



# Dubai Electronic Security Center

## Dubai PKI

### Timestamping CA Certification Practice Statement

**Project** DESC CA Project

**Title** Timestamping CA Certification Practice Statement

**Classification** PUBLIC

**File Name** DubaiPKI- TimestampingCA-CertificationPracticeStatement\_v1.6

**Created on** 15 Mar 2022

**Revision** 1.6

**Modified on** 27 February 2025

# Document History

Date	Revision	Author(s)	Summary
15 Mar 2022	0.1	Khawla Hassan	Initial version
1 <sup>st</sup> April 2022	1.0	Khawla Hassan	First Release
1 <sup>st</sup> June 2022	1.1	Khawla Hassan	Update section 4.1.2 to align with the technology in use
7 September 2022	1.2	Khawla Hassan	Correct typographical errors and general enhancements
6 April 2023	1.3	Khawla Hassan	<ul style="list-style-type: none"><li>• Annual review</li><li>• Add more options of identity vetting as per the CS BRs</li><li>• Align the definitions and log retention with the SSL BRs</li></ul>
2 November 2023	1.4	Khawla Hassan	<ul style="list-style-type: none"><li>• Update the certificates supported under the Devices CA in the PKI hierarchy</li><li>• Updates to accommodate the CA/B Forum ballots CSCWG-19</li></ul>
08 April 2024	1.5	Khawla Hassan	Annual review
27 February 2025	1.6	Mohamed Khalifa	<ul style="list-style-type: none"><li>• Annual review</li><li>• Updates to reflect CA migration to offline state</li></ul>

## Table of Contents

Document History .....	2
<b>1. Introduction.....</b>	<b>11</b>
<b>1.1 Overview .....</b>	<b>11</b>
1.1.1 Dubai PKI Hierarchy .....	12
1.1.2 Dubai PKI Policy Authority (PA) .....	12
1.1.3 Certificate Policy .....	13
1.1.4 Relationship Between the DESC Subordinate CAs CP and this CPS.....	13
<b>1.2 Document Name and Identification.....</b>	<b>14</b>
<b>1.3 PKI Participants.....</b>	<b>14</b>
1.3.1 Certification Authorities .....	14
1.3.2 Registration Authorities .....	15
1.3.3 Subscribers .....	15
1.3.4 Relying Parties .....	15
1.3.5 Other Participants .....	15
<b>1.4 Certificate Usage .....</b>	<b>15</b>
1.4.1 Appropriate Certificate Use .....	15
1.4.2 Prohibited Certificate Use .....	15
<b>1.5 Policy Administration .....</b>	<b>16</b>
1.5.1 Organization Administering the Document .....	16
1.5.2 Contact Person.....	16
1.5.3 Person Determining CPS Suitability for the Policy .....	16
1.5.4 CPS Approval Procedures .....	16
<b>1.6 Definitions, Acronyms and References .....</b>	<b>16</b>
1.6.1 Definitions .....	16
1.6.2 Acronyms .....	21
<b>2. Publication and Repository Responsibility.....</b>	<b>23</b>
<b>2.1 Repositories.....</b>	<b>23</b>
<b>2.2 Publication of Certificate Information.....</b>	<b>23</b>
<b>2.3 Time or Frequency of Publication Repositories.....</b>	<b>23</b>
2.3.1 Certificates .....	23
2.3.2 CRLs.....	24
<b>2.4 Access Controls on Repositories .....</b>	<b>24</b>
<b>3. Identification and Authentication .....</b>	<b>25</b>
<b>3.1 Naming .....</b>	<b>25</b>
3.1.1 Types of Names.....	25
3.1.2 Need for names to be meaningful.....	25

**Certificate Practice Statement**

3.1.3	Anonymity and Pseudonymity of Subscribers .....	25
3.1.4	Rules for Interpreting Various Name Forms .....	25
3.1.5	Uniqueness of Names .....	26
3.1.6	Recognition, Authentication and Role of Trademarks .....	26
<b>3.2</b>	<b>Initial Identity Validation.....</b>	<b>26</b>
3.2.1	Method to Prove Possession of Private Key .....	26
3.2.2	Authentication of Organization and Domain Identity .....	26
3.2.3	Authentication of Individual Identity .....	27
3.2.4	Non-Verified Subscriber Information .....	27
3.2.5	Validation of Authority .....	27
3.2.6	Criteria for Interoperation .....	27
<b>3.3</b>	<b>Identification and Authentication for Re-keying Requests.....</b>	<b>28</b>
3.3.1	Identification and Authentication for Routine Re-Keying .....	28
3.3.2	Identification and Authentication for Re-Key After Revocation .....	28
<b>3.4</b>	<b>Identification and Authentication for Revocation Requests .....</b>	<b>28</b>
<b>4.</b>	<b>Certificate Life Cycle Management .....</b>	<b>29</b>
<b>4.1</b>	<b>Certificate Application .....</b>	<b>29</b>
4.1.1	Who can Submit a Certificate Application .....	29
4.1.2	Enrolment Process and Responsibilities .....	29
4.1.3	Identification and Authentication for Routine Re-Keying .....	30
<b>4.2</b>	<b>Certificate Application Processing .....</b>	<b>30</b>
4.2.1	Performing Identification and Authentication Functions .....	30
4.2.2	Approval or Rejection of Certificate Applications .....	31
4.2.3	Time to Process Certificate Applications .....	31
<b>4.3</b>	<b>Certificate Issuance .....</b>	<b>31</b>
4.3.1	CA Actions During Certificate Issuance .....	31
4.3.2	Notification to Subscriber by the CA of Issuance of Certificate.....	31
<b>4.4</b>	<b>Certificate Acceptance .....</b>	<b>31</b>
4.4.1	Conduct Constituting Certificate Acceptance .....	31
4.4.2	Publication of the Certificate by the CA .....	32
4.4.3	Notification of Certificate Issuance by the CA to Other Entities.....	32
<b>4.5</b>	<b>Key Pair and Certificate Usage.....</b>	<b>32</b>
4.5.1	Subscriber Private Key and Certificate Usage .....	32
4.5.2	Relying Party Public Key and Certificate Usage .....	32
<b>4.6</b>	<b>Certificate Renewal.....</b>	<b>32</b>
4.6.1	Circumstance for certificate renewal.....	33
4.6.2	Who may request renewal .....	33
4.6.3	Processing certificate renewal requests .....	33
4.6.4	Notification of new certificate issuance to subscriber .....	33
4.6.5	Conduct constituting acceptance of a renewal certificate .....	33

**Certificate Practice Statement**

4.6.6	Publication of the renewal certificate by the CA .....	33
4.6.7	Notification of certificate issuance by the CA to other entities .....	33
<b>4.7</b>	<b>Certificate Re-Key.....</b>	<b>33</b>
4.7.1	Circumstance for Certificate Re-key .....	33
4.7.2	Who May Request Certification of a New Public Key .....	33
4.7.3	Processing Certificate Re-Keying Requests.....	33
4.7.4	Notification of New Certificate Issuance to Subscriber.....	34
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate.....	34
4.7.6	Publication of the Re-keyed Certificate by the CA.....	34
4.7.7	Notification of Certificate Issuance by the CA to Other Entities.....	34
<b>4.8</b>	<b>Certificate Modification .....</b>	<b>34</b>
4.8.1	Circumstance for certificate modification.....	34
4.8.2	Who may request certificate modification .....	34
4.8.3	Processing certificate modification requests .....	34
4.8.4	Notification of new certificate issuance to subscriber .....	34
4.8.5	Conduct constituting acceptance of modified certificate .....	34
4.8.6	Publication of the modified certificate by the CA.....	34
4.8.7	Notification of certificate issuance by the CA to other entities .....	34
<b>4.9</b>	<b>Certificate Revocation and Suspension.....</b>	<b>34</b>
4.9.1	Circumstances for Revocation .....	35
4.9.2	Who can Request Revocation .....	35
4.9.3	Procedure for Revocation Request.....	36
4.9.4	Revocation Request Grace Period.....	36
4.9.5	Revocation Request Response Time .....	36
4.9.6	Revocation Checking Requirement for Relying Parties .....	37
4.9.7	CRL Issuance Frequency .....	37
4.9.8	Maximum Latency for CRLs .....	37
4.9.9	Online Revocation/Status Checking Availability .....	37
4.9.10	Online Revocation Checking Requirements .....	37
4.9.11	Other Forms of Revocation Advertisements Available .....	37
4.9.12	Special Requirements — Key Compromise.....	38
4.9.13	Circumstances for Suspension .....	38
4.9.14	Who Can Request Suspension.....	38
4.9.15	Procedure for Suspension Request.....	38
4.9.16	Limits on Suspension Period.....	38
<b>4.10</b>	<b>Certificate Status Services.....</b>	<b>38</b>
4.10.1	Operational Characteristics .....	38
4.10.2	Service Availability.....	39
4.10.3	Optional Features .....	39
<b>4.11</b>	<b>End of Subscription .....</b>	<b>39</b>
<b>4.12</b>	<b>Key Escrow and Recovery.....</b>	<b>39</b>

**Certificate Practice Statement**

4.12.1	Key Escrow and Recovery Policy and Practices.....	39
4.12.2	Session Key Encapsulation and Recovery Policy and Practices.....	39
<b>5.</b>	<b>Facility, Management and Operational Controls .....</b>	<b>40</b>
<b>5.1</b>	<b>Physical Controls.....</b>	<b>40</b>
5.1.1	Site Location and Construction .....	40
5.1.2	Physical Access .....	40
5.1.3	Power and air conditioning .....	40
5.1.4	Water Exposures .....	40
5.1.5	Fire Prevention and Protection .....	41
5.1.6	Media Storage .....	41
5.1.7	Waste Disposal.....	41
5.1.8	Offsite Backup.....	41
<b>5.2</b>	<b>Procedural Controls.....</b>	<b>41</b>
5.2.1	Trusted Roles.....	41
5.2.2	Number of Persons Required per Task .....	42
5.2.3	Identification and Authentication for Each Role.....	42
5.2.4	Roles Requiring Separation of Duties .....	42
<b>5.3</b>	<b>Personnel Controls .....</b>	<b>42</b>
5.3.1	Qualifications Experience and Clearance Requirements .....	42
5.3.2	Background Check Procedures .....	43
5.3.3	Training Requirements .....	43
5.3.4	Retraining Frequency and Requirements .....	43
5.3.5	Job Rotation Frequency and Sequence.....	43
5.3.6	Sanctions for Unauthorized Actions .....	43
5.3.7	Independent Contractor Requirements.....	43
5.3.8	Documentation Supplied to Personnel .....	44
<b>5.4</b>	<b>Audit Logging Procedures.....</b>	<b>44</b>
5.4.1	Types of Event Recorded .....	44
5.4.2	Frequency of Processing Log.....	45
5.4.3	Retention Period for Audit Log.....	46
5.4.4	Protection of Audit Log.....	46
5.4.5	Audit Log Backup Procedures .....	46
5.4.6	Audit Collection System (Internal vs. External) .....	46
5.4.7	Notification to Event-Causing Subject.....	47
5.4.8	Vulnerability Assessments .....	47
<b>5.5</b>	<b>Records Archival.....</b>	<b>47</b>
5.5.1	Types of Records Archived.....	47
5.5.2	Retention Period for Archive .....	47
5.5.3	Protection of Archive .....	47
5.5.4	Archive Backup Procedures .....	47
5.5.5	Requirements for Time stamping of Records .....	48

**Certificate Practice Statement**

5.5.6	Archive Collection System (Internal or External).....	48
5.5.7	Procedures to Obtain and Verify Archive Information .....	48
<b>5.6</b>	<b>Key Changeover .....</b>	<b>48</b>
<b>5.7</b>	<b>Compromise and Disaster Recovery .....</b>	<b>48</b>
5.7.1	Incident and Compromise Handling Procedures.....	48
5.7.2	Computing Resources, Software Data Corruption.....	48
5.7.3	Entity Private Key Compromise Procedures.....	49
5.7.4	Business Continuity Capabilities After a Disaster .....	49
<b>5.8</b>	<b>CA or RA Termination.....</b>	<b>49</b>
<b>6.</b>	<b>Technical Security Controls.....</b>	<b>51</b>
<b>6.1</b>	<b>Key Pair Generation .....</b>	<b>51</b>
6.1.1	Key Pair Generation .....	51
6.1.2	Private Key Delivery to Subscriber.....	52
6.1.3	Public Key Delivery to Certificate Issuer .....	52
6.1.4	CA Public Key Delivery to Relying Parties.....	52
6.1.5	Key Sizes.....	52
6.1.6	Public Key Parameters Generation and Quality Checking .....	52
6.1.7	Key Usage Purposes (As per X.509 v3 Key Usage Field).....	53
<b>6.2</b>	<b>Private Key Protection and Cryptographic Module Engineering Controls.....</b>	<b>53</b>
6.2.1	Cryptographic Module Standards and Controls .....	53
6.2.2	Private key (n out of m) multi-person control.....	53
6.2.3	Private Key Escrow .....	54
6.2.4	Private Key Backup.....	54
6.2.5	Private Key Archival.....	54
6.2.6	Private Key Transfer Into or From a Cryptographic Module.....	54
6.2.7	Private Key Storage on Cryptographic Module .....	54
6.2.8	Method of Activating Private Key .....	54
6.2.9	Method of Deactivating Private Key.....	54
6.2.10	Method of Destroying Private Key .....	55
6.2.11	Cryptographic Module Rating.....	55
<b>6.3</b>	<b>Other Aspects of Key Pair Management .....</b>	<b>55</b>
6.3.1	Public Key Archival .....	55
6.3.2	Certificate Operational Periods and Key Pair Usage Periods .....	56
<b>6.4</b>	<b>Activation Data.....</b>	<b>56</b>
6.4.1	Activation Data Generation and Installation .....	56
6.4.2	Activation Data Protection .....	56
6.4.3	Other Aspects of Activation Data .....	56
<b>6.5</b>	<b>Computer Security Controls .....</b>	<b>57</b>
6.5.1	Specific Computer Security Technical Requirements .....	57
6.5.2	Computer Security Rating.....	57

**Certificate Practice Statement**

<b>6.6 Life Cycle Technical Controls</b> .....	<b>57</b>
6.6.1 System Development Controls.....	57
6.6.2 Security Management Controls.....	57
6.6.3 Life Cycle Security Controls.....	58
<b>6.7 Network Security Controls</b> .....	<b>58</b>
<b>6.8 Time Stamping</b> .....	<b>58</b>
<b>7. Certificate, CRL and OCSP Profiles</b> .....	<b>59</b>
<b>7.1 Certificate Profile</b> .....	<b>59</b>
7.1.1 Version Number .....	59
7.1.2 Certificate Extensions .....	59
7.1.3 Algorithm Object Identifiers .....	59
7.1.4 Name Forms .....	59
7.1.5 Name Constraints .....	59
7.1.6 Certificate Policy Object Identifier .....	59
7.1.7 Usage of Policy Constraints Extension .....	60
7.1.8 Policy Qualifiers Syntax and Semantics .....	60
7.1.9 Processing Semantics for Critical Certificate Extensions .....	60
7.1.10 Timestamping Certificate Profile .....	60
<b>7.2 CRL Profile</b> .....	<b>63</b>
7.2.1 Version Number(s).....	63
7.2.2 CRL and CRL Entry Extensions .....	63
7.2.3 CRL ASN1 Description .....	63
<b>7.3 OCSP Profile</b> .....	<b>65</b>
7.3.1 Version Number(s).....	65
7.3.2 OCSP Extensions .....	65
7.3.3 OCSP Response Signing Certificate ASN1 Description.....	65
<b>8. Compliance Audit and Other Assessments</b> .....	<b>69</b>
<b>8.1 Frequency or Circumstances of Assessment</b> .....	<b>69</b>
<b>8.2 Identity and Qualifications of the Assessor</b> .....	<b>69</b>
<b>8.3 Assessor’s Relationship to Assessed Party</b> .....	<b>69</b>
<b>8.4 Topics Covered by Assessment</b> .....	<b>70</b>
<b>8.5 Actions Taken as a Result of Deficiency</b> .....	<b>70</b>
<b>8.6 Communication of Results</b> .....	<b>70</b>
<b>9. Other Business and Legal Matters</b> .....	<b>71</b>
<b>9.1 Fees</b> .....	<b>71</b>
9.1.1 Certificate Issuance or Renewal Fees.....	71
9.1.2 Certificate Access Fees .....	71
9.1.3 Revocation or Status Information Access Fees.....	71
9.1.4 Fees for Other Service.....	71



