their role or function. All account types with access to information systems shall be documented along with the conditions and procedures to follow in creating new accounts. Groups and roles shall have a documented relationship to the business or mission roles involved in operating the CA.

The CA shall employ the principle of least privilege when creating users and assigning them to groups and roles; membership to a group or role is granted shall be justified based upon business need. The CA shall take appropriate action when a user no longer requires an account, their business role changes, or the user is terminated or transferred. Periodically, the CA shall review all active accounts to match active authorized users with accounts, and disable any accounts no longer associated with an active authorized user.

CA systems shall be configured, operated, and maintained so as to ensure the continuous logical separation of processes and their assigned resources.

The CA system shall employ malicious code protection mechanisms to mitigate the risk of malicious code on CA system components.

CA system components running standard operating systems that are not air-gapped from the Internet shall employ host-based anti-malware tools to detect and prevent the execution of known malicious code. These tools shall be configured to automatically scan removable media when it is inserted, as well as files received over the network. Introduction of removable media shall not cause automatic execution of any software residing on the media.

The CA shall protect the confidentiality and integrity of sensitive information stored or processed on CA systems that could lead to abuse or fraud. For example, the CA shall protect customer data that could

allow an attacker to impersonate a customer. The CA shall employ technical mechanisms to prevent unauthorized changes or accesses to this information, such as access control mechanisms that limit which users are authorized to view or modify files.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

For any software developed by the CA, evidence shall be produced relating to the use of a defined software development methodology setting out the various phases of development, as well as implementation techniques intended to avoid common errors to reduce the number of vulnerabilities. Automated software assurance (i.e. static code analysis) tools shall be used to catch common error conditions within developed code. For compiled code, all compiler warnings shall be enabled and addressed or acknowledged to be acceptable. Input validation shall be performed for all inputs into the system.

The CA system shall be implemented and tested in a non-production environment prior to implementation in a production environment. No change shall be made to the production environment unless the change has gone through the change control process as defined for the system baseline.

In order to prevent incorrect or improper changes to the CA system, the CA system shall require multi- party control for access to the CA system when changes are made.

All data input to CA system components from users or other system components shall be validated prior to consumption by the receiving entity. Validating the syntax and semantics of system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match the expected definitions for format and content.

6.6.2 Security Management Controls

A list of acceptable products and their versions for each individual CA system component shall be maintained and kept up-to-date within a configuration management system. Mechanisms and/or procedures shall be in operation designed to prevent the installation and execution of unauthorized software. A signed whitelist of the acceptable software for the system should be one of the ways to control the allowed software. A CA system shall have automated mechanisms to inventory on at least a daily basis software installed on a system and alert operators if invalid software is found.

The CA system shall establish and document mandatory configuration settings for all information technology components which comprise the CA system. For CA operations, hardware and software used must only be dedicated to performing the CA functions. Hardware and software purchased and shipped for CA operations is done in a fashion that reduces the likelihood of tampering.

6.6.3 Life Cycle Security Controls

The CA shall scan all CA systems for vulnerabilities using at least one vulnerability scanner at least once every month. The use of multiple scanners on the most sensitive systems is strongly encouraged.

Each vulnerability found shall be entered into a vulnerability tracking database, along with the date and time of location, and shall be remediated within 72 hours. Remediation shall be entered into the vulnerability database as well (including date and time).

In addition, the CA shall monitor relevant notification channels on a daily basis for updates to packages installed on CA systems (including networking hardware). CAs shall have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption.

6.7 Network Security Controls

CAs and RAs shall employ appropriate security measures to ensure their systems are guarded against denial of service and intrusion attacks. Such measures shall include the use of hardware firewalls, hardware filtering routers, and intrusion detection systems. Unused network ports and services shall be turned off. For CAs, protocols that provide network security attack vector(s) shall not be permitted through the boundary control devices.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Time-Stamping

Issuing CAs shall ensure that the accuracy of clocks used for time-stamping are within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

The CA shall issue X.509 v3 certificates (populate version field with integer “2”).

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. IGTF certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

7.1.3 Algorithm Object Identifiers

The CA shall issue certificates using the following OIDs for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
id-RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) 1 }
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4 }

If an Issuing CA signs certificates using RSA with PSS padding, the Issuing CA may use an RSA signature with PSS padding with the following algorithms and OIDs:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

The CA shall issue certificates using the following OIDs to identify the algorithm associated with the subject key:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public key-type (2) 1}
id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)}
id-keyExchangeAlgorithm	[joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22]
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}

7.1.4 Name Forms

The subject field in certificates issued under this policy shall be populated with an X.500 distinguished name. The Issuing CA shall restrict OU fields from containing Subscriber information that is not verified in accordance with Section 3.

