Dark Matter L.L.C.

DarkMatter Certification Authority

Certification Practice Statement

V1.8

October 2018
Signature Page

Chair, DarkMatter PKI Policy Authority

Date
## Document History

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Document Date</th>
<th>Revision Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAFT</td>
<td>May, 2016</td>
<td>First draft of the CPS</td>
</tr>
<tr>
<td>1.0</td>
<td>September, 2016</td>
<td>Initial version focused on Root</td>
</tr>
<tr>
<td>1.2</td>
<td>May 10, 2017</td>
<td>Initial version approved by the DMPPA</td>
</tr>
<tr>
<td>1.5</td>
<td>June 6, 2017</td>
<td>Updates based on IGTF and WebTrust audit reviews</td>
</tr>
<tr>
<td>1.6</td>
<td>July 10, 2018</td>
<td>Updates following annual review, maintain alignment with CABF BRs.</td>
</tr>
<tr>
<td>1.7</td>
<td>September 30, 2018</td>
<td>Updates following Mozilla feedback</td>
</tr>
<tr>
<td>1.8</td>
<td>October 17, 2018</td>
<td>Adding new Client CAs, updated OIDs</td>
</tr>
</tbody>
</table>
References

RFC 5280  Internet X.509 Public Key Infrastructure - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 6960  Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol – OCSP
RFC 2616  Hypertext Transfer Protocol -- HTTP/1.1
UAE Information Assurance Standards  The UAE Information Assurance Standards v1.0
Secure Communication Policy  UAE National PKI Secure Communication Policy - v1.00
UAE Digital Certificate Interoperability Guidelines  TBD
Business Continuity Management Plan  Available only to restricted entities
Contents

1 Introduction ........................................................................................................................................... 15
  1.1 Overview......................................................................................................................................... 16
  1.2 Document Name and Identification................................................................................................. 16
  1.3 PKI Participants............................................................................................................................... 18
    1.3.1 Certification Authorities ........................................................................................................... 19
    1.3.2 Registration Authorities ........................................................................................................... 20
    1.3.3 Subscribers ............................................................................................................................... 20
    1.3.4 Relying Parties ......................................................................................................................... 20
    1.3.5 Controller of Certifying Authorities for UAENRCA ................................................................. 21
    1.3.6 Accrediting Authorities ............................................................................................................ 21
  1.4 Certificate Usage ............................................................................................................................. 22
    1.4.1 Appropriate Certificate Uses .................................................................................................. 22
    1.4.2 Prohibited Certificate Uses .................................................................................................... 24
  1.5 Policy Administration ...................................................................................................................... 24
    1.5.1 Organization Administering the Document .............................................................................. 24
    1.5.2 Contact Person ......................................................................................................................... 24
    1.5.3 Person Determining CPS Suitability for the Policy ................................................................. 24
    1.5.4 CPS Approval Procedures ........................................................................................................ 25
  1.6 Definitions and Acronyms .............................................................................................................. 25

2 Publication and Repository Responsibilities ....................................................................................... 25
  2.1 Repositories .................................................................................................................................... 25
  2.2 Publication of Certification Information .......................................................................................... 26
    2.2.1 Publication of Certificates and Certificate Status .................................................................. 26
    2.2.2 Publication of CA Information ................................................................................................ 26
  2.3 Time or Frequency of Publication ................................................................................................... 26
  2.4 Access Controls on Repositories .................................................................................................... 26

3 Identification and Authentication .......................................................................................................... 27
  3.1 Naming ............................................................................................................................................ 27
    3.1.1 Types of Names ....................................................................................................................... 27
3.1.2 Need for Names to be Meaningful ................................................................. 27
3.1.3 Anonymity or Pseudonymity of Subscribers .................................................. 27
3.1.4 Rules for Interpreting Various Name Forms .................................................. 27
3.1.5 Uniqueness of Names .................................................................................... 28
3.1.6 Recognition, Authentication, and Role of Trademarks .................................... 28
3.2 Initial Identity Validation .................................................................................... 28
3.2.1 Method to Prove Possession of Private Key .................................................... 28
3.2.2 Authentication of Organization Identity .......................................................... 29
3.2.3 Authentication of Individual Identity ............................................................... 30
3.2.4 Non-Verified Subscriber Information ............................................................ 30
3.2.5 Validation of Authority .................................................................................. 34
3.2.6 Criteria for Interoperation ............................................................................ 35
3.3 Identification and Authentication for Re-Key Requests ........................................ 35
3.3.1 Identification and Authentication for Routine Re-Key .................................. 36
3.3.2 Identification and Authentication for Re-Key after Revocation ....................... 36
3.4 Identification and Authentication for Revocation Request .................................... 37
4 Certificate Life-Cycle Operational Requirements .................................................. 37
4.1 Certificate Application ....................................................................................... 37
4.1.1 Who can Submit a Certificate Application ..................................................... 38
4.1.2 Enrollment Process and Responsibilities ....................................................... 38
4.2 Certificate Application Processing ..................................................................... 38
4.2.1 Performing Identification and Authentication Functions .............................. 38
4.2.2 Approval or Rejection of Certificate Applications ......................................... 39
4.2.3 Time to Process Certificate Applications ..................................................... 40
4.3 Certificate Issuance ........................................................................................... 40
4.3.1 CA Actions During Certificate Issuance ....................................................... 40
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate .................... 40
4.4 Certificate Acceptance ...................................................................................... 40
4.4.1 Conduct Constituting Certificate Acceptance ................................................. 40
4.4.2 Publication of the Certificate by the CA ....................................................... 41
4.9.2 Who can Request Revocation ........................................................................................................ 45
4.9.3 Procedure for Revocation Request ............................................................................................ 45
4.9.4 Revocation Request Grace Period ............................................................................................... 46
4.9.5 Time Within which CA Must Process the Revocation Request .................................................. 46
4.9.6 Revocation Checking Requirement for Relying Parties ............................................................... 47
4.9.7 CRL Issuance Frequency (if applicable) ...................................................................................... 47
4.9.8 Maximum Latency for CRLs (if applicable) .................................................................................. 47
4.9.9 On-Line Revocation/Status Checking Availability ...................................................................... 47
4.9.10 On-Line Revocation Checking Requirements .......................................................................... 47
4.9.11 Other Forms of Revocation Advertisements Available .............................................................. 47
4.9.12 Special Requirements Key Compromise ................................................................................... 47
4.9.13 Circumstances for Suspension ................................................................................................. 48
4.9.14 Who can Request Suspension ................................................................................................ 48
4.9.15 Procedure for Suspension Request .......................................................................................... 48
4.9.16 Limits on Suspension Period .................................................................................................... 48
4.10 Certificate Status Services .......................................................................................................... 48
4.10.1 Operational Characteristics ...................................................................................................... 48
4.10.2 Service Availability .................................................................................................................. 48
4.10.3 Optional Features .................................................................................................................... 48
4.11 End of Subscription ....................................................................................................................... 48
4.12 Key Escrow and Recovery ............................................................................................................ 48
4.12.1 Key Escrow and Recovery Policy and Practices ....................................................................... 48
4.12.2 Session Key Encapsulation and Recovery Policy and Practices ............................................. 49
5 Facility, Management and Operational Controls ............................................................................. 49
5.1 Physical Controls .......................................................................................................................... 50
5.1.1 Site Location and Construction ................................................................................................ 50
5.1.2 Physical Access ......................................................................................................................... 50
5.1.3 Power and Air Conditioning ..................................................................................................... 50
5.1.4 Water Exposures ...................................................................................................................... 51
5.1.5 Fire Prevention and Protection ................................................................................................ 51
5.1.6 Media Storage
5.1.7 Waste Disposal
5.1.8 Off-Site Backup

5.2 Procedural Controls
5.2.1 Trusted Roles
5.2.2 Number of Persons Required per Task
5.2.3 Identification and Authentication for Each Role
5.2.4 Roles Requiring Separation of Duties

5.3 Personnel Controls
5.3.1 Qualifications, Experience, and Clearance Requirements
5.3.2 Background Check Procedures
5.3.3 Training Requirements
5.3.4 Retraining Frequency and Requirements
5.3.5 Job Rotation Frequency and Sequence
5.3.6 Sanctions for Unauthorized Actions
5.3.7 Independent Contractor Requirements
5.3.8 Documentation Supplied to Personnel

5.4 Audit Logging Procedures
5.4.1 Types of Events Recorded
5.4.2 Frequency of Processing Log
5.4.3 Retention Period for Audit Log
5.4.4 Protection of Audit Log
5.4.5 Audit Log Backup Procedures
5.4.6 Audit Collection System (Internal vs. External)
5.4.7 Notification to Event-Causing Subject
5.4.8 Vulnerability Assessments