**Certificate Practice Statement**

9.1.5	Refund Policy .....	71
<b>9.2</b>	<b>Financial Responsibility .....</b>	<b>71</b>
9.2.1	Insurance Coverage .....	71
9.2.2	Other Assets .....	71
9.2.3	Insurance or Warranty Coverage for End-Entities .....	71
<b>9.3</b>	<b>Confidentiality of Business Information .....</b>	<b>72</b>
9.3.1	Scope of Confidential Information .....	72
9.3.2	Information not within the scope of confidential information .....	72
9.3.3	Responsibility to protect confidential information .....	72
<b>9.4</b>	<b>Privacy of Personal Information .....</b>	<b>72</b>
9.4.1	Privacy plan .....	72
9.4.2	Information treated as Private .....	73
9.4.3	Information not Deemed Private .....	73
9.4.4	Responsibility to protect private information .....	73
<b>9.5</b>	<b>Intellectual Property Rights .....</b>	<b>73</b>
<b>9.6</b>	<b>Representations and Warranties .....</b>	<b>73</b>
9.6.1	CA Representations and Warranties .....	73
9.6.2	RA Representations and Warranties .....	74
9.6.3	Subscriber Representations and Warranties .....	74
9.6.4	Relying Party Representations and Warranties .....	75
9.6.5	Representations and Warranties of Other Participants .....	76
<b>9.7</b>	<b>Disclaimers of Warranties .....</b>	<b>76</b>
<b>9.8</b>	<b>Limitations of Liability .....</b>	<b>76</b>
<b>9.9</b>	<b>Indemnities .....</b>	<b>76</b>
<b>9.10</b>	<b>Term and Termination .....</b>	<b>76</b>
9.10.1	Term .....	76
9.10.2	Termination .....	76
9.10.3	Effect of Termination and Survival .....	77
<b>9.11</b>	<b>Individual Notices and Communications with Participants .....</b>	<b>77</b>
<b>9.12</b>	<b>Amendments .....</b>	<b>77</b>
9.12.1	Procedure for Amendment .....	77
9.12.2	Notification Mechanism and Period .....	77
9.12.3	Circumstances Under Which OID Must be Changed .....	77
<b>9.13</b>	<b>Dispute Resolution Procedures .....</b>	<b>77</b>
<b>9.14</b>	<b>Governing Law .....</b>	<b>77</b>
<b>9.15</b>	<b>Compliance with Applicable Law .....</b>	<b>77</b>
<b>9.16</b>	<b>Miscellaneous Provisions .....</b>	<b>78</b>
9.16.1	Entire Agreement .....	78
9.16.2	Assignment .....	78

**Certificate Practice Statement**

9.16.3	Severability.....	78
9.16.4	Enforcement (Attorney Fees/Waiver of Rights) .....	78
9.16.5	Force Majeure .....	78
<b>9.17</b>	<b>Other Provisions.....</b>	<b>78</b>

# 1. Introduction

This Certification Practice Statement (CPS) describes the certification practices that apply to the digital certificates issued by the Dubai PKI Timestamping Certification Authority (CA). The Timestamping CA is one of the subordinate CAs signed by the Dubai Root CA. This CPS complies with DESC Subordinate CAs Certificate Policy that applies to the provision of certification services offered by DESC through its Subordinate CAs (Issuing CAs).

This CPS covers the issuance and controls surrounding the following types of certificates issued by the Timestamping CA:

- **Certificates Issued for Timestamping Authority (TSA)** — A certificate issued to a Timestamp Authority to use to timestamp data,
- **OCSP Certificates** — Certificates for the DESC Online Certificate Status Protocol (OCSP) responder to sign OCSP responses related to certificates issued by this CA.

This CPS meets the formal requirements of Internet Engineering Task Force (IETF) [RFC 3647] regarding content, format and content. While certain clause titles are included according to the structure of [RFC 3647], the topic may not necessarily apply in the implementation of the Timestamping CA, such sections state “No stipulation”. Additional information is presented in subsections of the standard structure where required.

This CPS aims to comply with the below requirements published at <https://www.cpacanada.ca>:

- WebTrust Principles and Criteria for Certification Authorities - Network Security
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements

The Dubai PKI is committed to maintain this CPS in conformance with the current versions of the below requirements published at <http://www.cabforum.org>:

- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for Code Signing (“Baseline Requirements for Code Signing”)

If there is any inconsistency between this document and the requirements above, the above requirements take precedence over this document.

Further information about this document and the Timestamping CA can be obtained from the Dubai PKI Policy Authority (PA), which is representing the policy and governing body for the Dubai PKI including DESC Subordinate CAs. Contact information of the Dubai PKI PA is provided under section 1.5.

## 1.1 Overview

The “Dubai PKI” uses standard PKI technologies, policies and operating procedures and application interfaces. The Dubai PKI comprises the Dubai PKI Root CA that is the trust anchor of this PKI, which comes at the first level of the PKI hierarchy. The Dubai PKI also comprises currently multiple Subordinate Certification Authorities (CAs): Corporate CA, Code Signing CA, Timestamping CA (hereinafter, DESC Subordinate CAs), which come at the second level of the PKI hierarchy. DESC owns and operates the Dubai PKI Root and the aforementioned Subordinate CAs to provide

*Dubai PKI - Timestamping CA*  
**Certificate Practice Statement**

certification services that enable individuals and government entities in the UAE to conduct secure electronic transactions; this includes securing the machine-to-machine communication where Devices can transact securely, leveraging the PKI signing and encryption capabilities.

Additionally, the Dubai PKI Root CA aims to sign subordinate CAs belonging to government or private sector entities. Such entities have their own custom needs and reasons to implement their own CAs rather than using a DESC Subordinate CAs.

CAs belonging to other entities come at the second level of the Dubai PKI hierarchy, being signed by the Dubai PKI Root CA. These issuing CAs will be directly signed by the Dubai PKI Root CA, which makes them subordinate CAs owned by the corresponding government or private sector entity but operated by DESC. Policies and procedures of these Subordinate CAs must follow and be in full compliance with Dubai PKI Root CA CP/CPS.

The Dubai PKI Root CA and DESC Subordinate CAs are established and operated by DESC. DESC is the authority that has the final responsibility of providing governmental PKI certification services in Dubai, i.e., issuing and managing subordinate and end-entity certificates for Government entities, forming its community of subscribers.

### 1.1.1 Dubai PKI Hierarchy

The below Figure depicts the Trust Model of the Dubai PKI. The Dubai PKI Root CA is the top authority in this PKI with regard to the digital certification services offered by Dubai PKI. The Dubai PKI Root CA signs DESC Subordinate CAs, which come at the second level of the PKI hierarchy. In addition, the Root CA also signs issuing CAs belonging to authorized government or private sector entities.

DESC is fulfilling the role of the Policy Authority (PA) for the Dubai PKI (hereinafter, Dubai PKI PA) shall authorize the Root certification services for DESC Subordinate CAs as well as the issuing CAs owned by other government or private sector entities.

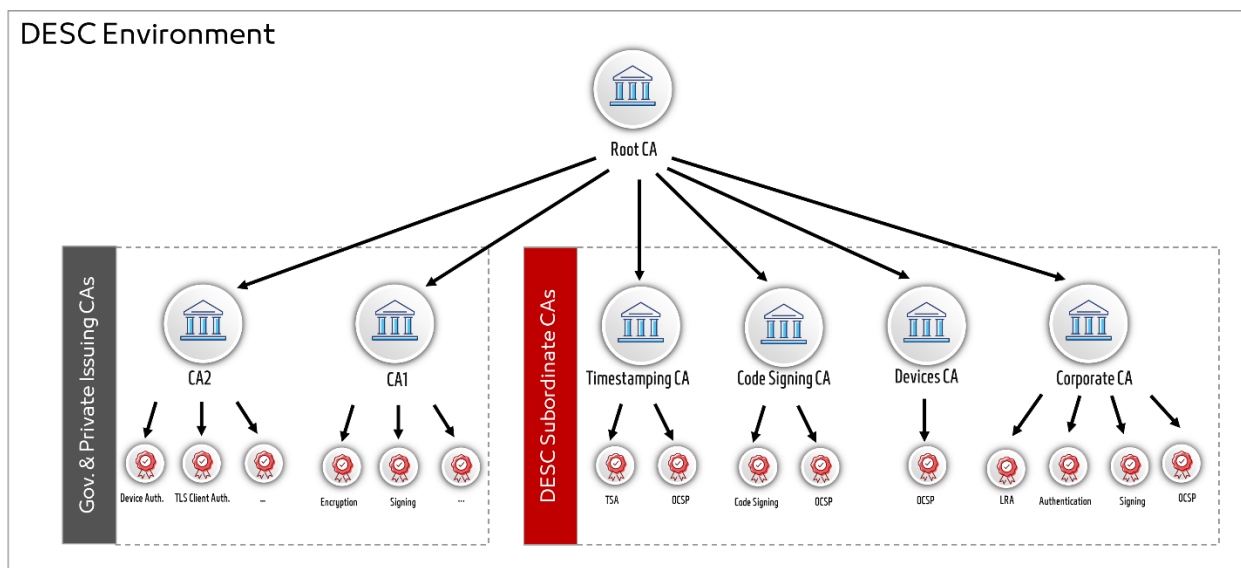


Figure 1: Trust Model for Dubai PKI

### 1.1.2 Dubai PKI Policy Authority (PA)

The Dubai PKI Policy Authority (PA), composed of appointed members of the DESC management and Dubai PKI team, is representing the policy and governing body for the Dubai PKI, including the Timestamping CA. The PA is the highest-level management body with final authority and responsibility for:

***Certificate Practice Statement***

- Specifying and approving the Dubai PKI infrastructure,
- Approving government and private sector entities applications to have their own Subordinate CA(s) within the Dubai PKI hierarchy,
- Specifying, maintaining and approving the Dubai PKI practices and policies, in particular the Certification Practice Statements (CPS) and the related Certificate Policies (CP) when applicable,
- Review annual audit report submitted by government or private sector entities CAs to ensure continuous compliance to Dubai PKI requirements,
- Review regular audit reports of LRAs,
- Enforcing CP/CPS and other policies applicable to Dubai PKI Environment,
- Defining the review process for such practices and policies including responsibilities for maintaining the Dubai PKI CPs/CPSs and related policies,
- Defining the review process that ensures that the Dubai PKI properly implements the above practices,
- Defining the review process that ensures that the related policies are supported by the Dubai PKI CPs and CPSs,
- Publication of CP and CPS documents,
- Specifying installation, key ceremonies, operation and life-cycle management (including deprecation) procedures of the Dubai PKI,
- Evaluating the proper working of the Dubai PKI environment,
- Allocating members to the key ceremonies as witness as well as trusted operatives and key custodians,
- Evaluating changes to the Dubai PKI environment (management, operational, hardware, software and security),
- Evaluating case-by-case issues where key Dubai PKI staff/personnel did not respect the security and/or operational procedures, including ethics,
- Deciding on critical issues in case of incidents, disasters and other severe problems with regards to the Dubai PKI.

### **1.1.3 Certificate Policy**

X.509 certificates issued by the Timestamping CA to subscribers will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RP) to decide whether a Certificate is trusted for a particular purpose. Subscriber Certificates issued by the Timestamping CA will identify the applicable policy in the certificate Policies extension by including applicable OID(s).

### **1.1.4 Relationship Between the DESC Subordinate CAs CP and this CPS**

This CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the Timestamping CA as governed by DESC Subordinate CAs CP and related documents which describe the Dubai PKI requirements and use of Certificates.

## 1.2 Document Name and Identification

This document is named and referred to as “Dubai PKI — Timestamping CA Certificate Practice Statement”.

The Object Identifier of this CPS is OID is .2.16.784.1.2.2.100.1.2.1.3.

DESC organizes the OID for the certificate that is issued by the Timestamping CA as depicted in the table below.

OID	Certificate Type	Description
2.16.784.1.2.2.100.1.3.1.1	Timestamping certificate	A certificate issued to a Timestamp Authority to use to timestamp data.

## 1.3 PKI Participants

The participants within the context of the Timestamping CA are as follows:

- Policy Authority (PA)
- Subordinate Certification Authorities
- Registration Authority (RA)
- Subscribers
- Relying Parties

These participants and their roles are described in the following sections.

### 1.3.1 Certification Authorities

The Timestamping CA (also referred to as “CA”) is the Certification Authority that issues Certificates in accordance with this CPS. The Timestamping CA issues only Timestamping certificates that are used to sign the time stamps issued by the a Timestamping Authority services, in addition to OCSP response signing certificates. This includes the following tasks:

- **Registration Service** — it verifies the identity and, if applicable, any specific attributes of end-entities applying for certificates. The results of this service are passed to the certificate generation service.
- **Certificate Generation Service** — it issues end-entity certificates based on the verification conducted by the registration service
- **Dissemination Service** — it disseminates OCSP and Timestamping CA certificates and makes them available to relying parties. This service also makes available any public policy and practice information to Subscribers and relying parties.
- **Revocation Management Service** — it processes requests and reports revocation data for determining the appropriate action to be taken. The results of this service are available through the certificate validity status service.
- **Certificate Validity Status Service** — it provides certificate validity status information to relying parties based upon certificate suspension/revocation lists and an OCSP responder service. The status information shall always reflect the current status of the certificates issued by this CA.

### **1.3.2 Registration Authorities**

Duly authorized members part of DUBAI PKI team act as Registration Authority (RA) for this CA. This team is involved in validating and accepting certificate issuance and management operations, in addition to triggering related certification operations by this CA.

### **1.3.3 Subscribers**

This CA issues certificate to DESC Timestamping Authority service, it may also issue Timestamping certificates to Timestamping authority services owned and operated by other Dubai Government entities.

### **1.3.4 Relying Parties**

Relying Parties are entities that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate issued by the Timestamping CA.

Relying parties shall always verify the validity of a digital certificate issued by the Timestamping CA using the Timestamping CA Certificate Validations Services (e.g. CRL, OCSP), prior to relying on information featured in the certificate.

### **1.3.5 Other Participants**

There are no other participants for this CA.

## **1.4 Certificate Usage**

### **1.4.1 Appropriate Certificate Use**

This CA issues Timestamping certificates that are used to sign the time stamps issued by a Timestamping Authority service, in addition to OCSP response signing certificates.

In accordance with its purpose of use, the certificate may be used without limitations.

DESC reserves the right to issue any of the above-mentioned certificates for DESC internal testing and quality assurance purposes. Test certificates will be issued by DESC RA that enforces the following rules:

- test certificates have a short lifetime (in days),
- certificate subject DN for test certificates always includes the word "TEST".

### **1.4.2 Prohibited Certificate Use**

Certificates referred to in this CPS document shall not be used for purposes other than the ones listed above under Section 1.4.1 of this CPS document. Using certificates for other purposes is explicitly prohibited.