7.1.5 Name Constraints

The CAs may assert name constraints in CA certificates using the nameConstraints extension.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP are entitled to assert the following OID(s):

<id-policy-defined-in-this-document>::=<OID>

Other OIDs as defined in section 1.2 are also permissible where appropriate.

7.1.7 Usage of Policy Constraints Extension

The CAs may assert policy constraints in CA certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued under this policy shall not contain a critical certificate policies extension.

7.2 CRL Profile

7.2.1 Version Number(s)

The CA shall issue X.509 version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension shall be specified when they are used.

7.3 OCSP Profile

7.3.1 Version Number(s)

The CA OCSP responders shall use OCSP version 1.

7.3.2 OCSP Extensions

Critical OCSP extensions shall not be used.

8 Compliance Audit and Other Assessments

The policies in this CP are designed to meet or exceed the requirements of generally accepted industry standards for PKIs, including the EV Guidelines and the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79/ISO 21188 PKI Practices and Policy Framework ("CA WebTrust/ISO 21188"). CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CPS meet the CP requirements and these are being implemented and enforced. This specification does not impose a requirement for any particular assessment methodology.

8.1 Frequency or Circumstances of Assessment

On at least an annual basis, Issuing CAs shall retain an independent auditor who shall assess the Issuing CA's compliance with this CP and its CPS. This audit must cover CMSs, Sub CAs, RAs, and each status server that is specified in a certificate issued by the Issuing CA. Any independent entity interoperating within the UAE National PKI shall submit its practices statement and the results of its compliance audit to the TRA on an annual basis for review and approval.

8.2 Identity/Qualifications of Assessor

The Issuing CA shall use an auditor that meets the following qualifications:

1. *Qualifications and experience*: Auditing must be the auditor's primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential.
2. *Expertise*: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with Public Key infrastructures, certification systems, and Internet security issues.
3. *Rules and standards*: The auditor must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.
4. *Reputation*: The firm must have a reputation for conducting its auditing business competently and correctly.
5. *Insurance*: EV auditors must maintain Professional Liability/Errors and Omissions Insurance, with policy limits of at least $1 million in coverage.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor either shall be a private firm that is independent from the entities (CA and RAs) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. To insure independence and objectivity, the compliance auditor should not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the Issuing CA. Under no circumstances shall a CA provider be audited for compliance by any subsidiary, parent, or sibling company of its corporate holdings.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a CA and its recognized RAs comply with all the requirements of the current versions of this CP and the CA's CPS and any relevant RPSs. All aspects of the CA/RA operation shall be subject to compliance audit inspections.

8.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS/RPS and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The auditor will document the discrepancy,
- The auditor will promptly notify the CA and the TRA; and
- The CA/RA will develop a plan to treat the noncompliance.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Controller of Certification Authorities via the TRA may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The TRA of the Controller of Certification Authorities will develop procedures for making and implementing such determinations.

8.6 Communication of Results

The compliance auditor shall report the results of a CA/RA compliance audit to the TRA and/or the Controller of Certification Authorities. The results will be reported to the audited CA/RA, and its superior CA if applicable. The implementation of remedies shall be communicated to the TRA of the Controller of Certification Authorities.

8.7 Self Audits

The Issuing CA shall perform regular internal audits of its operations, personnel, and compliance with this CP using a randomly selected sample of certificates issued since the last internal audit. The Issuing CA shall self-audit at least three percent of non-EV SSL Certificates and six percent of EV SSL Certificates.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Issuing CAs may charge fees for certificate issuance and renewal.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

This CP contains no limits on the use of certificates issued by CAs under the policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

The CA shall protect the confidentiality of sensitive business information (e.g. customer data) stored or processed on CA systems that could lead to abuse or fraud.

CA information not requiring protection may be made publicly available. Public access to organizational information shall be determined by the respective organization.

9.3.1 Scope of Confidential Information

Issuing CAs shall specify what constitutes confidential information in its CPS.

9.3.2 Information Not Within the Scope of Confidential Information

Issuing CAs may treat any information not listed as confidential in the CPS as public information.