5.5 Records Archival
5.5.1 Types of Records Archived
5.5.2 Retention Period for Archive
5.5.3 Protection of Archive
5.5.4 Archive Backup Procedures ................................................................. 61
5.5.5 Requirements for Time-Stamping of Records ...................................... 61
5.5.6 Archive Collection System (Internal or External) ................................... 61
5.5.7 Procedures to Obtain and Verify Archive Information ............................. 61
5.6 Key Changeover ..................................................................................... 61
5.7 Compromise and Disaster Recovery ......................................................... 62
  5.7.1 Incident and Compromise Handling Procedures ..................................... 62
  5.7.2 Computing Resources, Software, and/or Data are Corrupted .................. 62
  5.7.3 Entity Private Key Compromise Procedures ......................................... 62
  5.7.4 Business Continuity Capabilities after a Disaster ................................. 63
5.8 CA or RA Termination ............................................................................ 63

6 Technical Security Controls ........................................................................ 63
  6.1 Key Pair Security Controls ..................................................................... 63
  6.1.1 Key Pair Generation .......................................................................... 63
  6.1.2 Private Key Delivery to Subscriber ..................................................... 64
  6.1.3 Public Key Delivery to Certificate Issuer ............................................ 64
  6.1.4 CA Public Key Delivery to Relying Parties ......................................... 64
  6.1.5 Key Sizes ......................................................................................... 65
  6.1.6 Public Key Parameters Generation and Quality Checking ..................... 65
  6.1.7 Key Usage Purposes (as per X.509 v3 key usage field) .......................... 65
  6.2 Private Key Protection and Cryptographic Module Engineering Controls .. 65
  6.2.1 Cryptographic Module Standards and Controls .................................... 65
  6.2.2 Private Key \(n\) out of \(m\) Multi-Person Control ....................................... 66
  6.2.3 Private Key Escrow .......................................................................... 66
  6.2.4 Private Key Backup .......................................................................... 66
  6.2.5 Private Key Archival ......................................................................... 66
  6.2.6 Private Key Transfer into or from a Cryptographic Module .................... 66
  6.2.7 Private Key Storage on Cryptographic Module ..................................... 67
  6.2.8 Method of Activating Private Key ....................................................... 67
  6.2.9 Method of Deactivating Private Key .................................................... 67
6.2.10 Method of Destroying Private Key ................................................................. 67
6.2.11 Cryptographic Module Rating ........................................................................... 67
6.3 Other Aspects of Key Pair Management .............................................................. 67
  6.3.1 Public Key Archival ......................................................................................... 67
  6.3.2 Certificate Operational Periods and Key Pair Usage Periods ......................... 68
6.4 Activation Data ...................................................................................................... 68
  6.4.1 Activation Data Generation and Installation ................................................... 68
  6.4.2 Activation Data Protection .............................................................................. 68
  6.4.3 Other Aspects of Activation Data .................................................................... 69
6.5 Computer Security Controls ................................................................................ 69
  6.5.1 Specific Computer Security Technical Requirements ...................................... 69
  6.5.2 Computer Security Rating ............................................................................. 69
6.6 Life Cycle Technical Controls .............................................................................. 70
  6.6.1 System Development Controls ..................................................................... 70
  6.6.2 Security Management Controls .................................................................... 70
  6.6.3 Life Cycle Security Controls ........................................................................ 70
6.7 Network Security Controls .................................................................................. 71
6.8 Time-Stamping ...................................................................................................... 71

7 Certificate, CRL, and OCSP Profiles ..................................................................... 71
  7.1 Certificate Profile ............................................................................................... 71
    7.1.1 Version Number(s) ....................................................................................... 71
    7.1.2 Certificate Extensions .................................................................................. 71
    7.1.3 Algorithm Object Identifiers ....................................................................... 72
    7.1.4 Name Forms .................................................................................................. 72
    7.1.5 Name Constraints ......................................................................................... 72
    7.1.6 Certificate Policy Object Identifier .............................................................. 73
    7.1.7 Usage of Policy Constraints Extension ...................................................... 73
    7.1.8 Policy Qualifiers Syntax and Semantics ....................................................... 73
  7.2 CRL Profile .......................................................................................................... 73
7.2.1 Version Number(s) ........................................................................................................ 73
7.2.2 CRL and CRL Entry Extensions .................................................................................. 73
7.3 OCSP Profile ................................................................................................................... 73
  7.3.1 Version Number(s) .................................................................................................... 73
  7.3.2 OCSP Extensions .................................................................................................... 73
7.4 Lightweight Directory Access Protocol Profile ............................................................. 74
  7.4.1 Lightweight Directory Access Protocol Version Numbers ....................................... 74
  7.4.2 Lightweight Directory Access Protocol Extensions .................................................. 74
7.5 Digital Certificate Fields and Root CA Certificate Hashes ............................................ 74
  7.5.1 Digital Certificate Fields ........................................................................................ 74
  7.5.2 DarkMatter CA Certificate Hashes ....................................................................... 75

8 Compliance Audit and Other Assessments ............................................................................ 80
  8.1 Frequency or Circumstances of Assessment ................................................................. 80
  8.2 Identity/Qualifications of Assessor .............................................................................. 80
  8.3 Assessor’s Relationship to Assessed Entity ................................................................. 81
  8.4 Topics Covered by Assessment .................................................................................... 81
  8.5 Actions Taken as a Result of Deficiency ..................................................................... 81
  8.6 Communication of Results ......................................................................................... 82
  8.7 Self Audits ................................................................................................................... 82

9 Other Business and Legal Matters ....................................................................................... 82
  9.1 Fees ............................................................................................................................... 82
    9.1.1 Certificate Issuance or Renewal Fees .................................................................... 82
    9.1.2 Certificate Access Fees ....................................................................................... 82
    9.1.3 Revocation or Status Information Access Fees ................................................... 82
    9.1.4 Fees for Other Services ....................................................................................... 82
    9.1.5 Refund Policy ........................................................................................................ 82
  9.2 Financial Responsibility ................................................................................................. 82
    9.2.1 Insurance Coverage ............................................................................................ 83
    9.2.2 Other Assets ........................................................................................................ 83
    9.2.3 Insurance or Warranty Coverage for End-Entities ............................................... 83
9.3 Confidentiality of Business Information................................................................. 83
  9.3.1 Scope of Confidential Information ........................................................................ 83
  9.3.2 Information Not Within the Scope of Confidential Information ......................... 83
  9.3.3 Responsibility to Protect Confidential Information............................................... 83
9.4 Privacy of Personal Information.................................................................................. 84
  9.4.1 Privacy Plan .......................................................................................................... 84
  9.4.2 Information Treated as Private ............................................................................. 84
  9.4.3 Information not Deemed Private ........................................................................... 84
  9.4.4 Responsibility to Protect Private Information ....................................................... 84
  9.4.5 Notice and Consent to Use Private Information .................................................... 84
  9.4.6 Disclosure Pursuant to Judicial or Administrative Process ................................. 84
  9.4.7 Other Information Disclosure Circumstances ....................................................... 84
9.5 Intellectual Property Rights ....................................................................................... 84
9.6 Representations and Warranties ................................................................................ 85
  9.6.1 CA Representations and Warranties .................................................................... 85
  9.6.2 RA Representations and Warranties ................................................................... 85
  9.6.3 Subscriber Representations and Warranties ......................................................... 85
  9.6.4 Relying Party Representations and Warranties .................................................... 86
  9.6.5 Representations and Warranties of Other Participants ......................................... 86
9.7 Disclaimers of Warranties ......................................................................................... 86
9.8 Limitations of Liability .............................................................................................. 86
9.9 Indemnities ............................................................................................................. 86
9.10 Term and Termination .............................................................................................. 87
  9.10.1 Term .................................................................................................................... 87
  9.10.2 Termination ......................................................................................................... 87
  9.10.3 Effect of Termination and Survival ..................................................................... 87
9.11 Individual Notices and Communications with Participants ...................................... 87
9.12 Amendments .......................................................................................................... 87
  9.12.1 Procedure for Amendment ............................................................................... 87
  9.12.2 Notification Mechanism and Period ................................................................... 87
9.12.3 Circumstances Under Which OID Must be Changed ................................................................. 87
9.13 Dispute Resolution Provisions ........................................................................................................ 87
9.14 Governing Law .................................................................................................................................. 88
9.15 Compliance with Applicable Law ....................................................................................................... 88
9.16 Miscellaneous Provisions .................................................................................................................. 88
  9.16.1 Entire Agreement ......................................................................................................................... 88
  9.16.2 Assignment ................................................................................................................................. 88
  9.16.3 Severability .................................................................................................................................. 88
  9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) ................................................................. 88
  9.16.5 Force Majeure ............................................................................................................................. 88
9.17 Other Provisions .................................................................................................................................. 88
Annex A: Acronyms .................................................................................................................................... 89
Annex B: Definitions .................................................................................................................................... 90
1 Introduction

The UAE National Root Certification Authority (hereinafter, the UAENRCA) operates the core national PKI services, including a number of root Certification Authorities (hereinafter, CAs) for the UAE. The National Root CA is responsible for validating and signing digital certificates that are recognized as trusted issuers within the national PKI in order to establish and promote digital trust on a national scale. DarkMatter is the UAENRCA operator.