Certificates referred to in this CPS document shall not be used for man-in-the-middle (MITM) or traffic management of domain names or Ips that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

## 1.5 Policy Administration

### 1.5.1 Organization Administering the Document

DESC, through the Dubai PKI PA, bears responsibility for the drafting, publishing, Object Identifier (OID) registration, maintenance and interpretation of this CPS and other policies and practices within the realm of the Dubai PKI.

### 1.5.2 Contact Person

Inquiries, suggested changes or notices regarding this CPS should be directed to **Dubai PKI Policy Authority**:

Dubai Electronic Security Center

PO Box 36996, Dubai, UAE

Phone +97144150400

E-mail [pa@desc.gov.ae](mailto:pa@desc.gov.ae)

### Certificate Problem Report

Subscribers and Relying Parties, Application Software Suppliers, and other third parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to [pki.support@desc.gov.ae](mailto:pki.support@desc.gov.ae).

DESC will validate and investigate the revocation request before taking an action in accordance with section 4.9.

### 1.5.3 Person Determining CPS Suitability for the Policy

The Dubai PKI PA determines the suitability of any CPS part of the Dubai PKI.

### 1.5.4 CPS Approval Procedures

A dedicated process involves the Dubai PKI PA reviewing the initial version of this CPS and any subsequent updates. Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice. The PA formally approves the new version of the CPS.

In an effort to maintain credibility and promote trust in this CPS and better correspond to accreditation and legal requirements, the Dubai PKI PA shall review this CPS at least annually and may make revisions and updates to policies as it sees fit or as required by other circumstances. Any updates become binding for all Certificates that have been issued or are to be issued upon the date of the publication of the updated version of this CPS.

## 1.6 Definitions, Acronyms and References

### 1.6.1 Definitions

**Affiliate:** A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.



***Certificate Practice Statement***

**Applicant:** The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

**Applicant Representative:** A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: 1. who signs and submits, or approves a certificate request on behalf of the Applicant, and/or 2. who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or 3. who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

**Anti-Malware Organization:** An entity that maintains information about Suspect Code and/or develops software used to prevent, detect, or remove malware.

**Application Software Supplier:** A supplier of software or other relying-party application software that displays or uses Code Signing Certificates, incorporates Root Certificates, and adopts these Requirements as all or part of its requirements for participation in a root store program.

**Attestation Letter:** A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information. In the context of this CPS, attestation letters are signed by Human Resource teams of government entities.

**Audit Period:** In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.)

**Audit Report:** A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

**Authorized Representative:** A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

**Baseline Requirements:** The Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates as published by the CA/Browser Forum.

**CA Key Pair:** A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

**Certificate:** An electronic document that uses a digital signature to bind a public key and an identity.

**Certification Authority:** An organization subject to these Requirements that is responsible for a Timestamping Certificates and, under these Requirements, oversees the creation, issuance, revocation, and management of Timestamping Certificates. Where the CA is also the Root CA, references to the CA are synonymous with Root CA.

**Certificate Beneficiaries:** All Application Software Suppliers with whom the CA or its Root CA has entered into a contract for distribution of its Root Certificate in software distributed by such Application Software Suppliers and all Relying Parties who reasonably rely on such a Certificate while a Code Signature associated with the Certificate is valid.

**Certificate Data:** Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

**Certificate Management Process:** Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

**Certificate Policy:** A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

**Certificate Problem Report:** Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

**Certificate Profile:** A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of this CPS.

**Certificate Revocation List:** A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

**Certificate Requester:** An authorized administrator of a device or system who is responsible for submitting the certification requests to the CA/RA.

**Certification Practice Statement:** One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

**Code:** A contiguous set of bits that has been or can be digitally signed with a Private Key that corresponds to a Code Signing Certificate.

**Code Signature:** A Signature logically associated with a signed Code.

**Code Signing Certificate:** A digital certificate issued by a CA that contains a Code Signing EKU.

**Control:** “Control” (and its correlative meanings, “controlled by” and “under common control with”) means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for “control” under the law of the entity’s Jurisdiction of Incorporation or Registration but in no case less than 10%.

**Country:** Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

**CSPRNG:** A random number generator intended for use in a cryptographic system.

**Declaration of Identity:** A written document that consists of the following:

1. the identity of the person performing the verification,
2. a signature of the Applicant,
3. a unique identifying number from an identification document of the Applicant,
4. the date of the verification, and
5. a signature of the Verifying Person.

**Delegated Third Party:** A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

**Expiry Date:** The “Not After” date in a Certificate that defines the end of a Certificate’s validity period.

**Government Entity:** A Dubai government entity or other government entities in the UAE authorized by Dubai PKI PA to consume the PKI services.

**Hardware Security Module:** a device designed to provide cryptographic functions, especially the safekeeping of private keys.

**High Risk Certificate Request:** A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

**Issuing CA:** In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

**Key Compromise:** A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.

**Key Generation Script:** A documented plan of procedures for the generation of a CA Key Pair.

**Key Pair:** The Private Key and its associated Public Key.

**Legal Entity:** An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

**Object Identifier:** A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

**OCSP Responder:** An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

**Organizational Applicant:** An Applicant that requests a Certificate with a name in the Subject field that is for an organization and not the name of an individual.

**Online Certificate Status Protocol:** An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

**Parent Company:** A company that Controls a Subsidiary Company.

**Private Key:** The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

**Policy Qualifier:** Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

**Public Key:** The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

**Public Key Infrastructure:** A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

**Publicly-Trusted Certificate:** A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely- available application software.

**Qualified Auditor:** A natural person or Legal Entity that meets the requirements of Section 8.2.

**Random Value:** A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

**Registered Domain Name:** A Domain Name that has been registered with a Domain Name Registrar.

**Registration Authority (RA):** Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

***Certificate Practice Statement***

**Reliable Data Source:** An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate. In the context of this CPS, the UAE official gazette is the reliable data source for government entities in UAE.

**Reliable Method of Communication:** A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Requester.

**Relying Party:** Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

**Repository:** An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

**Root CA:** The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

**Root Certificate:** The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

**Signature:** An encrypted electronic data file which is attached to or logically associated with other electronic data and which (i) identifies and is uniquely linked to the signatory of the electronic data, (ii) is created using means that the signatory can maintain under its sole control, and (iii) is linked in a way so as to make any subsequent changes that have been made to the electronic data detectable.

**Sovereign State:** A state or country that administers its own government, and is not dependent upon, or subject to, another power.

**Subject:** The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

**Subject Identity Information:** Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

**Subordinate CA:** A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

**Subscriber:** A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

**Subscriber Agreement:** An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

**Subsidiary Company:** A company that is controlled by a Parent Company.

**Suspect Code:** Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes.

**Technically Constrained Subordinate CA Certificate:** A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

### ***Certificate Practice Statement***

**Terms of Use:** Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

**Timestamp Authority:** A service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via a secure hashing algorithm) existed at the specified time.

**Timestamp Certificate:** A certificate issued to a Timestamp Authority to use to timestamp data.

**Trusted Platform Module:** A microcontroller that stores keys, passwords and digital certificates, usually affixed to the motherboard of a computer, which due to its physical nature makes the information stored there more secure against external software attack or physical theft.

**Trusted Role:** Those individuals who perform a security role that is critical to the operation or integrity of a PKI.

**Trustworthy System:** Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

**UAE PASS:** The UAE national digital identity for citizens and residents, and visitors enabling them to access many online services across various sectors, sign and authenticate documents as well as transactions digitally, request a digital version of their official documents, and use the official documents to request services from service providers.

**Valid Certificate:** A Certificate that passes the validation procedure specified in RFC 5280.

**Validation Specialist:** Someone who performs the information verification duties specified by this CPS and the Baseline Requirements.

**Validity Period:** From RFC 5280 (<http://tools.ietf.org/html/rfc5280>): "The period of time from notBefore through notAfter, inclusive."

**Verifying Person:** A notary, attorney, Latin notary, accountant, individual designated by a government agency as authorized to verify identities, or agent of the CA, who attests to the identity of an individual.

## **1.6.2 Acronyms**

**CA** — Certification Authority

**CCTV** — Closed circuit TV

**CP** — Certificate Policy

**CPS** — Certification Practice Statement

**CRL** — Certificate Revocation List

**DRP** — Disaster Recovery Plan

**DN** — Distinguished Name

**FIPS** — Federal Information Processing Standards

**FQDN** — Fully Qualified Domain Name

**HSM** — Hardware Security Module

**HTTP** — Hyper Text Transfer Protocol

***Certificate Practice Statement***

**HVAC** — Heating, Ventilation and Air Conditioning

**IEC** — International Electro-technical Commission

**IETF** — Internet Engineering Task Force

**IPSEC** — Internet Protocol Security

**ISO** — International Standards Organization

**ITU** — International Telecommunications Union

**LDAP** — Lightweight Directory Access Protocol, a common standard for accessing directories

**DESC** — Dubai Electronics Security Center

**OID** — Object Identifier

**OSCP** — Online Certificate Status Protocol

**OTP** — One Time Password

**PA** — Policy Authority of Dubai PKI

**PIN** — A Personal Identification Number or password used to protect the private information and keys on hardware tokens

**PKCS # 1** — Public-Key Cryptography Standards (PKCS) #1

**PKCS # 7** — Cryptographic Message Syntax

**PKCS #10** — Certification Request Syntax Specification

**PKCS #12** — Personal Information Exchange Syntax published by RSA Security

**PKE** — Public Key Encryption

**PKI** — Public Key Infrastructure

**PKIX-CMP** — Internet X.509 Public Key Infrastructure — Certificate Management Protocol.

**RA** — Registration Authority

**RSA** — The acronym for the inventors of the RSA algorithm; Ron Rivest, Adi Shamir and Leonard Adleman

**SCEP** — Simple Certificate Enrolment Protocol

**Secret Shares** — A set of devices, smart cards, PINs, etc. used with MofN control

**SHA** — Secure Hash Algorithm

**S/MIME** — Secure Multipurpose Internet Mail Extensions

**SSL/TLS** — Secure Sockets Layer/Transport Layer Security

**SubjectAltName** — A certificate extension that contains FQDNs or authenticated domains or email addresses that are under the control of the Subscriber

**TSA** — Timestamping Authority

**UPS** — Uninterruptible Power Supply

**URI** — Universal Resource Identifier, a URL, FTP address, email address, etc.

**X.501** — A common standard for directory entry naming (ITU)

**X.509** — A public key certificate specification originally developed as part of the X.500 directory specification, often used in public key systems; It is now governed by IETF standards



# 2. Publication and Repository Responsibility

## 2.1 Repositories

DESC publishes information about all digital certificates it issues in (an) online publicly accessible repository at <https://ca-repository.desc.gov.ae/> that is also provided on a 24/7 basis.

## 2.2 Publication of Certificate Information

As part of the public repository, DESC publishes a copy of the Timestamping CA certificates, OCSP certificates and Timestamping Certificates as well as this CPS.

DESC also retains other documents that make certain disclosures about the Timestamping CA practices, procedures, and the content of certain of its policies as part of the public repository. DESC reserves its right to make available and publish information on its policies by any means it sees fit.

DESC publishes digital certificate status information in frequent intervals as indicated in this CPS. The provision of the Timestamping CA issued electronic certificate validity status information is a 24/7 available service offered as follows:

- Published CRLs including any changes since the publication of the previous CRL, at regular intervals. The Timestamping CA adds a pointer (URL) to the relevant CRL to Subscribers' certificates as part of the CDP extension whenever this extension is present,
- An OCSP responder compliant with RFC 6960. The OCSP URL is referenced in the AIA extension of the Subscribers' certificates issued by the Timestamping CA.

## 2.3 Time or Frequency of Publication Repositories

Modified versions of this CPS and other published documents are published within five days maximum after the Dubai PKI PA approval.

Due to their sensitivity, DESC refrains from making publicly available certain subcomponents and elements of such documents including certain security controls, procedures related with the functioning of registration authorities, internal security polices, etc. Such documents and documented practices are, however, conditionally available to designated authorized parties in the context of audit(s) that DESC owes duty to with regard to the Timestamping CA activities.

### 2.3.1 Certificates

The Timestamping CA certificate, Timestamping Certificate and OCSP Certificates are published to the Certificate Dissemination Webpage that is part of the public repository (<https://ca-repository.desc.gov.ae/>) as soon as they are issued.

### **2.3.2 CRLs**

DESC maintains the CRL distribution point and the information on this URL for a minimum of Ten (10) years after the expiration date of all certificates, containing the CRL distribution point.

For CRLs signed by the CA signing keys stored on online HSMs, CRLs are published at predefined intervals in accordance with the following rules:

- At the minimum, CRLs shall be refreshed every 26 hours, even if no changes have occurred since the last issuance.
- CRLs lifetime shall be set to 72 hours.

For CRLs signed by the CA signing keys stored on offline HSMs, CRLs are published at predefined intervals in accordance with the following rules:

- At minimum, once every six months, at an agreed time. In addition, a new CRL will be generated and published following the revocation of any certificate,
- CRLs lifetime shall be set to six months

## **2.4 Access Controls on Repositories**

Public read-only access to certificates, CRLs and documentation published to the repository is available.

Access controls are implemented on the repository to prevent any unauthorized addition or modification of any published data.



# 3. Identification and Authentication

## 3.1 Naming

### 3.1.1 Types of Names

This CA is identified in the Issuer's name field of the Subscriber certificates as follows:

cn=Timestamping Certification Authority, o=UAE Government, c=AE

The certificates issued by this CA contain X.500 Distinguished Names (DNs) as follows:

- **TSA Certificates**— The DN format is:  
cn = <TSA Service Name> e.g., Dubai Timestamping Authority  
o = DESC  
l = Dubai,  
c = AE

- **OCSP responder** — The DN format is:  
cn = Timestamping Certification Authority OCSP “C<n>”  
o = DESC  
l = Dubai  
c = AE

where “C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.

### 3.1.2 Need for names to be meaningful

- For Certificates issued for Timestamping Authorities: Distinguished Names (DN) are used to identify the service in a meaningful way,
- For OCSP certificate: name is meaningful since it indicates the OCSP responder name which is “Timestamping Certification Authority OCSP”.

### 3.1.3 Anonymity and Pseudonymity of Subscribers

This CPS does not permit anonymous Subscribers.

### 3.1.4 Rules for Interpreting Various Name Forms

No stipulation — this section is intentionally left blank.

### **3.1.5 Uniqueness of Names**

While this CA issues a limited number of certificates anyway, the usage unique services' (OCSP/TSA) name guarantees the uniqueness of DNSs.

### **3.1.6 Recognition, Authentication and Role of Trademarks**

Certificate applicants are prohibited from using names in their certificate application that infringe upon the Intellectual Property Rights of others. The Timestamping CA does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application.

The Timestamping CA shall have the right to revoke a Certificate upon receipt of a properly authenticated order from DESC or court of competent jurisdiction requiring the revocation of a Certificate or Certificates containing a Subject name in dispute.

## **3.2 Initial Identity Validation**

### **3.2.1 Method to Prove Possession of Private Key**

Certificate Signing Requests (CSRs) generated for the Timestamping Authorities contain a Proof-of-Possession (POP) of the private key as part of the certificate requests submitted to this CA.

### **3.2.2 Authentication of Organization and Domain Identity**

#### **3.2.2.1 Identity**

For certificates containing organization information, particularly Timestamping certificates issued for TSA operated by other Dubai Government Entities, the applicant is required to provide the Government entity's name, organizational unit (if applicable) and official address. DESC RA verifies the Organization's identity as follows:

#### **A. Presence / Legal standing**

- Verify the existence of the Organization using an Reliable Data Source that is expected to provide detailed information about the entity including its legal name and address, the most common Data Source used by DESC RA is the UAE Official Gazette,
- Verify authority of the Organization's authorized representative requesting the certificate as specified in section 3.2.5.