9.3.3 Responsibility to Protect Confidential Information

Issuing CAs shall contractually obligate employees, agents, and contractors to protect confidential information. Issuing CAs shall provide training to employees on how to handle confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The CA shall develop, implement and maintain a privacy plan.

The privacy plan shall document what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed.

9.4.2 Information Treated as Private

CAs shall protect all Subscriber personally identifiable information (PII) from unauthorized disclosure. Personal information about an individual that is not publicly available or in the contents of a certificate or CRL is considered private information. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents.

9.4.3 Information not Deemed Private

Information included in certificates or their validity status information is not subject to protections outlined in section 9.4.2.

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in section 9.4.

9.4.5 Notice and Consent to Use Private Information

Subscribers must consent to the global transfer and publication of any personal data contained in Certificates.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CA shall not disclose private information to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

None.

9.5 Intellectual Property Rights

The CA will not knowingly violate intellectual property rights held by others.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CAs operating under this Policy shall warrant that their procedures are implemented in accordance with this CP, and that any certificates issued under this CP are in accordance with the stipulations of this Policy.

9.6.2 RA Representations and Warranties

An RA that performs registration functions as described in this policy shall comply with the stipulations of this Policy, and comply with a CPS or RPS approved by the TRA or the Controller of Certification Authorities for use with this Policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

9.6.3 Subscriber Representations and Warranties

Each Subscriber shall represent to the Issuing CA that the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise (including protecting any tokens or corresponding activation data that provides access to Private Keys),
2. Provide accurate and complete information and communication to the Issuing CA and RA or their agent,
3. Confirm the accuracy of certificate data prior to using the certificate,
4. Promptly cease using a certificate and notify the Issuing CA if (i) any information that was submitted to the Issuing CA 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, and
5. Use the certificate only for authorized and legal purposes, consistent with the relevant CPS and Subscriber Agreement, including only installing SSL certificates on servers accessible at the domain listed in the certificate and not using code signing certificates to sign malicious code or any code that is downloaded without a user's consent.

9.6.4 Relying Party Representations and Warranties

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. It is however that recommended that relying party applications honor key usages contained in certificates and validate unexpired certificates with the Issuing CA or a published validation authority prior accepting their usage.

9.6.5 Representations and Warranties of Other Participants

None.

9.7 Disclaimers of Warranties

CAs operating under this policy may not disclaim any responsibilities described in this CP.

9.8 Limitations of Liability

Issuing CAs may limit their liability to any extent not otherwise prohibited by this CP, provided that the Issuing CA remains responsible for complying with this CP and the Issuing CA's CPS.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CP and any amendments are effective when published to the CA's online repository and remain in effect until replaced with a newer version.

9.10.2 Termination

The CP shall document under what conditions the CP may be terminated.

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued. Any termination communication will specify which provisions survive termination. At a minimum, responsibilities related to protecting confidential information will survive termination.

9.11 Individual Notices and Communications with Participants

The TRA shall establish appropriate procedures for communications with CAs operating under this policy via contracts or memoranda of agreement as applicable. Digitally signed or paper notices related to this CP that are addressed to the locations specified in Section 2.2 of this CP are acceptable. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from the CA or its agent. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested.

For all other communications, no stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The TRA shall review this CP at least once every year. If the TRA or the Controller of Certification Authorities determines modifications to this CP are required, the change will be communicated. Amendments are made by posting an updated version of the CP to the online repository. Controls are in place to reasonably ensure that this CP is not amended and published without the prior authorization of the TRA or the Controller of Certification Authorities.

9.12.2 Notification Mechanism and Period

The updated CP and any subsequent changes shall be made publicly available. Issuing CAs may make non-material changes to their CPSs without notice to the TRA if the non-material change does not require changing this CP.

9.12.3 Circumstances Under Which OID Must be Changed

If the TRA or the Controller of Certification Authorities determines that there is a requirement to change the OIDs, the TRA will amend the appropriate documents.

9.13 Dispute Resolution Provisions

The TRA shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this Policy.

9.14 Governing Law

The construction, validity, performance and effect of certificates issued under this CP for all purposes are governed by UAE law.