This DarkMatter Certification Practice Statement (hereinafter, CPS) applies to all certification services provided by DarkMatter in the context of the UAENRCA and any other PKIs authorized by the DarkMatter PKI Policy Authority (DMPPA). This CPS is consistent with the Internet Engineering Task Force (IETF) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, version November 2003 with regard to format and content recommendations. Minor editorial changes of [RFC 3647] structure have been inserted in this CPS to better adapt it for the needs of UAENRCA and other DarkMatter PKIs.

The aim of this CPS is to document the internal practices and procedures used by DarkMatter for certificate lifecycle services including issuance, certificate management (including publication and archiving), revocation, and renewal or re-keying in accordance with the UAE Certificate Policy (CP) and any other applicable CPs that DarkMatter is accredited under or operates in accordance with. In addition, this CPS covers the systems administration and the facilities management, which includes the DarkMatter repository functionality used to post CA digital certificates (referred to as certificates in this document), and certificate status issued by DarkMatter’s PKIs.

The scope of this CPS includes the UAENRCA that operates in compliance with X.509 Certificate Policy for [UAE National PKI Certificate Policy] and other approved DarkMatter PKI CPs. This CPS explicitly identifies all DarkMatter publicly trusted Root CAs and Issuing CAs (see Section 7.5.2) and covers all certificates issued and signed by these listed CAs. NOTE: None of the CAs listed in Section 7.5.2 are permitted to be or sign Bridge CAs.

A National PKI Policy Authority (NPPA) sets public policies governing the operation of all components of the National Public Key Infrastructure (PKI) and manages the operational components (Examples include Certification Authorities, Registration Authorities, repositories among others.) of the National PKI. The NPPA serves the interest of TRA, other UAE government entities, private organizations, and citizens and residents as Relying Parties within the National PKI. Other DarkMatter PKIs are governed and approved by the DMPPA. The DMPPA adopts any applicable NPPA policy updates as they are approved.

DarkMatter PKIs, including the UAE National PKI, conform to the current version of the guidelines adopted by the Certification Authority/Browser Forum (“CAB Forum”) when issuing publicly trusted certificates, including the Baseline Requirements for the Issuance and Management of Publicly- Trusted Certificates (“Baseline Requirements”) and the Guidelines for Extended Validation Certificates (“EV Guidelines”) both of which are published at https://www.cabforum.org. With regard to SSL/TLS Server Certificates or Code Signing Certificates, if any inconsistency exists between this CPS and the Baseline Requirements or the EV Guidelines, then the EV Guidelines take precedence for EV Certificates and the Baseline Requirements take precedence for publicly trusted SSL certificates. Time-stamping services are provided according to IETF RFC 3161 and other technical standards.
1.1 Overview
This CPS covers certificates issued by DarkMatter PKI trust anchors, including subordinate CAs to the UAENRCA trust anchors and any subordinate issuing CAs or the end entities that chain through these to the aforementioned trust anchors. The term “Entity” applies equally to government (federal and Emirate-level) organizations and other organizations owning or operating PKI domains (e.g., a bridge CA serving a community of interest).

This CPS is subject to a regular review process to reflect the changes in DarkMatter operations and practices considering the developments in international PKI standardization initiatives, development in technology and information security, as well as other relevant issues. Together with this CPS, other documents have to be taken into account. These documents are available through the DarkMatter repository at: http://ca.darkmatter.ae/CPS/

1.2 Document Name and Identification
This document is referred to as the DarkMatter CPS and incorporates the UAENRCA CPS. It is recognized under the following identifications:
- Title: DarkMatter Certification Authority Certification Practice Statement (CPS)
- Version: 1.0
- Object identifier (OID): 2.16.784.2.2.40.2.0.2.1

The OID for the UAE National PKI is joint-isoc-cctt (2) country (16) UAE (784) UAE-government (1) federal government (1) federal authorities (7) Agency (35) UAE National PKI (2). The OID for DarkMatter PKI related objects is joint-isoc-cctt (2) country (16) UAE (784) Commercial (2) Private (2) DarkMatter (40) PKI (2). The OID arcs for the various certificates and documents described in this CP are assigned under this arc as follows:

<table>
<thead>
<tr>
<th>Object Description</th>
<th>Object Identifier (OID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DarkMatter Certification Practice Statements</td>
<td>2.16.784.2.2.40.2.0.2</td>
</tr>
<tr>
<td>This CPS document</td>
<td>2.16.784.2.2.40.2.0.2.1</td>
</tr>
<tr>
<td>DarkMatter Levels of Assurance</td>
<td>2.16.784.2.2.40.2.1</td>
</tr>
<tr>
<td>DM LoA1</td>
<td>2.16.784.2.2.40.2.1.1</td>
</tr>
<tr>
<td>DM LoA2</td>
<td>2.16.784.2.2.40.2.1.2</td>
</tr>
<tr>
<td>DM LoA3</td>
<td>2.16.784.2.2.40.2.1.3</td>
</tr>
<tr>
<td>Certificate Profile</td>
<td>OID</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>DM LoA4</td>
<td>2.16.784.2.2.40.2.1.4</td>
</tr>
<tr>
<td>DarkMatter Certificate Profiles</td>
<td>2.16.784.2.2.40.2.2</td>
</tr>
<tr>
<td>DM TLS</td>
<td>2.16.784.2.2.40.2.2.1</td>
</tr>
<tr>
<td>DM EV</td>
<td>2.16.784.2.2.40.2.2.1.1</td>
</tr>
<tr>
<td>DM OV</td>
<td>2.16.784.2.2.40.2.2.1.2</td>
</tr>
<tr>
<td>DM Client</td>
<td>2.16.784.2.2.40.2.2.2</td>
</tr>
<tr>
<td>DM Authentication</td>
<td>2.16.784.2.2.40.2.2.2.1</td>
</tr>
<tr>
<td>DM SMIME Dual Use</td>
<td>2.16.784.2.2.40.2.2.2.2</td>
</tr>
<tr>
<td>DM SMIME Digital Signature</td>
<td>2.16.784.2.2.40.2.2.2.3</td>
</tr>
<tr>
<td>DM SMIME Encryption</td>
<td>2.16.784.2.2.40.2.2.2.4</td>
</tr>
<tr>
<td>DM SMIME Escrow Encryption</td>
<td>2.16.784.2.2.40.2.2.2.5</td>
</tr>
<tr>
<td>DM Device</td>
<td>2.16.784.2.2.40.2.2.6</td>
</tr>
<tr>
<td>DM HA Signer</td>
<td>2.16.784.2.2.40.2.2.7</td>
</tr>
<tr>
<td>DM Grid</td>
<td>2.16.784.2.2.40.2.2.3</td>
</tr>
<tr>
<td>DM Grid Host</td>
<td>2.16.784.2.2.40.2.2.3.1</td>
</tr>
<tr>
<td>DM Grid Client</td>
<td>2.16.784.2.2.40.2.2.3.2</td>
</tr>
<tr>
<td>DM Grid Robot</td>
<td>2.16.784.2.2.40.2.2.3.3</td>
</tr>
<tr>
<td>UAENRCA Certification Policy Documents</td>
<td>2.16.784.1.1.7.35.2.0.1</td>
</tr>
<tr>
<td>UAENRCA CP document</td>
<td>2.16.784.1.1.7.35.2.0.1.1.1</td>
</tr>
<tr>
<td>UAENRCA Levels of Assurance</td>
<td>2.16.784.1.1.7.35.2.1</td>
</tr>
<tr>
<td>UAENRCA LoA1</td>
<td>2.16.784.1.1.7.35.2.1.1</td>
</tr>
<tr>
<td>UAENRCA LoA2</td>
<td>2.16.784.1.1.7.35.2.1.2</td>
</tr>
<tr>
<td>UAENRCA LoA3</td>
<td>2.16.784.1.1.7.35.2.1.3</td>
</tr>
<tr>
<td>UAENRCA LoA4</td>
<td>2.16.784.1.1.7.35.2.1.4</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>UAENRCA Certificate Profiles</td>
<td>2.16.784.1.1.7.35.2.2</td>
</tr>
<tr>
<td>UAENRCA TLS Certificates</td>
<td>2.16.784.1.1.7.35.2.2.1</td>
</tr>
<tr>
<td>UAE EV TLS Certificates</td>
<td>2.16.784.1.1.7.35.2.2.1.1</td>
</tr>
<tr>
<td>UAE OV TLS Certificates</td>
<td>2.16.784.1.1.7.35.2.2.1.2</td>
</tr>
<tr>
<td>UAENRCA Client Certificates</td>
<td>2.16.784.1.1.7.35.2.2.2</td>
</tr>
<tr>
<td>UAE Authentication Certificate</td>
<td>2.16.784.1.1.7.35.2.2.2.1</td>
</tr>
<tr>
<td>UAE SMIME Dual Use</td>
<td>2.16.784.1.1.7.35.2.2.2.2</td>
</tr>
<tr>
<td>UAE SMIME Digital Signature</td>
<td>2.16.784.1.1.7.35.2.2.2.3</td>
</tr>
<tr>
<td>UAE SMIME Encryption</td>
<td>2.16.784.1.1.7.35.2.2.2.4</td>
</tr>
<tr>
<td>UAE SMIME Escrow Encryption</td>
<td>2.16.784.1.1.7.35.2.2.2.5</td>
</tr>
<tr>
<td>UAE Device</td>
<td>2.16.784.1.1.7.35.2.2.2.6</td>
</tr>
<tr>
<td>UAE Qualified Signer</td>
<td>2.16.784.1.1.7.35.2.2.2.7</td>
</tr>
<tr>
<td>UAENRCA Object Signing Certificates</td>
<td>2.16.784.1.1.7.35.2.2.3</td>
</tr>
<tr>
<td>UAE Code Signing</td>
<td>2.16.784.1.1.7.35.2.2.3.1</td>
</tr>
<tr>
<td>UAE EV Code Signing</td>
<td>2.16.784.1.1.7.35.2.2.3.2</td>
</tr>
<tr>
<td>UAE Document Signing</td>
<td>2.16.784.1.1.7.35.2.2.3.3</td>
</tr>
</tbody>
</table>