#### **B. Association**

The organization name to be inserted in the requested certificate must exactly match the legal name of the Government entity requesting the certificate unless there is an authentic proof linking the entity with the name to be included in the certificate.

#### **C. Authority of the applicant**

The authority of the requester/authorized representative to request a certificate on behalf of a Government entity is authenticated in accordance with section 3.2.5.

**For certificates issued to OCSP and the Dubai PKI TSA:** an authorized administrator under the supervision of the Dubai PKI PA initiates the certification process. A dedicated operational key ceremony is documented by DESC.

#### **3.2.2.2 DBA/Tradenname**

The use of DBA or Tradenname in the Subject Identity Information is not supported by the Timestamping CA.

### **3.2.2.6 Data Source Accuracy**

DESC RA uses documented internal processes to check the accuracy of information and documents received as part of the certificate enrolment process. The Official Gazette is used as the official government source to validate the Government entity information, including authorized representatives. Refer to sections 3.2.2 and 3.2.2.1 of this CPS for further details.

### **3.2.3 Authentication of Individual Identity**

**For the Timestamping certificates issued to Timestamping authority services owned and operated by other Dubai Government entities:** a human sponsor (requester) from the applying entity submits the certificate request and provides registration information to DESC RA.

DESC RA officers perform verification of the identity of the requester through the following procedures:

- (1) DESC RA conducts an identity proofing Identity validation through one of the following methods:
  - Face-to-face verification against his/her Emirates ID
  - Remote verification involving a government issued ID and biometric verification
  - Receive a digitally signed certificate from by the requestor using a valid UAE PASS certificate
- (2) DESC RA uses a proof of employment to validate the association between the requester and the Government entity.
- (3) DESC RA confirms the authenticity of the certificate application and the authenticity of the attestation letter directly with the government entity authorized representative. A reliable method of communication is used involving the usage of the government email addresses and where deemed necessary by an in-person meeting.

**For certificates issued to OCSP and the Dubai PKI TSA:** an authorized administrator under the supervision of the Dubai PKI PA initiates the certification process. DESC documents a dedicated operational key ceremony.

### **3.2.4 Non-Verified Subscriber Information**

All fields constituting the subscriber information written in the certificate are verified by DESC RA team.

### **3.2.5 Validation of Authority**

The authority of the certificate requestor to request a certificate on behalf of a Government entity will be performed through a reliable means of communication with the Government entity that include the following steps at minimum:

- (1) DESC RA receives a legible copy, which discernibly shows the requester's face, of at least one currently valid government-issued photo ID (Emirates ID, passport or a UAE driving license). DESC RA will then inspect the copy for any indication of alteration or falsification,
- (2) DESC RA receives a completed and signed certificate request form from the requestor. The form is signed by the authorized representative that attests the ability of the requestor to requests certificates on behalf of the government entity,
- (3) DESC RA verifies the authority of the authorized representative through the Official Gazette or through a formal communication of the Government entity HR, or based on a formal letter signed by the Organization's top authority (e.g. Director General).

### **3.2.6 Criteria for Interoperation**

No stipulation — this section is intentionally left blank.

## 3.3 Identification and Authentication for Re-keying Requests

### 3.3.1 Identification and Authentication for Routine Re-Keying

Identification and authentication for re-keying is performed as in initial registration.

### 3.3.2 Identification and Authentication for Re-Key After Revocation

Identification and authentication for re-keying after revocation is performed as in initial registration.

## 3.4 Identification and Authentication for Revocation Requests

**For the Timestamping certificates issued to Timestamping authority services owned and operated by other Dubai Government entities:** The identification and authentication of revocation requests are conducted by DESC RA as follows:

- Verify that the revocation request is signed by an authorized representative,
- The request is sent to DESC RA from a formal email address that belongs to the entity to which the certificate was issued,
- A communication is done by DESC RA with the entity to establish reasonable assurance on the legitimacy of the revocation request. Such communication, depending on the circumstances, may include one or more of the following: telephone or e-mail.

**For certificates issued to OCSP and the Dubai PKI TSA:** certificates revocation shall be conducted as part of DESC internal processes and shall be approved by the Dubai PKI PA.

Once the revocation request is successfully authenticated, DESC RA revokes the subject certificate through the relevant RA system.

# 4. Certificate Life Cycle Management

## 4.1 Certificate Application

### 4.1.1 Who can Submit a Certificate Application

**For the Timestamping certificates issued to Timestamping authority services owned and operated by other Dubai Government entities:** A Government entity authorized representative, or an authorized administrator of the TSA service. Whoever is submitting the certificate request (requester) needs to sign the application form and ensure that the government entity authorized representative approves the certificate request by signing and stamping the certificate request form and the appended subscriber agreement.

The DESC RA maintains its own internal blacklist of organizations from which it will not accept certificate requests. DESC RA logs in this database previously rejected certificate requests due to suspected or fraudulent usage and revoked certificate requests from government entities. This internal blacklist database is queried by the DESC RA whenever it receives any certificate request.

**For certificates issued to OCSP and the Dubai PKI TSA:** an authorized administrator under the supervision of the Dubai PKI PA initiates the certification process. A dedicated operational key ceremony is documented by DESC.

### 4.1.2 Enrolment Process and Responsibilities

**For the Timestamping certificates issued to Timestamping authority services owned and operated by other Dubai Government entities:**

- The DESC RA requests the certificate requester to fill certificate application request form then get it signed and stamped as specified in section 4.1.1,
- The DESC RA requests to sign the Subscriber Agreement, the agreement needs to be signed by an authorized representative of the entity requesting the certificate
- The DESC RA requests the following to be submitted via official email:
  - Singed/stamped certificate request form,
  - Signed/stamped subscriber agreement,
  - The information and documents required for identification and authorization.
- One of DESC RA verifies the authorized representative, certificate requester and the organization's identity as described in section 3.2.2.
- A second DESC RA officers reviews the work done the first officer to conclude application's approval.

Once the above request validation is completed, DESC RA then execute the certification request as follows:

***Certificate Practice Statement***

- DESC RA team communicates with the requester (through the email address mentioned in the certification application form) to generate their Timestamping key pair and a CSR including the information provided in the certificate request form. The CSR shall be signed as a Proof-of-Possession (POP) of the private key,
- The requester shares the CSR with DESC RA team through the requester's email (as provided in the certificate application form),
- DESC RA team validate the structure, format of the CSR that shall be a PKCS#10 CSR. The RA team also validates information included in the CSR against the information included in the certificate request form,
- DESC RA team use a dedicated RA application submit the CSR to this CA and retrieve the certificate,
- DESC RA team send the certificate to the requester's email address (as provided in the certificate application form).

**For certificates issued to OCSP and the Dubai PKI TSA:** the DESC RA and an authorized PKI administrator in trusted role oversee the execution of DESC internal operational ceremonies through which any of these certificates is issued. The Dubai PKI PA approves the operational ceremony documentation and validates the embedded certificate profiles and content against the provisions of this CPS.

### **4.1.3 Identification and Authentication for Routine Re-Keying**

Identification and authentication for re-keying is performed as in initial registration.

## **4.2 Certificate Application Processing**

### **4.2.1 Performing Identification and Authentication Functions**

Refer to section 3.2 in addition to the following:

**For the Timestamping certificates issued to Timestamping authority services owned and operated by other Dubai Government entities:**

- a) DESC RA blacklist check: If the requestor/entity is in the blacklist, the certificate application is rejected,  
*Any malicious certificate or revocation request or a request that fails multiple (more than 3) times is added to DESC RA blacklist.*
- b) Verify the Organization's identity as specified in section 3.2.2.1,
- c) verify that the legal name of the government entity requesting a certificate and the organization name to be inserted in the requested certificate are matching unless there is an authentic proof linking the entity with the name included in the certificate. The full name or the abbreviated version may be added to the certificate as agreed with the requesting entity.

All above activities (e-mail communication, phone calls, vetting evidence) are stored along with the certificate application.

**For certificates issued to OCSP and the Dubai PKI TSA:** the DESC RA and an authorized PKI administrator in trusted role oversee the execution of DESC internal operational ceremonies through which any of these certificates is issued. The Dubai PKI PA approves the operational ceremony documentation and validates the embedded certificate profiles and content against the provisions of this CPS.

## **4.2.2 Approval or Rejection of Certificate Applications**

The DESC RA team approve or reject the application for the certificate based on the results of the identification and authentication specified under section 4.2.1.

**For certificates issued to OCSP and the Dubai PKI TSA:** a certificate application is approved as part of the overall authorization of the internal operational ceremony.

Multi-factor authentication is implemented for an RA officer to access the relevant RA application to approve certificate applications for issuance.

## **4.2.3 Time to Process Certificate Applications**

No stipulation — this section is intentionally left blank.

# **4.3 Certificate Issuance**

## **4.3.1 CA Actions During Certificate Issuance**

Following the approval of the certificate application by the DESC RA team, the CSR is uploaded and submitted to the CA either manually using a dedicated RA application or automatically through a certificate management protocol.

The CA then validates the format and structure of the CSR then signs the certificate in accordance with the specified certificate template. The certificate is activated by the CA and is ready for usage.

The certificate is sent by the RA officer to the requester's email address or downloaded by the requester directly from RA application that is exposed over a private network or downloaded by the system/device through a certificate management protocol.

**For certificates issued to OCSP and the Dubai PKI TSA:** The DESC administrator manually delivers the CSR file including the device's PEM or DER encoded public key to DESC RA team. DESC RA team submit the CSR file directly to the CA who will sign and publish a certificate suitable for verification. The certificate is returned to the DESC administrator thereafter.

## **4.3.2 Notification to Subscriber by the CA of Issuance of Certificate**

The RA Officer notifies the Subscriber to collect his or her certificate.

# **4.4 Certificate Acceptance**

## **4.4.1 Conduct Constituting Certificate Acceptance**

When the requester downloads or receives the certificate, he/she validates the certificate content against the request made earlier. In case of any discrepancies noted by the requester, he/she initiates a communication with the DESC RA, that may lead to initiation of the certificate revocation request by the requester.

If no complaints were raised by the requester or the Government entity to the DESC RA within 10 business days from receiving the certificate, the certificate is deemed accepted by the applicant.

**For certificates issued to OCSP and the Dubai PKI TSA:** A certificate is deployed on the target system as part of the overall DESC internal operational ceremony.

## **4.4.2 Publication of the Certificate by the CA**

The Timestamping CA, TSA and OCSP certificates are published on the dissemination page as described in Section 2.2.

## **4.4.3 Notification of Certificate Issuance by the CA to Other Entities**

No stipulation — this section is intentionally left blank.

# **4.5 Key Pair and Certificate Usage**

## **4.5.1 Subscriber Private Key and Certificate Usage**

On the user of Private Key and Certificate, Subscribers of the CA are obligated to:

- Comply with the terms of the Subscriber agreement,
- Use certificates exclusively for legal activities consistent with the CP and this CPS,
- Protect the private key (and related secrets) from compromise, loss, disclosure, or otherwise from unauthorized use,
- Discontinue the use of a private key following expiration or revocation of the corresponding certificate unless a subsequent unexpired or unrevoked certificate corresponding to that private key has been issued,
- Notify the DESC RA immediately if any details in the certificate become invalid, or as a result of any compromise, loss, disclosure, or otherwise unauthorized use of their private keys,
- Avoid using the private key until after the CA has issued, and the Subscriber has accepted the corresponding certificate.

## **4.5.2 Relying Party Public Key and Certificate Usage**

On the user of Public Key and Certificate, Relying Parties are obligated to:

- Validate the certificate path,
- Ensure that the key is appropriate for the intended use as set forth in this CPS and that such use is consistent with the applicable certificate content including, but not limited to, the key usage, extended key usage, and certificate policies extension fields,
- Check the status of the certificate in accordance with the requirements stated in Section 4.9.6 of this CPS. As part of the validation process, the authenticity of the revocation must be validated as follows:
  - In case of using CRLs, the digital signature of the CRLs is validated,
  - In case of using OCSP, the digital signature of the OCSP response is validated.
- Ensure that reliance was reasonable and made in good faith in light of all the circumstances that were known or should have been known to the relying party at the time of reliance.

If a party relying on the Dubai PKI accepts a certificate that cannot be validated through the Timestamping CA OCSP or CRL, it decides to do so completely at his or her own risk.

# **4.6 Certificate Renewal**



### ***Certificate Practice Statement***

Certificate Renewal is the act of issuing a new certificate when all the identifying information and the public key from the old certificate are duplicated in the new certificate; however, there is a different (longer) validity period.

This CA does not support certificate Renewal. Only certificate re-key is supported.

#### **4.6.1 Circumstance for certificate renewal**

Not applicable.

#### **4.6.2 Who may request renewal**

Not applicable.

#### **4.6.3 Processing certificate renewal requests**

Not applicable.

#### **4.6.4 Notification of new certificate issuance to subscriber**

Not applicable.

#### **4.6.5 Conduct constituting acceptance of a renewal certificate**

Not applicable.

#### **4.6.6 Publication of the renewal certificate by the CA**

Not applicable.

#### **4.6.7 Notification of certificate issuance by the CA to other entities**

Not applicable.

## **4.7 Certificate Re-Key**

Certificate Re-key is the act of re-issuing a certificate for an existing Subscriber such that all the identifying information from the old certificate is duplicated in the new certificate; however, there is a different public key and a different validity period.

This CA supports Certificate Re-key. The re-key process (including identity validation, issuance) is similar to the initial certificate application.

#### **4.7.1 Circumstance for Certificate Re-key**

Certificate re-key may happen while the certificate is still active, after it has expired or after a revocation. The original certificate may be revoked after re-key is complete, however, the original certificate must not be further re-keyed.

#### **4.7.2 Who May Request Certification of a New Public Key**

As per initial certificate issuance.

#### **4.7.3 Processing Certificate Re-Keying Requests**

As per initial certificate issuance.

#### **4.7.4 Notification of New Certificate Issuance to Subscriber**

As per initial certificate issuance.

#### **4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate**

As per initial certificate issuance.

#### **4.7.6 Publication of the Re-keyed Certificate by the CA**

As per initial certificate issuance.

#### **4.7.7 Notification of Certificate Issuance by the CA to Other Entities**

As per initial certificate issuance.

## **4.8 Certificate Modification**

### **4.8.1 Circumstance for certificate modification**

This CPS does not provide provisions for certificate modification. If the Subscriber wants to change the information stored in the certificate or has requested revocation of his/her existing certificate and wishes to be issued a new certificate with modified information, the Subscriber shall submit a new certificate application.

### **4.8.2 Who may request certificate modification**

Not applicable. Refer to section 4.8.1.

### **4.8.3 Processing certificate modification requests**

Not applicable. Refer to section 4.8.1.

### **4.8.4 Notification of new certificate issuance to subscriber**

As per initial certificate issuance.

### **4.8.5 Conduct constituting acceptance of modified certificate**

Not applicable. Refer to section 4.8.1.

### **4.8.6 Publication of the modified certificate by the CA**

As per initial certificate issuance.

### **4.8.7 Notification of certificate issuance by the CA to other entities**

As per initial certificate issuance.

## **4.9 Certificate Revocation and Suspension**

Suspension of a certificate is not allowed by this CA. Only permanent certificate revocation is allowed.

#### **4.9.1 Circumstances for Revocation**

DESC shall revoke a certificate within 24 hours if one or more of the following occurs:

1. DESC received a written request from the Subscriber or an authorized Government entities' representative,
2. The Subscriber discovers that the original certificate request was not authorized and does not retroactively grant authorization,
3. The CA discovers or has reasons to believe that there has been a compromise of the private signing key,
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see <https://wiki.debian.org/SSLkeys>), or
5. The information on the certificate is no longer accurate.