9.15 Compliance with Applicable Law

All CAs operating under this policy are required to comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Issuing CAs shall contractually obligate each RA involved in Certificate issuance to comply with this CP and applicable industry guidelines. Issuing CAs shall contractually obligate parties using products and services issued under this CP, such as Subscribers and Relying Parties, to the relevant provisions herein. This CP does not give any third party rights under such agreements.

9.16.2 Assignment

Entities operating under this CP may not assign their rights or obligations without the prior written consent of the TRA or the Controller of Certification Authorities.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The CA is not liable for a delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by an occurrence beyond it's reasonable control. The operation of the Internet is beyond the CA's reasonable control.

9.17 Other Provisions

No stipulation.

Annex A: Acronyms

Acronyms	Definition
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
FIPS PUB	Federal Information Processing Standards Publication
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
TRA	Telecommunication Regulatory Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RPS	Registration Practices Statement
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
UPS	Uninterrupted Power Supply
VPN	Virtual Private Network

Annex B: Definitions

Term	Meaning
Anonymous	Having an unknown name
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.
Archive	Long-term, physically separate storage
Asset	Anything that has value to the organization such as software, information, documentation etc.
Audit	An independent review of event logs and related activities performed to determine the adequacy of current security measures, to identify the degree of conformance with established policy or to develop recommendations for improvements to the security measures currently applied
Authentication	Verifying the identity of an entity when that identity is presented
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication
Availability	The property of being accessible and usable upon demand by an authorized entity
Backup	Copy of files and programs made to facilitate recovery if necessary
Biometric	A physical or behavioral characteristic of a human being
Certificate	A digital representation of information which at least identifies the certification authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certification authority issuing it
Certificate Revocation List	A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date
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
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature Note: Control is also used as a synonym for safeguard or countermeasure
Cryptographic Module	A related set of hardware or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates
Cyber Security	Security measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means
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: whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and whether the message has been altered since the transformation was made
Firewall	A network protection device that filters incoming and outgoing network data, based on a series of rules
Guideline	A description that clarifies what should be done and how, to achieve the objectives

	set out in policies
Hardware	A generic term for any physical component of information and communication technology
Information Asset	An Information Asset is a definable piece of information, stored in any manner which is recognized as valuable to the organization. In general, information assets have recognizable and manageable value, risk, content and lifecycles.
Information Assurance	Practice of protecting information and managing risks related to the use, processing, storage and transmission of information or data, and the systems and processes used for those purposes
Information Security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Integrity	The property of safeguarding the accuracy and completeness of assets
Intrusion Detection System (IDS)	A security device, resident on a specific host, which monitors system activities for malicious or unwanted behavior
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
Key Management	The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction
Key Pair	Two mathematically related keys having the properties that one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and even knowing the public key, it is computationally infeasible to discover the private key
Malicious Code or Malware	Any software that attempts to subvert the confidentiality, integrity or availability of a system. Types of malicious code include logic bombs, trapdoors, Trojans, viruses and worms
Media	A generic term for hardware that is used to store information
Network Device	Any device designed to facilitate the communication of information destined for multiple system users. For example: cryptographic devices, firewalls, routers, switches and hubs
Non-Repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
Online Certificate Status Protocol	Protocol which provides on-line status information for certificates

Policy	Overall intention and direction as formally expressed by management
Pseudonym	A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing
Regulator	A government body that sets regulations and monitors compliance and behavior of regulated entities in a particular sector (or market)
Re-key	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
Remote Access	Access to a system from a location not under the physical control of the system owner
Repository	A database containing information and data relating to certificates
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time
Third party	That person or body that is recognized as being independent of the parties involved, as concerns the issue in question
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.

Annex C: Public Trust Partnerships

The UAE National PKI may use additional policy OIDs when issuing certificates to indicate their compliance with corresponding alternate policies. The set of policies that certificates may additionally include are detailed here below. This is intended to be a definitive list of the policies that may be included but the TRA reserves the right to amend this list as needed.

Object Description	**Object Identifier (OID)**	**Reference**
CAB Forum Extended Validation	2.23.140.1.1	https://cabforum.org/extended-validation/
CAB Forum Organizational Validation	2.23.140.1.2.2	https://cabforum.org/baseline-requirements-documents/
QuoVadis Extended Validation	1.3.6.1.4.1.8024.0.2.100.1.2	https://ca.darkmatter.ae/iCPS
QuoVadis Adobe Acrobat Trust List	1.3.6.1.4.1.8024.1.300	https://ca.darkmatter.ae/iCPS