### 1.3 PKI Participants

In the UAE, six types of entities fill the roles of participants within the UAE National Public Key Infrastructure. The parties mentioned hereunder are collectively called PKI participants and include Certification Authorities, Registration Authorities, Subscribers, Relying Parties, Controller of Certification Authorities and the Market Regulator as illustrated in Figure 1. The following sections introduce the PKI participants involved in issuing and maintaining key management certificates. More details on specific roles within the PKI participants are described in detail in Section 5.2.
All communications among the participants within the PKI regarding any phase of the life cycle of certificates should be in compliance with [Secure Communication Policy]. This includes communications containing certificate requests, issuance, suspension, un-suspension and revocation.

### 1.3.1 Certification Authorities

Within a PKI, a Certification Authority (CA) is a trusted entity that performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and validating the certificates it issues. The Certification Authorities name appears as the issuer in a certificate.

The DarkMatter CA (which incorporates the UAENRCA) is a Certification Authority that operates a hierarchical model in which DarkMatter Root CAs issue certificates to Entity CAs requesting to become a subordinate CA or a bridge CA. A subordinate CA is an unaffiliated entity that is issued a CA Certificate by a Root CA (or possibility another subordinate CA) where the Private Key associated with that subordinate CA Certificate is not maintained under the control of Root CA. Subordinate CAs issue certificates to other subordinate CAs or to End Entities.
The set of DarkMatter CAs receive requests from the Entity CAs or End Entities, issues, revokes, renews CA’s certificates and End Entity certificates, and maintains CRLs and Online Certificate Status Protocol (OCSP) responses.

The UAENRCA operates within a grant of authority provided by the TRA. The DarkMatter CA is a Private entity.

### 1.3.2 Registration Authorities

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

The UAENRCA does not operate a separate Registration Authority; instead a registration function within the UAENRCA is established to fill in this role. The UAENRCA issues certificates only to Entity CAs requesting to become a subordinate CA. The UAENRCA collects and validates the authenticity of the Entity CA and the identity information about the CA organization including Point of Contact (POC) information for those individuals authorized to act on behalf of the CA in the certification process. The UAENRCA verifies the information to be included in the certificate, and validates that the individual representing the Entity CA matches the POC information in the Letter of Authorization (LOA) provided to UAENRCA.

DarkMatter CAs may operate a separate Registration Authority (RA); or the registration function may be contained within the CA function as is the case with the UAENRCA. DarkMatter CAs issue certificates not only to Entity CAs requesting to become a subordinate CA, but also to End Entities requesting leaf certificates. The DarkMatter RA collects and validates the authenticity of the certificate applicant and the identity information about any affiliated organizations that will be included in a certificate, including Point of Contact (POC) information for those individuals authorized to act on behalf of an organization in the certification process. The DarkMatter RA verifies the information to be included in the certificate, and validates that the individual representing an affiliated organization for a given certificate matches the POC information in the Letter of Authorization (LOA) provided to DarkMatter RA.

### 1.3.3 Subscribers

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

However, the term “Subscriber” as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

### 1.3.4 Relying Parties

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

This document makes no assumptions or limitations regarding the identity of Relying Parties. Relying Parties are not required to have an established relationship with the DarkMatter CA and are outside the scope of this document.

1.3.5 Controller of Certifying Authorities for UAENRCA

The Controller of Certifying Authorities is the custodian of the national CA strategy and is responsible for setting guidelines and monitoring CA activity to ensure adherence to national CA program strategic objectives.

The Controller of Certifying Authorities has the following responsibilities:

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

The Telecommunications Regulatory Authority (TRA) is the Controller of Certification Authorities operating under the UAE NPKI.

1.3.6 Accrediting Authorities

The DarkMatter CA may seek accreditation from various industry groups and trust federations. Specific accreditation controls may be detailed further beneath the relevant accrediting bodies included below.

1.3.6.1 CA and Browser Forum

DarkMatter PKIs conform to the current version of the guidelines adopted by the Certification Authority/Browser Forum ("CAB Forum") when issuing publicly trusted certificates, including the Baseline Requirements for the Issuance and Management of Publicly- Trusted Certificates ("Baseline Requirements") and the Guidelines for Extended Validation Certificates ("EV Guidelines") both of which are published at https://www.cabforum.org. With regard to SSL/TLS Server Certificates or Code Signing Certificates, if any inconsistency exists between DarkMatter's CPS and the Baseline Requirements or the EV Guidelines, then the
EV Guidelines take precedence for EV Certificates and the Baseline Requirements take precedence for publicly trusted SSL certificates.

The DMPPA reviews changes to published CAB Forum guidelines at least annually and more frequently when updated guidelines are published to ensure new requirements are incorporated into CP and CPS that DarkMatter uses in conjunction with any publicly trusted CA operations, in a timely manner.

1.3.6.2 IGTF

DarkMatter hereby grants to IGTF, the EUGridPMA, and all other accreditation authorities with whom DarkMatter has requested accreditation (“Accreditation Authority”) a non-exclusive, worldwide, transferable, sub-licenseable right to digitalize, reproduce, publish, distribute, and re-distribute DarkMatter’s Root CA Certificates, issued IGTF certificates, the metadata associated with DarkMatter’s Root and IGTF certificates, DarkMatter’s CP and CPS, and all other documents or information not marked confidential and either provided by DarkMatter or posted on DarkMatter’s website (“Documentation’). This license is provided without any fee or royalty obligations, provided that the Documentation is reproduced or distributed without modifying the Documentation’s contents, and Accreditation Authority attributes DarkMatter as the author and source of the Documentation.

DarkMatter retains, and the Accreditation Authorities may not obtain, any title, interest, and ownership rights in either (i) the Documentation and all copies or derivative works of the Documentation, regardless of who produced, requested, or suggested the copy or derivative work or (ii) all of DarkMatter’s copyrights, patent rights, trade secret rights and other proprietary rights.

Accreditation Authorities may not decompile or create derivative works of any Documentation without the prior written consent of DarkMatter.

This license lasts until revoked. DarkMatter may only revoke this license after sending notice of the revocation to the Accreditation Authority. Revocation is effective on the latter of 30 days after the notice is received by the Accreditation Authority and 30 days after the last IGTF certificate issued by DarkMatter expires.

1.4 Certificate Usage

A digital certificate (or certificate) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital certificate potentially allows an entity taking part in an electronic transaction to prove its identity to other participants in such transactions, depending on the data included in the certificate. A time stamp token (TST) cryptographically binds a representation of data to a particular time stamp, thus establishing evidence that the data existed at a certain point in time.

1.4.1 Appropriate Certificate Uses

The DarkMatter CA is intended to support applications involving information, which can include sensitive classified and unclassified data. Note that the data in such transactions never traverse the DarkMatter CA infrastructure.
The UAENRCA only issues certificates to CAs, and updates the status relating to those certificates.