This CA will revoke the certificate if one or more of the following occurs. Revocation may be done within 24 hours and shall be done within 5 days:

1. DESC obtains evidence that the certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6,
2. DESC obtains evidence that the Certificate was misused,
3. DESC is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use,
4. DESC is made aware of a material change in the information contained in the Certificate,
5. DESC is made aware that the Certificate was not issued in accordance with DESC CP/CPS,
6. Finding that the certificate was issued without the authorization of the individual named as the subject of such certificate,
7. DESC determines or made aware that any of the information appearing in the Certificate is inaccurate or misleading,
8. Revocation is required by DESC's CP and/or CPS,
9. The Government entity or the individual has been declared legally incompetent,
10. DESC is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed,
11. The Timestamping CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate, or
12. The Timestamping CA's right to issue Certificates under the requirements defined in this CPS expires or is revoked or terminated, unless the Timestamping CA has made arrangements to continue maintaining the CRL/OCSP Repository.

On the other hand, this CPS does not provide provisions for revoking an OCSP/Dubai PKI TSA Certificate apart from the compromise of the OCSP/Dubai PKI TSA key pair which is treated by DESC as per its disaster recovery and business continuity procedures.

The following sub-sections focus only on the revocation provisions that apply to the certificates issued by this CA.

#### **4.9.2 Who can Request Revocation**

- The Subscriber or an authorized representative.

### ***Certificate Practice Statement***

- The subscriber or an authorized representative can request the revocation of their certificate(s) to the DESC RA.
- Any relying party possessing evidence of compromise of the Subscriber's certificate may request revocation from DESC.
- DESC's RA officers directly initiate revocations in the cases described in Section 4.9.1.
- DESC at its own discretion (if for instance, a compromise is known for this CA key).
- Subscribers, relying parties, application software suppliers, and other third parties may submit Certificate Problem Reports to notify DESC of a suspected reasonable cause to initiate the certificate revocation process.

#### **4.9.3 Procedure for Revocation Request**

Subscribers can submit revocation requests anytime to DESC RA. Authenticated and approved revocation requests shall be processed promptly as per the time constraints described in section 4.9.5.

Revocation requests are raised and executed as follows:

- Subscribers fill the certificate revocation form, sign it, then share it with DESC RA,
- DESC RA team authenticates the requester's identity as described in section 3.4, this includes confirmation of the revocation reason,
- DESC RA team validates the information in the revocation request form,
- DESC RA team apply certificate revocation through a dedicated RA application,
- The CA produces a new CRL which is published to its repository, the CA also pushes the revocation status to the OCSP service,
- DESC RA notifies the subscriber via email on the completion of revocation,
- If applicable based on the circumstance of revocation, DESC RA may update their internal blacklist with details of the revoked certificate and/or the subscriber's details.

**For certificates issued to OCSP and the Dubai PKI TSA:** certificates revocation is conducted as part of a PKI process internal to the DESC and approved by the Dubai PKI PA. This process involves communications with relying parties in order to update them on the OCSP/TSA certificate revocation.

#### **Certificate Problem Report**

Subscribers and Relying Parties, Application Software Suppliers, and other third parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to [pki.support@desc.gov.ae](mailto:pki.support@desc.gov.ae).

#### **4.9.4 Revocation Request Grace Period**

There is no revocation grace period. Revocation requests are processed by DESC RA timely after a decision for revocation is made and within the timeframes listed under section 4.9.1.

#### **4.9.5 Revocation Request Response Time**

Certificate revocation requests received from the applicant representative or initiated by DESC RA are processed within 24 hours.

For certificate problem reports, DESC RA begins investigations within 24 hours from receiving the report. DESC RA initiates communication with the Subscriber and where appropriate, with other concerned authorities (e.g. local regulator). A preliminary communication on the certificate problem is sent to the Subscriber and to the originator of the problem report.

DESC RA performs further investigations involving the Dubai PKI PA, the subscriber and other relevant authorities (e.g. local regulator) to decide on the action to be taken on the subject certificate.

If the investigations results led to one of the certificate revocation circumstances listed in section 4.9.1, then the certificate within the timeframe set forth in Section 4.9.1.

Based on the revocation circumstance, DESC RA may agree with subscriber on a plan to issue a new certificate.

#### **4.9.6 Revocation Checking Requirement for Relying Parties**

The Timestamping CA provides revocation information to relying parties through CRLs published on a publicly available web server and through its publicly available OCSP responder.

Certificates issued by this CA (except OCSP certificates) include the name of the web-based distribution point and OCSP responder link from where a relying party could get revocation information. It is the relying party's obligation to retrieve and process the most up-to-date revocation information.

#### **4.9.7 CRL Issuance Frequency**

CRLs are issued as per section 2.3.

#### **4.9.8 Maximum Latency for CRLs**

The Timestamping CA issues CRLs as per the CRL issuance frequency listed in section 2.3.

#### **4.9.9 Online Revocation/Status Checking Availability**

OCSP is supported within this PKI solution and is compliant with RFC 6960. OCSP information is available immediately to relying party applications based on the updates done by the CA on the certificates' status.

The actual OCSP URL to be queried by relying party organizations is referred to in the certificates.

#### **4.9.10 Online Revocation Checking Requirements**

The Timestamping CA OCSP responder supports both HTTP GET and HTTP POST methods.

The Timestamping CA OCSP responder's responses define value in the nextUpdate field which is not more than 8 hours after the thisUpdate field.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused" (i.e. not issued by) the Timestamping CA, then the OCSP responder responds with a "revoked" status as defined by RFC 6960.

#### **4.9.11 Other Forms of Revocation Advertisements Available**

The Timestamping CA only uses OCSP and CRL as methods for publishing certificate revocation information.

#### **4.9.12 Special Requirements — Key Compromise**

If DESC discovers, or has a reason to believe, that there has been a compromise of the private key of the Timestamping CA, DESC will immediately declare a disaster and invoke Dubai PKI business continuity plan. DESC will (1) determine the scope of certificates that must be revoked, (2) revoke impacted certificates within 24 hours and publish online CRLs within 24 hours of creation, (3) use reasonable efforts to notify subscribers and potential relying parties that there has been a key compromise, and (4) generate new CA key pair as per DESC operations policies and procedures.

Parties may use the following methods to demonstrate key Compromise:

- Submission of a signed CSR, Private Key or other challenge response signed by the Private Key and verifiable by the Public Key, or
- The private key itself.

#### **4.9.13 Circumstances for Suspension**

Certificate suspension is not supported by this CA.

#### **4.9.14 Who Can Request Suspension**

Not applicable.

#### **4.9.15 Procedure for Suspension Request**

Not applicable.

#### **4.9.16 Limits on Suspension Period**

Not applicable.

## **4.10 Certificate Status Services**

Refer to Section 4.9.6 of this document. In addition, the following provisions are made.

### **4.10.1 Operational Characteristics**

CRLs are published by this CA on a public repository which is available to relying parties through HTTP interface (an HTTP URL of the CRL distribution point is included in the certificate's CDP extension).

The Timestamping CA OCSP responder exposes an HTTP interface accessible to relying parties. It provides revocation information as below:

- it supports real-time revocation status i.e. for every revocation performed by this CA, revocation information is available to the OCSP service immediately,
- responses define value in the nextUpdate field which is not more than 8 hours after the thisUpdate field,
- the value in the nextUpdate field always before or equal to the notAfter date of all certificates included within the BasicOCSPResponse.certs field, or if the certs field is omitted, before or equal to the notAfter date of the CA certificate which issued the certificate that the BasicOCSPResponse is for.

Revocation entries in OCSP responder are maintained for the same amount of time as for the CRL entries, as described in Section 2.3.2.

#### **4.10.2 Service Availability**

The repository including the latest CRL should be available 24X7 at least 99% per year.

The CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA maintains a 24X7 ability to respond internally to high-priority certificate problem report as described in section 4.9.3 of this CPS.

#### **4.10.3 Optional Features**

No stipulation — this section is intentionally left blank.

### **4.11 End of Subscription**

No stipulation — this section is intentionally left blank.

## **4.12 Key Escrow and Recovery**

Key escrow and recovery are not supported by this CA.

#### **4.12.1 Key Escrow and Recovery Policy and Practices**

Key escrow is not supported by this CA.

#### **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

Not applicable.

# 5. Facility, Management and Operational Controls

## 5.1 Physical Controls

### 5.1.1 Site Location and Construction

All critical components of the PKI system are housed within a highly secure enclave within a secure Data Center premises. Physical access controls are in place to protect the infrastructure, management systems and related operational activities of the PKI solution.

### 5.1.2 Physical Access

Physical security controls include security guard-controlled building access, biometric access, and Closed-Circuit TV (CCTV) monitoring. These physicals controls protect the hardware and software from unauthorized access, furthermore these controls are be monitored on a 24x7x365 basis.

The Dubai PKI systems are protected by six tiers of physical security, with access to the lower tier required before gaining access to the higher most restrictive tier. Sensitive CA operational activities related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Physical access is enforced through the use of two factor biometric authentication. Further, access to the enclave where the Dubai PKI systems are hosted is enabled only if two trusted employees are present to open the enclave's door.

Unauthorized personnel, including un-trusted or third-party employees or visitors, are not allowed into such secured areas without a prior approval and without an escort from one of trusted employees. Similar restrictions exist for the Disaster Recovery site.

All the Networking and systems components including the certification components are located in secure Data cabinets with locks from both sides. To prevent tampering, cryptographic hardware is stored in the most secure area, with access limited to authorized personnel.

### 5.1.3 Power and air conditioning

The secure enclave is furnished with an Uninterruptible Power Supply (UPS), and heating ventilating and air conditioning (HVAC) sufficient to maintain the computer equipment within the manufacturers recommended range of operating temperatures and humidity.

### 5.1.4 Water Exposures

The data centers hosting the PKI systems are implementing reasonable precautions to minimize impact of water exposure. These include installing the PKI equipment on elevated floors with moisture detectors.



### **5.1.5 Fire Prevention and Protection**

The secure enclave is protected from fire, heat with a smoke detection equipment monitored on a 24\*7\*365. Fire suppression equipment are installed within the enclave.

### **5.1.6 Media Storage**

Electronic optical and other media shall be stored, so that they are protected from accidental damage (water, fire, electromagnetic radiation). Media that contains audit archives and backup information shall be stored in a secure fire-proof safe, while it is stored within the enclave.

### **5.1.7 Waste Disposal**

All obsolete paper, magnetic media, optical media, etc., created within the enclave, must be shredded before discarding. Reusable magnetic and optical media may be reused indefinitely within the enclave but must be properly wiped and/or destroyed depending on the confidentiality of the data stored on the medium.

### **5.1.8 Offsite Backup**

Backups taken from the Dubai PKI systems provide sufficient recovery information to allow the recovery from system failure(s). Backups are made on a daily basis and copies are transferred to a secure offsite location on regular basis.

Facilities used for offsite backup and archives shall have the same level of security as the DESC's main site.

## **5.2 Procedural Controls**

DESC follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of electronic signature-related technologies.

DESC obtains a signed statement from each member of the staff concerned on not having conflicting interests with the Timestamping CA activities, maintaining confidentiality and protecting personal data.

### **5.2.1 Trusted Roles**

All members of the staff operating the key management operations, administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position (i.e., trusted operatives). The following are the trusted roles for a Timestamping CA:

- Director of Cybersecurity Systems and Solutions Department
- Operations Manager
- Credentials Owners
- Chief Information Security Officer (CISO)
- Registration Authority (RA) Officers
- PKI Administrators

### ***Certificate Practice Statement***

DESC conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to ensure their trustworthiness and competence. Trusted roles individuals must go through an annual background checks.

#### **5.2.2 Number of Persons Required per Task**

DESC maintains and enforces rigorous control procedures to ensure the segregation of duties, based on job responsibility, in order to prevent single trusted personnel to perform sensitive operations.

The most sensitive tasks such as the following require the involvement of two or more persons:

- physical access to the secure enclave where the CA systems are hosted,
- access to and management of CA cryptographic hardware security module (HSM),
- validate and authorize the issuance of end-entity certificates. This is enforced during the certificate application processing where an RA officer review and verify all the Applicant information and a second RA officer reviews and finally cross sign the application to get it approved.

All operational activities performed by the personnel having trusted roles are logged and maintained in a verifiable and secure audit trail.

#### **5.2.3 Identification and Authentication for Each Role**

Before carrying out the responsibilities of a trusted role:

- DESC confirms the identity of the employee by carrying out background checks,
- DESC issues an access credentials to the individual who needs to access equipment located in the secure enclave,
- DESC provides the required dedicated credentials that allow designated individuals to conduct their functions.

#### **5.2.4 Roles Requiring Separation of Duties**

DESC ensures separation among the following discreet work groups:

- Personnel managing operations on certificates,
- Administrative personnel who operate the supporting platform,
- Security personnel who enforce security measures.

## **5.3 Personnel Controls**

DESC ensures implementation of security controls with regard to the duties and performance of the members of its staff with regards to the Timestamping CA activities. These security controls are documented in an internal confidential policy and include the areas below.

#### **5.3.1 Qualifications Experience and Clearance Requirements**

Prior to the commencement of employment of a DUBAI PKI personnel, whether as an employee, agent, or an independent contractor, DESC ensures that checks are performed to establish the background, qualifications and experience needed to perform within the competence context of the specific job. Such checks include:

1. Verify the Identity of Such Person: Verification of identity MUST be performed through:

***Certificate Practice Statement***

- A. The personal (physical) presence of such person before trusted persons who perform human resource or security functions, and
  - B. The verification of well-recognized forms of government-issued photo identification (e.g., Emirates ID); and
2. Verify the Trustworthiness of Such Person: Verification of trustworthiness includes background checks, which address at least the following, or their equivalent:
- A. Criminal convictions for serious crimes
  - B. Misrepresentations by the candidate
  - C. Appropriateness of references
  - D. Any clearances as deemed appropriate

### **5.3.2 Background Check Procedures**

DESC conducts background investigations for all the Dubai PKI personnel, contractors, trusted roles and management positions. Additionally, DUBAI PKI staff who have Trusted roles go through an annual background check to ensure continuous trustworthiness of those employees

### **5.3.3 Training Requirements**

DESC makes available relevant technical training for their personnel to perform their functions.

For personnel performing information verification and vetting (i.e., RA officers), public key infrastructure topics, authentication and vetting policies and procedures, applicable CP and CPS material and common threats to the information verification process are included.

The required skills and knowledge for validation specialists are tested through an examination on the information verification requirements outlined in the Baseline Requirements.

### **5.3.4 Retraining Frequency and Requirements**

The training content is reviewed and amended on a yearly basis to reflect latest leading practices, CA configuration changes and relevant updates on applicable requirements.

### **5.3.5 Job Rotation Frequency and Sequence**

The Dubai PKI PA ensures that any change or rotation in staff shall not affect the operational effectiveness, continuity and integrity of the Timestamping CA services.

### **5.3.6 Sanctions for Unauthorized Actions**

DESC sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the Dubai PKI personnel, as it might be appropriate under the circumstances and as per the prevailing HR policy and the applicable Dubai law.

### **5.3.7 Independent Contractor Requirements**

Independent subcontractors and their personnel are subject to the same background checks as DESC employees. The background checks include:

- Criminal convictions for serious crimes,

### ***Certificate Practice Statement***

- Misrepresentations by the candidate,
- Appropriateness of references,
- Any clearances as deemed appropriate,
- Privacy protection,
- Confidentiality conditions.