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

This CPS covers several different types of end entity Certificates/tokens with varying levels of assurance. The following table provides a brief description of the appropriate uses of each. The descriptions are general and for guidance only and are not considered binding:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Appropriate Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>EV TLS Certificate</td>
<td>Used to secure online communication where risks and consequences of data compromise are highest, including transactions having significant monetary value, risk of fraud, or where involving access to private information where the likelihood of malicious access is significant.</td>
</tr>
<tr>
<td>OV TLS Certificate</td>
<td>Used to secure online communication where the risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.</td>
</tr>
<tr>
<td>Code Signing Certificates</td>
<td>Establishes the identity of the Subscriber named in the Certificate and that the signed code has not been modified since signing.</td>
</tr>
<tr>
<td>(including EV CS)</td>
<td></td>
</tr>
<tr>
<td>Client Certificate – Level 1</td>
<td>Provides the lowest degree of assurance concerning identity of the individual and is generally used only to provide data integrity to the information being protected. These Certificates should only be used where the risk of malicious activity is low and if an authenticated transaction is not required.</td>
</tr>
<tr>
<td>Client Certificate – Level 2</td>
<td>Issued to identity-vetted individuals. Certificates specify if the name is a pseudonym. Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.</td>
</tr>
<tr>
<td>Client Certificate – Level 3</td>
<td>Used in environments where risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.</td>
</tr>
<tr>
<td>Client Certificate – Level 4</td>
<td>Used in environments where risks and consequences of data compromise are high, including transactions having high monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is high.</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IETF and Grid Certificates</td>
<td>Support identity assertions and system authentication amongst participants in the Interoperable Global Trust Federation. IETF Certificates include those issued as publicly-trusted client Certificates and those issued under private trust hierarchies also.</td>
</tr>
</tbody>
</table>

1.4.2 **Prohibited Certificate Uses**

The UAENRCA does not directly issue certificates to Subscribers, and does not restrict the usage of certificates issued by any subordinate CA as long as it is in conformity with the subordinate CA CPS under which the UAENRCA issued the certificate.

DarkMatter CAs outside the UAENRCA scope do not have the above restrictions, they may issue certificates to Subscribers and End Entities, so long as they are conformant with the policies asserted in the certificate.

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

1.5 **Policy Administration**

1.5.1 **Organization Administering the Document**

The DMPPA is responsible for the development, publishing and amendment of this document.

1.5.2 **Contact Person**

Questions regarding this document shall be directed to:

DarkMatter PKI Policy Authority

DarkMatter PKI
Level 15 AlDdar HQ
PO Box 27655
Abu Dhabi, UAE
Phone: +971-800-DARKCERT (32752378) (UAE)
Email: CA-Admins@darkmatter.ae

1.5.3 **Person Determining CPS Suitability for the Policy**

The DMPPA is responsible for asserting whether this CPS conforms to the corresponding CA’s CP.
The determination of suitability may be based on an independent compliance auditor’s results and recommendations. Refer to Section 8 for further details.

1.5.4 CPS Approval Procedures
For the UAE National Root CA CPS approval procedure:
- The UAENRCA submits its CPS and the results of a compliance audit to TRA (the Controller of Certification Authorities) for approval
- TRA accepts or rejects the UAENRCA CPS and accompanying compliance audit
- If rejected, the UAENRCA is tasked to resolve the identified discrepancies.

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

For the DarkMatter Certification Authority CPS approval procedure:
- The DarkMatter CA submits its CPS and the results of a relevant compliance audit to the DMPPA or other accepted Accrediting Authority for approval
- The Accrediting Authority accepts or rejects the DarkMatter CPS and accompanying compliance audit
- If rejected, the DarkMatter CA is tasked to resolve the identified discrepancies
- The DMPPA publishes the CPS once all discrepancies are resolved and corresponding practices are updated in the CPS

1.6 Definitions and Acronyms
Refer to Annex A and Annex B.

2 Publication and Repository Responsibilities
2.1 Repositories
The DarkMatter CA sets up and maintains different types of repositories of all certificates it has issued, in addition to the status of these certificates. The repositories include:
- An internal Directory service, which allows access and retrieval of the certificate information including all certificates issued by the DarkMatter CA, as well as the CRLs maintained by the DarkMatter CA;
- An online server which allows anonymous access and retrieval of certificate information via HTTP and OCSP, including all certificates issued by and to the DarkMatter CA trust anchors and the status of all certificates issued by the DarkMatter CA;

In addition, the DarkMatter CA retains an online repository of related documents and policies (such as this document) where it discloses certain practices and procedures. This repository includes an online web server which allows anonymous access and retrieval of these documents and policies via HTTPS.
2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status
The DarkMatter CA publishes information about the digital certificates it issues including all End Entity certificates, as well as the CRLs. The digital certificates information is published in the DarkMatter CA repositories that are publicly accessible and are installed within the DarkMatter CA premises. Published information includes:

- Certificates issued by and to the DarkMatter CA in the CA Directory through the DarkMatter CA web server
- CRLs are also published on the DarkMatter VA web service

The DarkMatter CA makes available an OCSP server that provides notice on the status of a certificate, issued by the DarkMatter CA upon request from a relying party, in compliance with IETF RFC 6960.

The digital certificates that are published by DarkMatter CA include information submitted directly or indirectly by the respective PKI participants.

The certificates and certificate status published by DarkMatter CA are available for anonymous access 24 hours a day, 7 days a week.

2.2.2 Publication of CA Information
The DarkMatter CA makes available and publishes information on its policies. The policies online repository is accessible at https://ca.darkmatter.ae/.

The DarkMatter CA reserves its right to make available and publish information on its policies by any means it sees fit.

2.3 Time or Frequency of Publication
CA Certificates issued are published in a repository as soon as possible after issuance. CRLs for Entity CA certificates are issued every month. End Entity certificates are available via RA interfaces whenever the Managed PKI interfaces has been implemented. CRLs for End Entity certificates are issued in accordance with the corresponding certificate profile.

In case a CA certificate is revoked, the CRLs will be updated within 18 hours.

New or modified versions of DarkMatter CA documents and policies are typically published within 10 business-days after their approval.

2.4 Access Controls on Repositories
Read-only access to all repositories is unrestricted. Logical and physical controls are implemented to prevent unauthorized write access to repositories.

Network addresses for the available repositories are provided in Table 1: DarkMatter CA Repository Addresses.
Table 1: DarkMatter CA Repository Addresses

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Network Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Repository</td>
<td>HTTP access to repositories: <a href="https://ca.darkmatter.ae">https://ca.darkmatter.ae</a></td>
</tr>
<tr>
<td>OCSP</td>
<td>OCSP access to repository: <a href="http://ocsp.darkmatter.ae/">http://ocsp.darkmatter.ae/</a></td>
</tr>
</tbody>
</table>

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names
The DarkMatter CA generates and signs certificates containing an X.500 Distinguished Name (DN) in the Issuer and in Subject fields.

The DarkMatter CA does not issue anonymous certificates to subscribers or certificates with an empty subject Distinguished Name (DN).

To identify an Entity CA or End Entity, the DarkMatter CA follows naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names.

Names assigned to subscribers of a certificate are unique within the domain of the DarkMatter CA as they are always used together with a unique sequential number. The DarkMatter CA may assign the name at its sole discretion.

3.1.2 Need for Names to be Meaningful
The DarkMatter CA supports the generation and publication of both CA and End Entity certificates. Subject names used in the certificates must identify the entity to which they are assigned in a meaningful way. As such, the Subscriber should provide the DarkMatter CA with proper evidence of the association existing between the subject name and the entity to which it belongs.

3.1.3 Anonymity or Pseudonymity of Subscribers
Within the DarkMatter CA hierarchy, Subscribers certificates are issued by Entity CAs. The UAENRCA does not issue Subscriber certificates. The DarkMatter CA may issue end-entity anonymous or pseudonymous certificates provided that (i) such certificates are not prohibited by applicable policy (e.g. for certificate type, assurance level, or certificate profile) and (ii) name space uniqueness is preserved.

3.1.4 Rules for Interpreting Various Name Forms
Distinguished Names in CA Certificates are interpreted using X.500 standards and ASN.1 syntax. Refer to [RFC 4510] and [RFC 2616] for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.
3.1.5 Uniqueness of Names

The DarkMatter CA ensures that created names uniquely identify all Entity CAs. The names should conform to X.500 standards for name uniqueness. For End Entity certificates, the following practices are used to ensure uniqueness:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS Certificates</td>
<td>Inclusion of the domain name in the Certificate. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).</td>
</tr>
<tr>
<td>Client Certificates</td>
<td>Requiring a unique email address or a unique organization name combined/associated with a unique serial integer.</td>
</tr>
<tr>
<td>IGTF and Grid Device Certificates</td>
<td>For device certificates, an FQDN is included in the DN fields. For other certificates, DarkMatter may append a unique ID to the name listed in the CN field if necessary.</td>
</tr>
<tr>
<td>Code Signing Certificates</td>
<td>Requiring a unique organization name and address or a unique organization name combined/associated with a unique serial integer.</td>
</tr>
<tr>
<td>Time Stamping</td>
<td>Requiring a unique hash and time or unique serial integer assigned to the time stamp</td>
</tr>
</tbody>
</table>

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers and Entity CAs may not request certificates with any content that infringes the intellectual property rights of another entity. Unless otherwise specifically stated in this CPS, the DarkMatter CA does not verify an Applicant’s right to use a trademark and does not resolve trademark disputes. The DarkMatter CA may reject any application or require revocation of any certificate that is part of a trademark dispute.

3.2 Initial Identity Validation

The DarkMatter CA may use any legal means of communication or investigation to ascertain the identity of an organizational applicant and the representative of a legal person. The DarkMatter CA may refuse to issue a Certificate at its sole discretion.

3.2.1 Method to Prove Possession of Private Key

The DarkMatter CA verifies that certificate applicant possesses the private key corresponding to the public key submitted with the application by verifying the signature on the certificate request received from the entity (typically a PKCS#10 format). For Entity CA certificates, the Entity should supply the Subject Key Identifier (SKI) independently from the certificate request. The DarkMatter CA will verify that the SKI in the request and resulting certificate match the SKI provided by the Entity. All transactions involved in CA certificate issuance are recorded as part of the security audit data.
### 3.2.2 Authentication of Organization Identity

DarkMatter in its role as the UAENRCA issues certificates to Entity CAs. The DarkMatter CA authenticates the entity’s identity as part of the application process. The authentication of the entity may involve other relevant sources to ensure the legitimacy and authority of the applicant organization and representation.

The DarkMatter CA shall ensure that an Entity’s Organizational identity information is verified in accordance with the minimum requirements detailed in the table below for the corresponding certificate type:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Identity Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TLS Certificates</strong></td>
<td>DarkMatter validates the Applicant’s right to use or control the domain names that will be listed in the Certificate using one or more of the following procedures:</td>
</tr>
<tr>
<td>Private</td>
<td>1. Relying on enterprise DNS records obtained from an authenticated source</td>
</tr>
<tr>
<td></td>
<td>2. Communicating with one of the following email addresses: helpdesk@domain, administrator@domain, admin@domain, or any address listed in the technical, registrar, or administrative contact field of the domain’s Registrar record;</td>
</tr>
<tr>
<td></td>
<td>3. A domain authorization letter from an authorized representative; and/or</td>
</tr>
<tr>
<td></td>
<td>4. A similar procedure that offers an equivalent level of assurance in the Applicant’s ownership, control, or right to use the Domain Name.</td>
</tr>
<tr>
<td>Public Trust</td>
<td>DarkMatter validates the Applicant’s right to use or control the domain names that will be listed in the Certificate using one or more of the following procedures:</td>
</tr>
<tr>
<td></td>
<td>1. Relying on publicly available records from the Domain Name Registrar, such as WHOIS or other DNS record information;</td>
</tr>
<tr>
<td></td>
<td>2. Communicating with one of the following email addresses: webmaster@domain, administrator@domain, admin@domain, hostmaster@domain, postmaster@domain, or any address listed in the technical, registrant, or administrative contact field of the domain’s Registrar record;</td>
</tr>
<tr>
<td></td>
<td>3. Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a DNS zone file or a live page on the given domain); and/or</td>
</tr>
<tr>
<td></td>
<td>4. A similar procedure (as defined in current CAB Forum Baseline Requirements) that offers an equivalent level of assurance in the Applicant’s ownership, control, or right to use the Domain Name.</td>
</tr>
<tr>
<td>DarkMatter verifies an included country code using (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant’s IP address; (b) the ccTLD of the requested Domain Name; or (c) information provided by the Domain Name Registrar.</td>
<td></td>
</tr>
<tr>
<td>OV TLS</td>
<td>DarkMatter validates the Applicant’s right to use or control the Domain Name(s) that will be listed in the Certificate using one of the Public Trust TLS methods listed above.</td>
</tr>
<tr>
<td></td>
<td>DarkMatter also verifies the identity and address of the Applicant using:</td>
</tr>
<tr>
<td></td>
<td>1. a reliable third party/government databases or through communication with the entity or jurisdiction governing the organization’s legal creation, existence, or recognition;</td>
</tr>
<tr>
<td></td>
<td>2. a site visit;</td>
</tr>
<tr>
<td></td>
<td>3. an attestation letter that is signed by an accountant, lawyer, government official, or other reliable third party; or</td>
</tr>
</tbody>
</table>
4. for address only, a utility bill, bank statement, credit card statement, tax document, or other reliable form of identification.

DarkMatter verifies any DBA included in a Certificate using a third party or government source, attestation letter, or reliable form of identification.

<table>
<thead>
<tr>
<th>EV TLS</th>
<th>Information concerning organization identity related to the issuance of EV Certificates is validated in accordance with the EV Guidelines.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGTF Grid or Device</td>
<td>An RA or Trusted Agent validates the applicant’s information in accordance with an RPS (or similar document) applicable to the community of interest.</td>
</tr>
<tr>
<td>Client – Level 1</td>
<td>DarkMatter verifies organizational control over the email domain using authentication procedures similar to those used when establishing domain control before issuance of OV TLS Server Certificates.</td>
</tr>
<tr>
<td>Client – Levels 2, 3, 4</td>
<td>If the Certificate contains organization information, DarkMatter obtains documentation from the organization sufficient to confirm that the individual has an affiliation with the organization named in the Certificate.</td>
</tr>
</tbody>
</table>

Before issuing a TLS Certificate with a domain name that has not been previously verified as within the scope of an RA’s or other Delegated Third Party’s allowed domain names, DarkMatter establishes that the RA or Delegated Third Party has the right to use the Domain Name by independently verifying the authorization with the domain owner, as described above, or by using other reliable means, such as performing a DNS lookup to determine whether there is a matching DNS record that points to the Delegated Third Party’s IP address or domain namespace.

### 3.2.3 Authentication of Individual Identity

Authentication of individual identity is employed for Subscriber’s certificate using the following procedures:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Identity Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client – Level 1</td>
<td>DarkMatter or an RA verifies Applicant’s control of the email address or corroborative information listed in the Certificate application. Any of the following methods can be used for validating asserted identity:</td>
</tr>
<tr>
<td></td>
<td>1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent with presentment of an identity credential (e.g., Emirates ID, driver’s license or birth certificate).</td>
</tr>
<tr>
<td></td>
<td>2. Using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as:</td>
</tr>
<tr>
<td></td>
<td>a. the ability to place or receive calls from a given number; or</td>
</tr>
<tr>
<td></td>
<td>b. the ability to obtain mail sent to a known physical address.</td>
</tr>
<tr>
<td></td>
<td>3. Through information derived from an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, employer, or retail company). Acceptable information includes:</td>
</tr>
<tr>
<td></td>
<td>a. the ability to obtain mail at the billing address used in the business relationship;</td>
</tr>
<tr>
<td></td>
<td>b. verification of information established in previous transactions (e.g., previous order number); or</td>
</tr>
</tbody>
</table>
| Client – Level 2, IGTF Cedar & Birch | The CA or an RA confirms that the following are consistent with the application and sufficient to identify a unique individual:
   a) the name on the government-issued photo-ID referenced below;
   b) date of birth; and
   c) current address or personal telephone number. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Proofing is performed by one of the following methods:</td>
<td></td>
</tr>
<tr>
<td>1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent (or entity certified by an Emirate, state, federal, or national entity as authorized to confirm identities) with presentment of a reliable form of current government-issued photo ID.</td>
<td></td>
</tr>
<tr>
<td>2. The Applicant must possess a valid, current, government-issued, photo ID e.g. Emirate ID. The Registration Authority or Trusted Agent performing identity proofing must obtain and review, which may be through remote verification, the following information about the Applicant: (i) name, date of birth, and current address or telephone number; (ii) serial number assigned to the primary, government-issued photo ID; and (iii) one additional form of ID such as another government-issued ID, an employee or student ID card number, telephone number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the applicant's residence. Identity proofing through remote verification may rely on database record checks with an agent/institution or through credit bureaus or similar databases.</td>
<td></td>
</tr>
<tr>
<td>NOTE: DarkMatter or an RA may confirm an address by issuing credentials in a manner that confirms the address of record or by verifying knowledge of recent account activity associated with the Applicant's address and may confirm a telephone number by sending a challenge-response SMS text message or by recording the applicant's voice during a communication after associating the telephone number with the applicant in records available to DarkMatter or the RA.</td>
<td></td>
</tr>
<tr>
<td>3. Where DarkMatter or an RA has a current and ongoing relationship with the Applicant, identity may be verified through the exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo-ID, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret.</td>
<td></td>
</tr>
<tr>
<td>4. Any of the methods used to verify the identity of an applicant for a Level 3 or 4 Client Certificate.</td>
<td></td>
</tr>
<tr>
<td>Client – Level 3</td>
<td>In-person proofing before an RA, Trusted Agent, or an entity certified by an Emirate, state, federal, or national entity that is authorized to confirm identities. The information must be collected and stored in a secure manner. Required identification consists of one unexpired Federal/National Government-issued Picture I.D. (e.g. Emirate ID or passport), or two unexpired Non-Federal Government I.D.s, one of which must be a...</td>
</tr>
</tbody>
</table>
photo I.D. Acceptable forms of government ID include a driver’s license, passport, national identity card, permanent resident card, trusted traveler card, military ID, or similar photo identification document.