#### **5.3.8 Documentation Supplied to Personnel**

DESC makes available documentation to personnel during initial training and retraining.

## **5.4 Audit Logging Procedures**

### **5.4.1 Types of Event Recorded**

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. At a minimum, each audit record includes the following:

- The date and time the event occurred,
- A success or failure indicator of the event (e.g. CA signing event, revocation event, certificate validation event),
- The identity of the entity and/or operator that caused the event,
- Description of the event.

DESC ensures that at least the following details are recorded:

- CA key lifecycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction,
  - Cryptographic device lifecycle management events.
- CA and subscriber certificate lifecycle management events, including:
  - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles,
  - Certificate requests, re-key requests, and revocation,
  - All verification activities stipulated in these requirements and the CA's Certification Practice Statement,
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls,
  - Acceptance and rejection of certificate requests,,
  - Issuance of Certificates,
  - Generation of Certificate Revocation Lists and OCSP entries.
- Security events, including:
  - Successful and unsuccessful PKI system access attempts,
  - PKI and security system actions performed,
  - Security profile changes,

***Certificate Practice Statement***

- System crashes, hardware failures and other anomalies,
- Firewall and router activities,
- Entries to and exits from the CA facility.

In addition, DESC maintains internal logs and audit trails of relevant operational events in the infrastructure, including, but not limited to:

- Start and stop of servers,
- Outages and major problems,
- Physical access of personnel and other persons to sensitive parts of DESC site,
- Backup and restore,
- Report of disaster recovery tests,
- Audit inspections,
- Upgrades and changes to systems, software and infrastructure,
- Security intrusions and attempts at intrusion
- System configuration changes and maintenance, as defined in the CPS,
- CA personnel changes,
- Discrepancy and compromise reports,
- Information concerning the destruction of sensitive information,
- Current and past versions of all Certificate Policies,
- Current and past versions of Certification Practice Statements,
- Vulnerability Assessment Reports,
- Threat and Risk Assessment Reports,
- Compliance Inspection Reports.
- Current and past versions of Agreements
- Other documents that are required for audits include:
  - Infrastructure plans and descriptions,
  - Physical site plans and descriptions,
  - Configuration of hardware and software,
  - Personnel access control lists.

### **5.4.2 Frequency of Processing Log**

DESC ensures that designated personnel reviews log files at regular intervals to validate log integrity and ensure timely identification of anomalous events.

For online systems: designated personnel must report and perform follow-up of these events and any issues affecting audit log integrity as per the following audit log review cycle:

- On a monthly basis, the PKI operations management reviews the CA applications and security logs to validate the integrity of the logging processes and to test/confirm the daily monitoring function is being operated properly,

### ***Certificate Practice Statement***

- On a quarterly basis, the PKI operation management reviews the physical access logs and the user management on the CA systems with an objective to continuously validate the ongoing physical and logical access policies,
- Evidence of audit log reviews, outcome of the review process, and executed remediation actions are collected and archived for inspection by authorized DESC personnel.

For offline systems: Log files are properly protected by an access control mechanism, so that no others can have access. Log files and audit trails are made available upon request by designated auditors.

#### **5.4.3 Retention Period for Audit Log**

The audit logs are retained for at least two years:

- CA certificate and key lifecycle management event records (as set forth in Section 5.4.1) after the later occurrence of:
  - destruction of the CA Private Key; or
  - revocation or expiration of the CA certificate.
- Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1) after the revocation or expiration of the Subscriber Certificate;
- Any security event records (as set forth in Section 5.4.1) after the event occurred.

These may be made available to auditors upon request.

#### **5.4.4 Protection of Audit Log**

Audit logs shall be protected by a combination of physical and procedural security controls, this includes:

- The CA generates a message authentication code for each audit log file it keeps,
- The security of audits logs is maintained while these logs transit by the backup system and when these logs are archived,
- Only authorized roles can obtain access to systems where audit logs are stored and any attempts to tamper with audit logs can be tracked to the respective trusted operative personnel.

#### **5.4.5 Audit Log Backup Procedures**

The following rules apply for the backup of the Timestamping CA audit log:

- Backup media shall be stored locally in DESC's main site in a secure location,
- A second copy of the audit log data and files shall be stored outside DESC's main site, in a site that provides similar physical and environmental security as the main site.

#### **5.4.6 Audit Collection System (Internal vs. External)**

Automatic audit processes are initiated at system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, DESC determines whether to suspend the CA's or RA's operations until the problem is fixed.

### **5.4.7 Notification to Event-Causing Subject**

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device or application that caused the event.

### **5.4.8 Vulnerability Assessments**

DESC conducts an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes,
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes, and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that DESC has in place to counter such threats.

DESC also performs regular vulnerability assessment and penetration testing covering the Dubai PKI systems. Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration, or destruction of the certificate issuance process. Evidence of the vulnerability assessment and penetration testing activities' execution are collected and archived by the Dubai PKI PA Information Security function.

## **5.5 Records Archival**

### **5.5.1 Types of Records Archived**

DESC archives the audit logs set forth in Section 5.4.1, in addition to the following:

1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, and Root CA Systems; and
2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

### **5.5.2 Retention Period for Archive**

DESC retains audit logs (as set forth in Section 5.4.1) and records (as set forth in Section 5.5.1) for 7 years after any certificate based on that documentation/logs ceases to be valid.

### **5.5.3 Protection of Archive**

Records are archived in such a way that they cannot be deleted or destroyed. Controls are in place to ensure that only authorized personnel are able to manage the archive without modifying integrity, authenticity and confidentiality of the contained records.

### **5.5.4 Archive Backup Procedures**

The PKI operations team use backup, restore and archive procedures that document how the archive information is created, transmitted and stored.

### **5.5.5 Requirements for Time stamping of Records**

All recorded events include the date and time of when the event took place, based on the time of the operating system. Procedures are in place to ensure that all systems rely on and are synchronized with a trusted time source.

### **5.5.6 Archive Collection System (Internal or External)**

Only authorized and authenticated staff is allowed to handle archived material.

### **5.5.7 Procedures to Obtain and Verify Archive Information**

Only DESC staff members with a clear hierarchical control and a definite job description may obtain and verify archived information. DESC retains records in electronic or paper-based format.

## **5.6 Key Changeover**

To minimize impact of key compromise, Timestamping CA private key is periodically changed over as specified in section 6.3.2.

To support revocation management of issued certificate, the old CA private keys are maintained until such time as all relying certificates have expired.

## **5.7 Compromise and Disaster Recovery**

### **5.7.1 Incident and Compromise Handling Procedures**

If DESC detects a potential hacking attempt or other form of compromise to the CA, it shall perform an investigation to determine the nature and the degree of damage. If the CA Private key is suspected of compromise, the procedures outlined in DESC's Business continuity and disaster recovery plan shall be followed. Otherwise, the scope of potential damage shall be assessed to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised. DESC also specifies applicable compromise reporting and relevant communications as part of the Business continuity and disaster recovery plan.

Apart from the circumstance of key compromise, DESC specifies the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

### **5.7.2 Computing Resources, Software Data Corruption**

Participants (other than Subscribers and Relying Parties), establish the necessary measures to ensure full recovery of Timestamping CA services in case of a disaster, and corrupted servers, software or data.

DESC establishes:

- Disaster recovery resources in a location sufficiently distant from the regular DESC Subordinate CAs operation facility,
- Fast communications between the two sites to ensure data integrity.

Disaster recovery infrastructure and procedures shall be fully tested at least once a year with the witnessing of more than one member of the Dubai PKI PA as the witness.



### **5.7.3 Entity Private Key Compromise Procedures**

For Subscribers key compromise, see Section 4.9 of the present CPS.

In the event of a key compromise of the Timestamping CA, or of the associated activation data, DESC triggers the Key compromise and CA termination plans detailed as part of DESC Business continuity and disaster recovery plan.

As part of the Key compromise and CA termination plan, the Dubai PKI PA will be invited for an emergency meeting to take decisions and handle communications as required with law enforcement authorities and other relevant stakeholders such as Root Programs and Relying Parties.

### **5.7.4 Business Continuity Capabilities After a Disaster**

DESC establishes the necessary measures to full and automatic recovery of the online services such as the OCSP and the public repository hosting CRLs in case of a disaster, in addition to corrupted servers, software or data.

DESC establishes the necessary measures to ensure full recovery of the offline services service in case of a disaster, and corrupted servers, software or data.

Failover scenarios to the disaster recovery location are made possible considering the policy in place for replicating backups to the disaster recovery site.

A **Business Continuity Plan** has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document. The business continuity plan includes the following:

1. Conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. Maintenance schedule for the plan,
6. Awareness and education requirements,
7. The responsibilities of the individuals,
8. Recovery time objective (RTO),
9. Regular testing of contingency plans,
10. Plan to maintain or restore the business operations in a timely manner following interruption to or failure of critical business processes,
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
12. What constitutes an acceptable system outage and recovery time,
13. How frequently backup copies of essential business information and software are taken,
14. The distance of recovery facilities to the main site,
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

## **5.8 CA or RA Termination**

***Certificate Practice Statement***

If DESC determines that termination of this CA services is deemed necessary, the CA termination plan shall be executed and it shall cover the following actions:

1. Minimize disruption caused by the termination of an Issuing CA is minimized as much as possible,
2. ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings. The retention of archived data specified in Section 5.5,
3. ensure Certificate status information services are maintained for the applicable period,
4. terminate all authorization of sub-contractors to act on behalf of the terminated service (Timestamping CA or RA) in the performance of any functions related to the process of issuing certificates,
5. notify subscribers, relying parties and other stakeholders (e.g. auditors and root programs). Notification procedures shall exist for informing affected entities and transferring archived CA records to an appropriate custodian.

# 6. Technical Security Controls

## 6.1 Key Pair Generation

The requirements for key generation and delivery are stated in the following sections.

### 6.1.1 Key Pair Generation

#### 6.1.1.1 CA Key Pair Generation

The Timestamping CA keys shall be generated as part of a key ceremony produced by the PA and executed under the supervision of the PA.

CA key pairs shall be generated within the memory of an HSM certified to the level required by this CA operation (at minimum FIPS 140-2 Level 3).

DESC ensures the implementation and documentation of key generation procedures in line with this CPS. It acknowledges public, international and WebTrust and CA/Browser Forum Guidelines on trustworthy systems, incorporating the following requirements:

- The key generation ceremony is subject to the formal authorization of the Dubai PKI PA,
- The key generation ceremony is conducted in presence of a combination of authorized personnel with trusted roles including the Dubai PKI PA representatives,
- The Timestamping CA Key Generation Ceremony is witnessed by DESC internal auditor,
- DESC ensures the distribution of the tokens giving access to the private key(s) to the trusted operatives and key custodians,
- DESC internal auditor then issues a report, covering that the Timestamping CA, during its Key Pair and Certificate generation process:
  - Documented its Timestamping CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement,
  - Included appropriate detail in its Timestamping CA Key Generation Script,
  - Maintained effective controls to provide reasonable assurance that the Timestamping CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Timestamping CA Key Generation Script,
  - Performed, during the Timestamping CA key generation process, all the procedures required by its Timestamping CA Key Generation Script.

A video of the entire key generation ceremony will be recorded and stored securely for auditing purposes.

### **6.1.1.2 Subscriber Key Pair Generation**

The Timestamping CA does not perform Subscriber key generation.

Subscribers shall generate their keys as per the below table:

<b>Certificate Type</b>	<b>Key generation requirements</b>
TSA certificates	Key generation is done using a dedicated TSA key management utility. The TSA key pair is generated inside the memory of a FIPS 140-1 level 3 hardware security module
OCSP certificates	Key generation is done using a dedicated OCSP key management utility. The OCSP key pair is generated inside the memory of a FIPS 140-1 level 3 hardware security module

### **6.1.2 Private Key Delivery to Subscriber**

Not applicable. The Timestamping CA does not perform Subscriber key generation.

### **6.1.3 Public Key Delivery to Certificate Issuer**

A subscriber generates his/her key pair then constitutes a PKCS#10 CSR that is submitted to DESC RA as part of the certificate request process through one of the following channels:

- Manually by the requester through e-mail or media exchange,
- Manually by the requester through the RA application exposed over a private network, or
- Automatically through key management protocols (e.g., XKMS, PKIX CMP and SCEP).

### **6.1.4 CA Public Key Delivery to Relying Parties**

The Timestamping CA makes its certificates available to Subscribers and relying parties by publishing them in a public repository (<https://ca-repository.desc.gov.ae/>).

### **6.1.5 Key Sizes**

This Timestamping CA key pair is 4096-bit RSA.

The Subscriber key pair must be at least 2048-bit RSA, recommended 4096-bit RSA or at least 256-bit ECDSA, recommended 384-bit ECDSA.

DESC RA rejects a certificate request if the requested public key does not meet the requirements set forth in this Section.

### **6.1.6 Public Key Parameters Generation and Quality Checking**

#### **6.1.6.1 Timestamping CA**

The Timestamping CA relies on off-the-shelf implementation of key PKI functionality including public key parameters generations. Timestamping CA HSMs and associated software meet FIPS 186-2 requirements for random generation and primality checks, they also meet the Baseline Requirements Section 6.1.6 on quality checking.

### 6.1.6.2 Subscribers

DESC RA uses reasonable techniques to validate the suitability of public keys presented by Subscribers. Known weak keys are tested for and rejected as described in the CA/Browser Forum Baseline Requirements section 6.1.6.

DESC RA rejects a certificate request if the requested public key does not meet the requirements set forth in this Section.

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

The certificates will always contain a key usage bit string in accordance with RFC 5280. The below tables elaborate further on the key usage of the CA certificate and the end-entity certificates issued by this CA.

#### 6.1.7.1 Timestamping CA Certificate

##### CA Signing

CA signing keys are the only keys permitted to be used for signing Certificates and CRLs.

The Certificate Key Usage field must be set to: Key Cert Sign and cRL Sign.

**Table 1:** Timestamping CA Key Usage

#### 6.1.7.2 Subscribers

Certificates issued to subscribers contain a key usage extension depending on their intended usage in accordance with RFC 5280. Refer to section 7.1 and 7.3 of this CPS.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic Module Standards and Controls

DESC generates the CAs' key pairs and store their private keys within a Cryptographic Device that is certified according to the rating specified in 6.2.11.

The Cryptographic modules used for Subscribers' key generation and storage are at least compliant to FIPS 140-2 Level 2.

### 6.2.2 Private key (n out of m) multi-person control

DESC implements technical and procedural mechanisms that implement the principles of multi-person control and split knowledge. These principles guarantee the participation of multiple trusted individuals for performing sensitive operations with CAs cryptographic hardware.

For offline HSMs, a certain number of persons 'm' (at least 2), out of 'n' persons (3 persons), the total number of key custodians, need to be present concurrently together with two (2) trusted operatives to activate or re-activate the HSM.

DESC keeps written, auditable, records of tokens and related password distribution to trusted operatives and key custodians. In case trusted operatives or key custodians are to be replaced, it keeps track of the renewed tokens and/or password distribution.

### **6.2.3 Private Key Escrow**

Not applicable.

### **6.2.4 Private Key Backup**

The Timestamping CA private key is backed up within backup HSMs that meet the same certification level as the Subordinate CA HSM and as described in Section 6.2.1. Backup operations are executed as part of the Timestamping CA key generation ceremonies. The Timestamping CA key is backed up under the same dual control and split knowledge as the primary key.

The Timestamping CA key backup is physically transported from the primary site to the DR site as part of the overall Timestamping CA key ceremony procedure.

Trusted operatives or key custodians participate in the transport operation, which is escorted by an auditor. The backup is to be stored in a locked safe at the disaster recovery site.