The person performing identity proofing examines the credentials and determines whether they are authentic and unexpired and checks the provided information (name, date of birth, and current address) to ensure legitimacy. The Applicant signs a Declaration of Identity, defined below, to which the person performing identity proofing attests. DarkMatter or the RA reviews and keeps a record of the Declaration of Identity.

DarkMatter may also employ an in-person antecedent process, to meet this in-person identity proofing requirement. A historical in-person identity proofing is sufficient if (1) it meets the thoroughness and rigor of in-person proofing described above, (2) supporting ID proofing artifacts exist to substantiate the antecedent relationship, and (3) mechanisms are in place that bind the individual to the asserted identity. In one use case, the Applicant (e.g. an employee) has been identified previously by an employer and is bound to the asserted identity remotely through the use of known attributes or shared secrets. In another use cases, DarkMatter uses a third party Identity Verification Provider that constructs a real-time, five-question process, based on multiple historic antecedent databases, and the applicant is given two minutes to answer at least four of the five questions correctly.

The identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance.

A Declaration of Identity consists of:

1. the identity of the person performing the verification;
2. a signed declaration by the verifying person stating that they verified the identity of the Subscriber as required, the signature on the declaration may be either a handwritten or digital signature using a Certificate that is of equal or higher level of assurance as the credential being issued;
3. unique identifying number(s) from the Applicant’s identification document(s), or a facsimile of the ID(s);
4. the date of the verification; and
5. a declaration of identity by the Applicant that is signed (in handwriting or using a digital signature that is of equivalent or higher assurance than the credential being issued) in the presence of the person performing the verification.

If in-person identity verification is required and the Applicant cannot participate in face-to-face registration alone (e.g. because Applicant is a network device, minor, or person not legally competent), then the Applicant may be accompanied by a person already certified by the PKI or who has the required identity credentials for a Certificate of the same type applied for by the Applicant. The person accompanying the Applicant (i.e. the “Sponsor”) will present information sufficient for registration at the level of the Certificate being requested, for himself or herself, and for the Applicant.

3.2.3.1 Authentication for Role-based Client Certificates
DarkMatter may issue Certificates that identify a specific role that the Subscriber holds, if the role identifies a specific individual within an organization (e.g., Chief Information Officer is a unique individual whereas Program Analyst is not). These role-based Certificates are used when non-repudiation is desired. DarkMatter only issues role-based Certificates to Subscribers who first obtain an individual Subscriber Certificate that is at the same or higher assurance level as the requested role-based Certificate. DarkMatter may issue Certificates with the same role to multiple Subscribers. However, DarkMatter requires that each Certificate have a unique Key Pair. Individuals may not share their issued role-based Certificates and are required to protect the role based Certificate in the same manner as individual Certificates.

DarkMatter verifies the identity of the individual requesting a role-based Certificate (the sponsor) in accordance with Section 3.2.3 before issuing a role-based Certificate. The sponsor must hold a DarkMatter-issued client individual Certificate at the same or higher assurance level as the role-based Certificate. If the Certificate is a pseudonymous Certificate that identifies subjects by their organizational roles, then DarkMatter or an RA validates that the individual either holds that role or has the authority to sign on behalf of the role.

Regarding the issuance of role-based Certificates, this CPS requires compliance with all provisions of DarkMatter’s CP regarding key generation, private key protection, and Subscriber obligations.

IGTF Certificates are not issued as role-based Certificates.

3.2.3.2 Authentication for Group Client Certificates
DarkMatter issues group Certificates (a Certificate that corresponds to a Private Key that is shared by multiple Subscribers) if several entities are acting in one capacity and if non-repudiation is not required. Direct Address Certificates and Direct Organizational Certificates are used as group Certificates consistent with applicable requirements of the Direct Program. DarkMatter or the RA records the information identified in Section 3.2.3 for a sponsor before issuing a group Certificate. The sponsor must be at least an Information Systems Security Officer (ISSO) or of the equivalent rank or greater within the organization.

The sponsor is responsible for ensuring control of the Private Key. The sponsor must maintain and continuously update a list of Subscribers with access to the Private Key and account for the time period during which each
Subscriber had control of the key. Group Certificates may list the identity of an individual in the subjectName DN provided that the subjectName DN field also includes a text string, such as “Direct Group Cert,” so that the Certificate specifies the subject is a group and not a single individual. Client Certificates issued in this way to an organization are always considered group client Certificates.

3.2.3.3 Authentication of Devices with Human Sponsors
DarkMatter issues Level 1, 2, 3 or 4 Client and Device Certificates for use on computing or network devices, provided that the entity owning the device is listed as the subject. In all cases, the device has a human sponsor who provides:

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

If the Certificate’s sponsor changes, the new sponsor is required to review the status of each device to ensure it is still authorized to receive Certificates. Each sponsor is required to provide proof that the device is still under the sponsor’s control or responsibility on request. Sponsors are contractually obligated to notify DarkMatter if the equipment is no longer in use, no longer under their control or responsibility, or no longer requires a Certificate. All registration is verified commensurate with the requested certificate type.

3.2.4 Non-Verified Subscriber Information
The common name of a Client Level 1 Certificate is not verified as the legal name of the Subscriber. Any other non-verified information included in a Certificate is designated as such in the Certificate. Unverified information is never included in a Level 2, Level 3, Level 4, Object Signing, OV TLS, EV TLS, or Device Certificate. All information in Entity CA certificates issued by the DarkMatter CA matches the information in the certificate request.

3.2.5 Validation of Authority
Certificates that contain explicit or implicit organization affiliations are issued only after ascertaining the Subscriber has the authorizations to act on behalf of the organization in the implied capacity. Examples of these per certificate type are contained in the following table:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS Certificate</td>
<td>The request is verified with an authorized contact listed with the Domain Name Registrar, through a person with control over the domain, or through an out-of-band confirmation with the applicant.</td>
</tr>
</tbody>
</table>
A person with control over the domain name is considered to have authority to request TLS Certificates, including any individual with access to one more of the following email addresses:

- webmaster@domain
- administrator@domain
- admin@domain
- hostmaster@domain
- postmaster@domain
- any address listed as a contact field of the domain’s Domain Name Registrar record.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OV TLS</td>
<td>The request is verified using a Reliable Method of Communication, in accordance with the Baseline Requirements.</td>
</tr>
<tr>
<td>EV TLS</td>
<td>The request is verified in accordance with the EV Guidelines.</td>
</tr>
<tr>
<td>Client – Level 1</td>
<td>The request is verified through the email address listed in the Certificate or with a person who has technical or administrative control over the domain and the email address to be listed in the Certificate.</td>
</tr>
<tr>
<td>Client – Levels 2, 3, 4</td>
<td>The organization named in the Certificate confirms to DarkMatter or an RA that the individual is authorized to obtain the Certificate. The organization is required to request revocation of the Certificate when that affiliation ends.</td>
</tr>
<tr>
<td>IGTF Certificates</td>
<td>An authorized individual approves the certificate request. For device Certificates, the RA retains contact information for each device’s registered owner. The device owner is required to notify the RA and request revocation if the device sponsor is no longer authorized to use the device or the FQDN in the Certificate.</td>
</tr>
</tbody>
</table>

An organization may limit who is authorized to request Certificates by sending a request to DarkMatter. A request to limit authorized individuals is not effective until approved by DarkMatter. DarkMatter will respond to an organization’s verified request for DarkMatter’s list of its authorized requesters.

### 3.2.6 Criteria for Interoperation

Certificates shall be issued in accordance with [UAE Digital Certificate Interoperability Guidelines] in order to ensure interoperability.

### 3.3 Identification and Authentication for Re-Key Requests

Re-keying a certificate means that a new certificate is created that has the same characteristics as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key), a different serial number, and may be assigned a different validity period.

For re-keying, DarkMatter CA follows the same procedures as in the Initial Identity Validation.
3.3.1 Identification and Authentication for Routine Re-Key

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

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

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

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

3.3.2 Identification and Authentication for Re-Key after Revocation

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

Revocation requests to the DarkMatter CA must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised. In the case of loss of key, DarkMatter CA can suspend/revoke the certificate on verifying the subscriber’s identity as described in Section 3.2.

4 Certificate Life-Cycle Operational Requirements

This Section is used to specify requirements imposed by the DarkMatter CA upon Entity CAs, Subscribers, or other participants with respect to the life-cycle of a certificate.