### **6.2.5 Private Key Archival**

No stipulation — this section is intentionally left blank.

### **6.2.6 Private Key Transfer Into or From a Cryptographic Module**

The Timestamping CA key shall only be transferred to another hardware cryptographic device, for backup purposes, of the same specification as described in 6.2.11 by direct token-to-token copy via trusted path under multi-person control. At no time should the CA private key be copied to disk or other media during this operation.

CA Key backups are generated with the enforcement of multi-person control and split knowledge mechanisms. The transfer of the CA Key backups to the DR site is subject to the same multi-person control and split knowledge principles.

### **6.2.7 Private Key Storage on Cryptographic Module**

No further stipulation other than those stated in sections 6.2.1, 6.2.2, 6.2.4 and 6.2.6.

### **6.2.8 Method of Activating Private Key**

#### **6.2.8.1 CA keys**

The Timestamping CA private keys remain under multi-person control. The Timestamping CA trusted operatives and key custodians are assigned with the task to activate and deactivate the Timestamping CA private keys.

The Timestamping CA keys that are stored on offline HSMs are activated only for defined time periods (during key ceremonies).

#### **6.2.8.2 Subscribers keys**

Subscribers are responsible for activating and protecting their private key according to the obligations articulated in the Subscriber Agreement.

### **6.2.9 Method of Deactivating Private Key**

For the CA private keys stored on online HSMs:

The Timestamping CA private Key is deactivated in the following situations:

- The CA HSM is manually switched off,
- There is a power failure within the CA facility,
- The CA HSM is operated outside the range of supported temperatures,
- The HSM detects a security breach and deletes all key material within its internal memory.

When private keys are deactivated, they are cleared from memory before the memory is de-allocated. Any disk space where keys were stored must be overwritten before the space is released to the operating system.

For the CA private keys stored on offline HSMs:

The HSMs used for the Timestamping CA key ceremony are deactivated at the end of the ceremony which prevents any further use of the Timestamping CA private keys. This activity applies to the principles of multi-person control and split knowledge and shall always be witnessed by the relevant personnel (The Dubai PKI PA, auditor). The HSMs are safely powered off at the end of the ceremony, and all material used during the ceremony are stored inside dedicated safes inside the secure enclave.

### **6.2.10 Method of Destroying Private Key**

At the end of their lifetime, taking into account business purpose and legal obligations, the Timestamping CA private keys shall be destroyed by multi-person presence, including at least one representative of the Dubai PKI PA, in order to ensure that these private keys cannot ever be retrieved and used again.

The key destruction process is documented in Cryptographic Devices Lifecycle Management Policy and Procedure. Any associated records are archived.

The decision for private key destruction outside the context of the end of its lifetime needs to be authorized in writing by multiple members of the Dubai PKI PA. This decision includes the assignment of the personnel.

### **6.2.11 Cryptographic Module Rating**

#### **6.2.11.1 Timestamping CA**

The Timestamping CA uses a Cryptographic Device certified to FIPS 140-2 Level 3 or ISO 15408 Common Criteria (CC) EAL 4+ or above.

#### **6.2.11.2 Subscribers**

The Cryptographic modules used for Subscribers' key generation and storage are at least compliant to FIPS 140-2 Level 2.

## **6.3 Other Aspects of Key Pair Management**

### **6.3.1 Public Key Archival**

Refer to Section 5.5 of this CPS.

## 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

- The maximum operational period of the CA's key pair must be set for eight years
- The maximum operational period for a Subscriber's key pair must be five years

Key Certificate Type	Maximum Validity Period
Certification Authority Certificate and associated keys	Recommended 96 months, re-key at 37% lifetime, i.e., 36 months
Certificates for Subscribers and associated keys	Maximum operational period for a Subscriber's key pair must be 60 months

## 6.4 Activation Data

### 6.4.1 Activation Data Generation and Installation

#### 6.4.1.1 Timestamping CA

DESC ensures that activation data associated to the Timestamping CA private keys and operations are securely generated, managed, stored and archived as described in the relevant sub-section of Sections 6.1 and 6.2.

During the Key Generation ceremony of the Timestamping CA, trusted individuals (key custodians) are instructed to use strong passwords and PINs. A password policy, that meet the requirements specified by the CAB Forums Network Security Requirements, is distributed to the trusted roles as part of the key ceremony documentation.

#### 6.4.1.2 Subscribers

Subscribers shall set and protect the activation data for their private keys to the extent necessary to prevent the loss, theft, unauthorized disclosure and use of these private keys. Such obligation is articulated as part of the Subscriber Agreement.

### 6.4.2 Activation Data Protection

#### 6.4.2.1 Timestamping CA

The Timestamping CA activation data consists of PINs, passwords and accounts that are used to activate the HSMs hosting the CA keys. Activation data is protected by same security controls used for the CA private key protection. A combination of physical security, technical and procedural controls ensure that the CA private keys and activation data is always protected. Refer to section 6.2 of this CPS for further details.

#### 6.4.2.2 Subscribers

Refer to section 6.4.1.2 of this CPS.

### 6.4.3 Other Aspects of Activation Data

No stipulation — this section is intentionally left blank.



## **6.5 Computer Security Controls**

The Timestamping CA performs all CA and RA functions using trustworthy systems that meet DESC security in addition to the present requirements.

### **6.5.1 Specific Computer Security Technical Requirements**

The Timestamping CA shall be operated according to the following security controls:

- Physical access control to the CA servers shall be enforced,
- Separation of duties and dual controls for CA-sensitive operations,
- Identification and authentication of PKI roles and their associated identities,
- Archival of CA's history and audit data,
- Audit of security related events,
- Automatic and regular validation of the CA systems' integrity,
- Recovery mechanisms for keys and CA systems,
- Hardening CA servers operating system according to best practices and PKI vendor requirements,
- Network protection, including intrusion detection systems (where applicable),
- Proactive patch management for the CA systems,
- Multi-factor authentication for all accounts capable of directly causing certificate issuance.

### **6.5.2 Computer Security Rating**

No stipulation — this section intentionally left blank.

## **6.6 Life Cycle Technical Controls**

### **6.6.1 System Development Controls**

Purchased hardware or software shall be shipped or delivered in a sealed, tamper-proof container and be installed by trained and trusted personnel. Hardware and software updates shall be handled in the same manner as the original equipment.

The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operations.

The CA hardware or software shall be tested, deployed and configured in accordance with industry best practices and vendor recommendations. All changes are controlled through the Dubai PKI change management processes. For offline systems, changes are done as part of a formal ceremony approved and planned by the Dubai PKI PA.

### **6.6.2 Security Management Controls**

The hardware and software used to set up the Dubai PKI shall be dedicated to performing only CA-related tasks. There shall be no other applications, hardware devices, network connections or component software, which are not part of the Dubai PKI, connected to or installed on CA hardware.

### ***Certificate Practice Statement***

A change management process is enforced to ensure that the CA systems configuration, modification and upgrades are documented and controlled by the PKI operations management. For the offline deployment, changes are done as part of a formal ceremony approved and planned by the Dubai PKI PA.

A vulnerability management process is enforced to ensure that the CA systems are scanned for malicious code on first use and periodically thereafter. The vulnerability management process supports the processing within 96 hours of discovery of critical vulnerabilities not previously met by the PKI operations team. For offline systems, equipment is scanned for malicious code on first use and periodically thereafter. Authorized personnel must ensure up-to-date virus definition databases is applied as needed on those systems.

#### **6.6.3 Life Cycle Security Controls**

No stipulation — this section is intentionally left blank.

## **6.7 Network Security Controls**

DESC ensures maintenance of network security, including managed firewalls and intrusion detection systems.

The network is segmented into several zones, based on their functional, logical and physical relationship. Network boundaries are applied to limit the communication between systems (within zones) and communication between zones, with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations, disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

Issuing Systems, Certificate Management Systems, and Security Support Systems are maintained and protected in a highly secure network zone.

Offline systems are kept in an offline state, located in a high security zone inside a secure safe within DESC secure premises.

## **6.8 Time Stamping**

Online CA systems' internal clock shall be synchronized using the NTP. Offline systems rely on its internal clock for time-stamping the archive records as required by section 5.5.5 of the present CPS in the context of "audit logging procedures" and any purposes or activities for which time is a critical element. Whenever offline systems are powered on during operational ceremonies, local time should be checked, and updated if necessary to ensure continuous time accuracy.

# 7. Certificate, CRL and OCSP Profiles

## 7.1 Certificate Profile

The Timestamping CA meets the technical requirements set forth in Section 2.2 – Publication of Information, Section 6.1.5 – Key Sizes, and Section 6.1.6 – Public Key Parameters Generation and Quality Checking of the CA/Browser Baseline Requirements.

The Timestamping CA generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

### 7.1.1 Version Number

This CA issues X.509 version 3 certificates as defined in RFC 5280.

### 7.1.2 Certificate Extensions

X.509 v3 extensions are supported and used in alignment with the CA/B Forum Baseline Requirements section 7.1. Refer to section 7.1.10 of this CPS for the details of the contents of the certificates issued by the Timestamping CA.

### 7.1.3 Algorithm Object Identifiers

X.509v3 standard OIDs is used. Algorithm must be RSA encryption for the subject key and SHA256withRSA encryption for the certificate signature.

### 7.1.4 Name Forms

As per the naming conventions and constraints listed in Section 3.1.1 of this CPS, that is followed while defining the certificate profiles in section 7.1.10 of this CPS.

The certificate subject attributes shall not contain values as meta data of period, hyphen, empty space, etc (Eg: '.' OR '-' OR ' ') indicating the attribute as blank or not applicable.

### 7.1.5 Name Constraints

Name constraints extension is not supported.

### 7.1.6 Certificate Policy Object Identifier

The Timestamping CA uses certificate policy object identifiers that are defined as part of OID scheme for the Dubai PKI. Refer to section 7.1.10 of this CPS for the profiles of the certificates issued by the Timestamping CA including the values of the OID identifiers.

### 7.1.7 Usage of Policy Constraints Extension

Policy constraints extension is not supported.

### 7.1.8 Policy Qualifiers Syntax and Semantics

The use of policy qualifiers as per the RFC 5280 is supported. Refer to section 7.1.10 of this CPS for the profiles of the certificates issued by the Timestamping CA including the used policy qualifiers.

### 7.1.9 Processing Semantics for Critical Certificate Extensions

Processing of certificate policies extensions shall conform with the RFC 5280.

### 7.1.10 Timestamping Certificate Profile

This is the complete ASN1 description of the certificate associated to TSA signing private keys. DESC rekeys its Timestamping Certificate every maximum period of 15 months.

Field	CE <sup>1</sup>	O/M <sup>2</sup>	CO <sup>3</sup>	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2 of RFC 3280
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Timestamping CA Signature	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
certificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M	S		
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements".

<sup>1</sup> CE = Critical Extension.

<sup>2</sup> O/M: O = Optional, M = Mandatory.

<sup>3</sup> CO = Content: S = Static, D = Dynamic

*Dubai PKI - Timestamping CA  
Certificate Practice Statement*

					PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	PrintableString
commonName		M	S	Timestamping Certification Authority	PrintableString
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using Generalized Time
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + not more than <b>[60]</b> Months	
Subject	False	M			
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	DESC	PrintableString
localityName		M	S	Dubai	PrintableString
commonName		M	S	Dubai Timestamping Authority	PrintableString
Subject Public Key Info	False	M			
algorithm		M	S	RSA	
subjectPublicKey		M	S	Key length: 4096 bits (RSA)	
Extensions		M			
Authority Properties					
authorityKeyIdentifier	False	O			Mandatory in all certificates except for self-signed CA certificates
keyIdentifier		M	D	SHA-1 Hash of the Timestamping CA public key	When this extension is used, this field MUST be supported at minimum
authorityInfoAccess	False	M			

*Dubai PKI - Timestamping CA  
Certificate Practice Statement*

accessMethod		M	S	Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
accessLocation		M	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
accessMethod		O	S	Id-ad-2 2 id-ad-calssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
accessLocation		O	S	http://ca-repository.desc.gov.ae/certificate/TimestampingCA.crt	Timestamping CA Certificate download URL
<b>cRLDistributionPoints</b>	<b>False</b>	<b>O</b>			
distributionPoint		O	D	http://ca-repository.desc.gov.ae/CRL/Timestamping/TimestampingCA.crl	CRL download URL
<b>Subject Properties</b>					
<b>subjectKeyIdentifier</b>	<b>False</b>	<b>M</b>			
keyIdentifier		M	S	SHA-1 Hash	
<b>Key Usage Properties</b>					
<b>keyUsage</b>	<b>True</b>	<b>O</b>			
digitalSignature		M	S	True	
<b>extendedKeyUsage</b>	<b>True</b>	<b>M</b>			
timeStamping		M	S	True	
<b>Certificate Policy Property</b>					
<b>certificatePolicies</b>	<b>False</b>	<b>M</b>			
policyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.3	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	D	URL location of Timestamping CA's CPS	

	certificatePolicies	False	M			
	policyIdentifier		M	S	2.16.784.1.2.2.100.1.3.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of the TSA practice disclosure statement	
	certificatePolicies	False	M			
	policyIdentifier		M	S	2.23.140.1.4.2	Timestamping Certificates issued in compliance with the Code Signing Baseline Requirements

## 7.2 CRL Profile

### 7.2.1 Version Number(s)

The version field in the certificate states 1, indicating X.509 v2 CRL.

### 7.2.2 CRL and CRL Entry Extensions

The CRL extensions contain the CRL Number (a sequential number incremented with each new CRL produced).

Please refer to section 7.2.3 below for the other supported extension in the CRLs issued by the Timestamping CA.

### 7.2.3 CRL ASN1 Description

This is the complete ASN1 description of the CRL certificate.

Field	CE <sup>4</sup>	CO <sup>5</sup>	Value	Comment
Certificate List				
TBSCertificate				
Signature	False			
algorithm		S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		D	Timestamping CA Signature	CA signature value
TBSCertList				

<sup>4</sup> CE = Critical Extension.

<sup>5</sup> CO = Content: S = Static, D = Dynamic

*Dubai PKI - Timestamping CA  
Certificate Practice Statement*

<b>Version</b>		False			
			S	2	Version 3
<b>Signature</b>		False			
	algorithm		S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
<b>Issuer</b>		False	S		
	countryName		S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". Printable String, size 2 (rfc5280)
	organizationName		S	UAE Government	Printable String
	commonName		S	Timestamping Certification Authority	Printable String
<b>Validity</b>		False			Implementations <b>MUST</b> specify using UTC time until 2049 from then on using Generalized Time
	ThisUpdate		D	CRL generation date/time	
	NextUpdate		D	CRL generation date/time + 6 months	
<b>Revoked Certificates</b>					
<b>certificate</b>					
	certificateSerial		D	Serial of the revoked certificate	
	revocationDate		D	Date & Time of revocation	
	invalidityDate		D	Date & Time on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid	
	reasonCode		D	Reason for the certificate revocation as per the RFC 5280	
<b>crlExtensions</b>					



authorityKeyIdentifier	False	D	This MUST be the same value as the subject Key Identifier field in the CRL Issuer's certificate.  Non-critical <subject key identifier CA>	SHA-1 Hash of the Timestamping CA public key
crlNumber	False	D	< Sequential CRL number >	
expiredCertsOnCRL (2.5.29.60)	False	D	< a date-time value specifies the date on or after which revoked certificates are retained on the CRL>	
Authority Information Access	False	S		
accessMethod	O	S	Id-ad-2 2 id-ad-caIssuers OID i.e., 1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
accessLocation	O	S	http://ca-repository.desc.gov.ae/certificate/TimestampingCA.crt	Timestamping CA Certificate download URL

## 7.3 OCSP Profile

### 7.3.1 Version Number(s)

The OCSP responder issues OCSP responses of version 1.

### 7.3.2 OCSP Extensions

No stipulation – this section intentionally left blank.

### 7.3.3 OCSP Response Signing Certificate ASN1 Description

This is the complete ASN1 description of the certificate associated to the OCSP response signing private key.

Field	CE <sup>6</sup>	O/M <sup>7</sup>	CO <sup>8</sup>	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2
Signature	False	M			
algorithm		M	S	OID =	SHA256 with RSA

<sup>6</sup> CE = Critical Extension.

<sup>7</sup> O/M: O = Optional, M = Mandatory.

<sup>8</sup> CO = Content: S = Static, D = Dynamic

*Dubai PKI - Timestamping CA  
Certificate Practice Statement*

				1.2.840.113549.1.1.11	Encryption
signatureValue		M	D	Timestamping CA Signature	CA signature value
<b>TBS Certificate</b>					
Version	False				
		M	S	2	Version 3
Serial Number	False				
certificateSerialNumber		M	D		At least 64 bits of entropy  Validated on duplicates
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M	S		
countryName		M	S	AE	Encoded according to “ISO 3166-1- alpha-2 code elements”. Printable String, size 2 (rfc5280)
organizationName		M	S	UAE Government	Printable String
CommonName		M	S	Timestamping Certification Authority	Printable String
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore			D	Certificate generation process date/time	
NotAfter			D	Certificate generation process date/time + not more than <b>[6]</b> Months	
Subject	False	M			
countryName		M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280)

*Dubai PKI - Timestamping CA  
Certificate Practice Statement*

localityName		M	S	Dubai	
organizationName		M	S	DESC	
commonName		M	S	Timestamping Certification Authority OCSP "C<n>"	"C<n>" is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
subjectPublicKeyInfo	False	M			
algorithm		M	S	RSA	
subjectPublicKey		M	D	Public key length: 2048 or 4096 (RSA)	
Extensions		M			
Authority Properties					
authorityKeyIdentifier	False	O			Mandatory in all certificates except for self-signed CA certificates
keyIdentifier		M	D	SHA-1 Hash of the Timestamping CA public key	When this extension is used, this field MUST be supported at minimum
Subject Properties					
subjectKeyIdentifier	False	M			
KeyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
nonrepudiation		M	S	True	
extendedKeyUsage	False	M			
OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M	S	05 00	
Certificate Policy Property					
certificatePolicies	False	M			

*Dubai PKI - Timestamping CA*  
*Certificate Practice Statement*

	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1. 2.1.3	
	policyQualifiers:policyQualifie rId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPS uri		O	D	URL location of Timestamping CA's CPS	

# 8. Compliance Audit and Other Assessments

## 8.1 Frequency or Circumstances of Assessment

DESC organizes an external WebTrust audit to ensure that it meets applicable requirements, standards, procedures, and service levels at least on an annual basis. DESC accepts this auditing of its own practices and procedures and will make the audit report publicly available no later than three months after the end of the audit period. The Dubai PKI PA evaluates the results of such audits before further implementing them.

DESC also perform an internal audit at least a quarterly basis against a randomly selected sample for monitor adherence and service quality. This internal audit is part of the Dubai PKI management cycle, and remediation for the audit findings is implemented by the CA operations team in a timely manner.

## 8.2 Identity and Qualifications of the Assessor

To carry out the audits, an independent auditor will be appointed, who will not be affiliated directly or indirectly in any way with DESC nor any person having any conflicting interests thereof.

These audits will be performed by qualified auditors who fulfill the following requirements:

- Independence from the subject of the audit,
- The ability to conduct an audit that addresses the WebTrust criteria specified in section 8.4,
- Employs individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function,
- Licensed by WebTrust,
- Bound by law, government regulation, or professional code of ethics,
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least US\$1m in coverage.

## 8.3 Assessor's Relationship to Assessed Party

The entity that performs the annual audit SHALL be completely independent of the CA.

## **8.4 Topics Covered by Assessment**

The Timestamping CA is audited for compliance to the following standards:

- WebTrust Principles and Criteria for Certification Authorities,
- WebTrust Principles and Criteria for Certification Authorities — Network Security,
- WebTrust Principles and Criteria for Certification Authorities — Publicly Trusted Code Signing Certificates.

## **8.5 Actions Taken as a Result of Deficiency**

Deficiencies identified by the auditor during the compliance audit will determine the actions to be taken. The Dubai PKI PA is responsible for ensuring that remediation actions are documented taken within an adequate timeframe corresponding to the significance of identified matters.

## **8.6 Communication of Results**

The results of the audit are reported to the Dubai PKI PA for analysis and resolution of findings. The results can also be made available to any other appropriate entities that may be entitled to a copy of the results by law, regulation, or agreement.

The external audit reports are published through the CA repository no later than three months after the end of the audit period..

# 9. Other Business and Legal Matters

Certain Legal conditions apply to the issuance of certificates issued by the Timestamping CA under this CPS as described in this section.

## 9.1 Fees

### 9.1.1 Certificate Issuance or Renewal Fees

Fee details will be provided at the time of certificate issuance.

### 9.1.2 Certificate Access Fees

Not Applicable.

### 9.1.3 Revocation or Status Information Access Fees

No fee will be charged for Certificate revocation or status information access.

### 9.1.4 Fees for Other Service

DESC may charge for other services depending on business needs and subject to the Dubai PKI PA approval.

### 9.1.5 Refund Policy

Charged fees cannot be refunded.

## 9.2 Financial Responsibility

### 9.2.1 Insurance Coverage

DESC ensures that this CA is covered by existing government insurance provisions. Details of coverage are specified in the applicable agreements.

### 9.2.2 Other Assets

DESC maintains sufficient financial resources to maintain operations and fulfill duties of this CA.

### 9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

## **9.3 Confidentiality of Business Information**

### **9.3.1 Scope of Confidential Information**

DESC considers the following as confidential information:

- Subscriber's personal information that are not part of certificates or CRLs issued by the Timestamping CA,
- Correspondence between the subscribers and DESC RA during the certificate management processing (including the collected subscribers data),
- Contractual agreements between DESC and its suppliers,
- The Dubai PKI internal documentation (technical documentation, operational processes, ....).

### **9.3.2 Information not within the scope of confidential information**

Any information not defined as confidential (refer to section 9.3.1) is deemed public. This includes the information published at the CA repository.

### **9.3.3 Responsibility to protect confidential information**

DESC guarantees the protection of confidential information according to the applicable laws on privacy.

## **9.4 Privacy of Personal Information**

### **9.4.1 Privacy plan**

DESC observes personal data privacy rules and confidentiality rules as described in this CPS. Refer to section 9.4.2 for the scope of private information.

Both private and non-private information can be subject to data privacy rules if the information contains personal data.

Only limited trusted personnel are permitted to access subscribed private information for the purpose of certificate lifecycle management.

DESC does not release any confidential information without the consent of the legitimate data owner or explicit authorization by a court order. When DESC releases private information, DESC ensures through reasonable means that this information is not used for any purpose apart from the requested purposes. Parties requesting and receiving confidential information are granted permission on the condition that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third-parties. Also, these parties are bound to observe personal data privacy rules in accordance with the UAE applicable laws.

DESC respects all applicable privacy, confidential information, and trade secret laws and regulations, as well as its published privacy policy in the collection, use, retention and disclosure of non-public information.

All communications channels with DESC/RA shall preserve the privacy and confidentiality of any exchanged private information. Data encryption shall be used when electronic communication channels are used with the Timestamping CA systems. This shall include:



- The communications link between the Timestamping CA and the RA,
- Sessions to deliver certificates and certificate status information.

### **9.4.2 Information treated as Private**

All personal information that is not publicly available in the content of a certificate or CRL are considered as private information.

### **9.4.3 Information not Deemed Private**

Information included in the certificate or CRL is not considered as private.

### **9.4.4 Responsibility to protect private information**

DESC employees, suppliers and contractors handle personal information in strict confidence under DESC contractual obligations that at least as protective as the terms specified in section 9.4.1.

## **9.5 Intellectual Property Rights**

DESC owns and reserves all intellectual property rights associated with its own databases, web sites, the Timestamping CA digital certificates and any other publication whatsoever originating from the Timestamping CA, including this CPS.

When DESC uses software from suppliers, it is possible that this software remains intellectual property of the supplier. This is defined in the license agreement of contract of this supplier.

## **9.6 Representations and Warranties**

### **9.6.1 CA Representations and Warranties**

By issuing a Certificate, the Dubai PKI CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

- The Subscriber that is a party to the Subscriber Agreement,
- All Application Software Suppliers with whom the Dubai PKI Root CA will enter into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier,
- and all Relying Parties who reasonably rely on a Valid Certificate.

DESC represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the Timestamping CA has complied with the Baseline Requirements and its CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

- **Compliance:** The Timestamping CA has complied with the Baseline Requirements for Code Signing and the applicable Certificate Policy and Certification Practice Statement in issuing each Timestamp Certificate and operating its PKI;
- **Identity of Subscriber:** At the time of issuance, the Timestamping CA represents that it (i) operated a procedure for verifying the identity of the Subscriber that at least meets the requirements in Section 3.2 of this document, (ii) followed the procedure when issuing or managing the Certificate, and (iii) accurately described the same procedure in the applicable Certificate Policy or Certification Practice Statement;

- **Authorization for Certificate:** That, at the time of issuance, the Timestamping CA
  - I. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject,
  - II. followed the procedure when issuing the Certificate, and
  - III. accurately described the procedure in this CPS.
- **Accuracy of Information:** That, at the time of issuance, the Timestamping CA
  - I. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate,
  - II. followed the procedure when issuing the Certificate, and
  - III. accurately described the procedure in this CPS.
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the Timestamping CA
  - I. implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2,
  - II. followed the procedure when issuing the Certificate,
  - III. accurately described the procedure in this CPS.
- **Subscriber Agreement:** That, if the Timestamping CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use.
- **Status:** That the Timestamping CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates.
- **Revocation:** That the Timestamping CA will revoke the Certificate for any of the reasons specified in these Requirements.

### **9.6.2 RA Representations and Warranties**

DESC RA warrant that it performs registration functions as per the stipulations specified in the applicable CP and this CPS.

### **9.6.3 Subscriber Representations and Warranties**

DESC requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant makes the commitments and warranties in this section for the benefit of the Timestamping CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, DESC shall obtain, for its express benefit and the Certificate Beneficiaries, either:

- The Applicant's agreement to the Subscriber Agreement with DESC, or
- The Applicant's acknowledgement of the Terms of Use.

DESC implements a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the certificate request. A separate Agreement is used for each certificate request.

***Certificate Practice Statement***

The Subscriber Agreement or Terms of Use contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

- **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to DESC, both in the certificate request and as otherwise requested by DESC in connection with the issuance of the Certificate(s) to be supplied by the Timestamping CA,
- **Protection of Private Key:** Applicant shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g., password or token. Subscriber represents that it will generate and operate any device storing private keys in a secure manner. Subscriber shall use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys,
- **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy,
- **Use of Certificate:** When TLS server certificates are requested, an obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use,
- **Reporting and Revocation:** An obligation and warranty to:
  - promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
  - promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
- **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- **Responsiveness:** An obligation to respond to DESC's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance:** An acknowledgment and acceptance that DESC is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by this CPS, or the Baseline Requirements.

#### **9.6.4 Relying Party Representations and Warranties**

Relying Parties who rely upon the certificates issued under the Timestamping CA shall:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension),
- Verify the Validity by ensuring that the Certificate has not Expired,
- Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment,

### ***Certificate Practice Statement***

- Ensure that the Certificate has not been revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon, and
- Determine that such Certificate provides adequate assurances for its intended use.

#### **9.6.5 Representations and Warranties of Other Participants**

No stipulation.

## **9.7 Disclaimers of Warranties**

Within the limitations of the laws in Dubai, DESC cannot be held liable (except in case of fraud or deliberate abuse) for:

- Profit loss,
- Loss of data,
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificate or digital signatures,
- Any liability incurred in any case if the error in such verified information is the result of fraud or willful misconduct of the applicant or if it is the result of negligence or with intent to deceive DESC, the Timestamping CA, or any person receiving or relying on the certificate,
- Any liability incurred as a result of the applicant breaking any laws applicable in Dubai, including those related to intellectual property protection, viruses, accessing computer systems, etc.
- Other damage.

## **9.8 Limitations of Liability**

The Timestamping CA does not offer any guarantees or warranties or enter into agreements that could be the subject of performance penalties, that could lead to legal actions on behalf of Subscribers or relying parties.

## **9.9 Indemnities**

Not applicable.

## **9.10 Term and Termination**

### **9.10.1 Term**

This CPS remains in force until notice of the opposite is communicated by DESC on its document repository (see Chapter 2 “Publication and Repository Responsibilities”).

### **9.10.2 Termination**

Amendments to this document are applied and approved by the Dubai PKI PA and marked by an indicated new version of the document. Upon publishing on the Timestamping CA repository, the

newer version becomes effective. The older versions of this document are also archived on the Timestamping CA repository.

### **9.10.3 Effect of Termination and Survival**

The Dubai PKI PA will communicate the conditions and effect of this CPS termination via appropriate mechanisms.

## **9.11 Individual Notices and Communications with Participants**

Notices related to this CPS can be addressed to the Dubai PKI PA contact address as stated in section 1.5.

## **9.12 Amendments**

### **9.12.1 Procedure for Amendment**

When changes are required to be done on this CPS. The Dubai PKI PA will incorporate any such change into a new version of this document and, upon approval, publish the new version. The new document will carry a new version number.

### **9.12.2 Notification Mechanism and Period**

The Dubai PKI PA reserve the right to amend this CPS without notification for amendments that are not material, including without limitation corrections of typographical errors or minor enhancements. The decision to designate amendments as material or non-material shall be at the Dubai PKI PA sole discretion.

### **9.12.3 Circumstances Under Which OID Must be Changed**

Major changes to this CPS that may materially change the acceptability of certificates for specific purposes, may require corresponding changes to the OID or qualifier (URL).

## **9.13 Dispute Resolution Procedures**

Any dispute arising out of or related to the digital certificates issued by the Dubai PKI shall be first addressed to the Dubai PKI PA. If mediation is not successful, then the dispute will be escalated to the relevant court in Dubai.

## **9.14 Governing Law**

The laws of Dubai shall govern the enforceability, construction, interpretation and validity of the present CPS.

## **9.15 Compliance with Applicable Law**

The present CPS and provision of Timestamping CA certification services are compliant to relevant, and applicable laws in Dubai.

## **9.16 Miscellaneous Provisions**

### **9.16.1 Entire Agreement**

No stipulation.

### **9.16.2 Assignment**

Except where specified by other contracts, no party may assign or delegate rights or duties under this CPS, without the prior written consent of DESC.

### **9.16.3 Severability**

In the event of a conflict between the Baseline Requirements and any regulation in Dubai, DESC may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Dubai. This applies only to operations or certificate issuances that are subject to that Law. In such event, DESC will immediately (and prior to issuing a certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification of the Baseline Requirements under this section, and the specific modification to the Baseline Requirements implemented by DESC. DESC will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS. Any modification to DESC practice enabled under this section will be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CPS and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

### **9.16.4 Enforcement (Attorney Fees/Waiver of Rights)**

No stipulation.

### **9.16.5 Force Majeure**

DESC shall not be liable for any failure or delay in their performance under the provisions of this CPS due to causes that are beyond their reasonable control, including, but not limited to unavailability of interruption or delay in telecommunications services.

## **9.17 Other Provisions**

Not applicable.