4.1 Certificate Application

The Entity CA must perform the following steps, in no particular order, when it applies for a certificate to become a subordinate CA:

- Establish and record identity of Entity CA;
- Generate a key pair for each certificate required;
- Establish that the public key forms a functioning key pair with the private key held by the Entity CA (per Section 3.2.1);
- Provide a Letter of Authorization (LOA) for the point of contact (POC) for verification of any roles or authorizations requested that could be downloaded from https://trustlink.darkmatter.ae;
- Complete the certificate applicable forms (including sections such as Entity general information, Entity CA type, Repository information, etc.) that could be downloaded from http://trustlink.darkmatter.ae;
- Submit supporting documents;
- Acknowledge any applicable agreements; and
- Pay any applicable fees.

These steps must be completed prior to certificate issuance. All communications among Entity CAs supporting the certificate application and issuance process shall be in accordance with [Secure Communication Policy] to ensure exchanged data is protected. Any electronic transmission of shared secrets (such as a password, a passphrase, or an array of randomly chosen bytes) shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

Following successful completion of the application process by Entity CA and subsequent approval by the DarkMatter CA, the DarkMatter CA and Entity CA will establish a Memorandum of Agreement (MOA), and then the DarkMatter CA issues the certificate.

Once the certificate is issued, it is manually checked to ensure each field and extension is populated with the correct information before it is delivered to the Entity CA and before it is posted in the DarkMatter CA Repository.

The Entity CA is required to provide accurate information and has also the responsibility to check the issued certificate to ensure each field and extension is populated with the correct information.
For End Entity Certificates, a Subscriber will make an application to the appropriate Entity CA, and provide the required mandatory information (varies based on certificate profile being requested). An RA will validate the information provided and verify the binding of the key to the identity being asserted.

4.1.1 Who can Submit a Certificate Application

An Entity CA certification request must be submitted by an authorized POC by the Entity.

Either the Applicant or an individual authorized to request Certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to DarkMatter.

EV Certificate requests must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The certificate request must be accompanied by a signed (in writing or electronically) Subscriber Agreement from a Contract Signer.

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

4.1.2 Enrollment Process and Responsibilities

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

All communication among PKI Authorities supporting the certificate application and issuance process are authenticated and protected from modification.

At a high level, the enrollment process will be similar to the following (not necessarily in this strict order):

1. Certificate Application is submitted
2. Key pair is generated and provided to DarkMatter
3. RA validates Subscriber identities and Application information
4. RA confirms binding of identity to keys
5. Applicant pays any applicable fees
6. DarkMatter issues certificates for verified Subscribers

4.2 Certificate Application Processing

The DarkMatter CA verifies that information in certificate applications is accurate before certificates are issued. The process includes verification of information by an RA. The Applicant remains responsible for the provided information.

4.2.1 Performing Identification and Authentication Functions

After receiving a certificate application, the DarkMatter CA or an RA verifies the application information and other information in accordance with Section 3.2 and following defined procedures. After verification is complete, the DarkMatter CA decides whether or not to issue the certificate. As part of this verification, the
DarkMatter CA checks the certificate application against an internal database of previously rejected certificate applications to identify suspicious certificate requests. If some or all of the documentation used to support an application is in a language other than English, a DarkMatter employee, RA, or agent skilled in the language performs the final cross-correlation and due diligence.

In accordance with Baseline Requirements section 3.2.2.8, prior to issuing of publicly trusted SSL/TLS certificates, DarkMatter validates each of the requested FQDNs against the domain’s CAA records for listed authorized CA(s).

If a CAA record exists that does not contain darkmatter.ae as an authorized CA, DarkMatter will reject the request and not issue the certificate.

DarkMatter processes the CAA records as follow.
- Validate and act on, Issue and Issuewild
- Validate but don’t act on iodef.
- Do not validate nor act on any other property tags
- If no property tags are found, DarkMatter considers it approved to issue

If a request is rejected for any of the reasons above, DarkMatter will document the details for reporting purposes. DarkMatter does not commit to submit reports to contacts mentioned in the iodef property tag.

### 4.2.2 Approval or Rejection of Certificate Applications

The DarkMatter CA may approve or reject a certificate application based on the certification application verification and compliance with requirements. The DarkMatter CA or an RA may reject any certificate application that cannot be verified. At their sole discretion, the DarkMatter CA may work with appropriate parties to resolve certificate application issues.

Except for EV Certificates in pre-approved domains of the Managed PKI (MPKI), EV Certificate issuance approval requires two separate DarkMatter validation specialists. The second validation specialist cannot be the same individual who collected the documentation and originally approved the EV Certificate. The second validation specialist reviews the collected information and documents any discrepancies or details that require further explanation. The second validation specialist may require additional explanations and documents prior to authorizing the Certificate’s issuance. MPKI RAs may perform the final cross-correlation and due diligence described herein using a single person representing the MPKI RA. If satisfactory explanations and/or additional documents are not received within a reasonable time, DarkMatter will reject the EV Certificate request and notify the Applicant accordingly.

If the certificate application is not rejected and is successfully validated in accordance with this CPS, DarkMatter will approve the certificate application and issue the Certificate. DarkMatter is not liable for any rejected Certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply.

The DarkMatter CA shall contractually require subscribers to verify the information in a certificate prior to using the certificate.
4.2.3 Time to Process Certificate Applications

Under normal circumstances, the DarkMatter CA verifies Applicant information and issues a digital certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. The DarkMatter CA will usually complete the validation process and issue or reject a certificate application within two business days after receiving all of the necessary details and documentation from the Applicant. EV TLS may take longer depending on the additional checks that need to be completed.

Identity shall be established no more than 30 days before initial issuance of Level 3 and Level 4 Certificates.

Occasionally, events outside of the control of the DarkMatter CA might delay the issuance process.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The DarkMatter CA issues certificates to Applicants through the following procedure:

1. Upon receiving a certificate request from the Applicant, the public key is verified to prove possession of the private key. Then, after all requirements criteria have been satisfied depending on the profile of the certificate type being requested, the DarkMatter CA signs and issues the certificate to the Applicant.
2. Each CA certificate issued by the DarkMatter CA is manually checked to ensure each field and extension is populated with the correct information, before the certificate is delivered to the Entity CA. It is the responsibility of Subscribers to verify the contents of the other certificates before first use.
3. The certificate issued by the DarkMatter CA is delivered to the Subscriber as either PEM or DER-encoded X.509 certificate.

The DarkMatter CA posts any issued CA certificates on an HTTP server for public access where appropriate. CA processes occurring during certificate issuance and databases are protected from unauthorized modification.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

DarkMatter may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, DarkMatter delivers Certificates via email to the email address designated by the Subscriber during the application process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued Certificate on the Subscriber’s computer or hardware security module. Certificates are considered accepted 5 days after the Certificate’s issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate. The Subscriber has a responsibility to verify the accuracy of the issued certificate and must immediately contact the DarkMatter CA to revoke erroneously issued certificates.
4.4.2 Publication of the Certificate by the CA
As specified in Section 2.2.1, all CA certificates are published in the DarkMatter CA Repositories. DarkMatter publishes end-entity Certificates by delivering them to the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities
RAs may receive notification of a Certificate’s issuance if the RA was involved in the issuance process. There is no provision for notifying other entities.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage
Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

4.5.2 Relying Party Public Key and Certificate Usage
Critical certificate extensions (including the basic constraints and key usage extensions) are employed to specify restrictions on the usage of the certificate.

Any relying party using a certificate that has been issued within the context of this CPS should:

- Have a fundamental understanding of how certificates are used and applied in general;
- Have checked the validity of a certificate before using it; and
- Only use the certificate in compliance with the certificate acceptable usage and restrictions (based on the critical certificate extensions)
- Use discretion when relying on a certificate and should consider the totality of the circumstances and risk of loss prior to relying on a certificate. Relying on a digital signature or certificate that has not been processed in accordance with applicable standards may result in risks to the Relying Party. The Relying Party is solely responsible for such risks. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate.

A Relying Party should rely on a digital signature or SSL/TLS handshake only if:

a. the digital signature or SSL/TLS session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
b. the Certificate is not revoked and the Relying Party checked the revocation status of the Certificate prior to the Certificate’s use by referring to the relevant CRLs or OCSP responses, and
c. the Certificate is being used for its intended purpose and in accordance with this CPS.

It is recommended that Relying Parties process and comply with this information whenever using the DarkMatter CA certificates in a transaction.
4.6 Certificate Renewal

For the UAENRCA there is no Certificate renewal specific procedure, any Entity CA should follow the same procedure as for a new Certificate in Section 4.1.

It is DarkMatter Subscriber’s responsibility to request a new certificate providing enough time to issue the new certificate before the expiration date of the original certificate. To renew its certificate, the Subscriber should follow the same procedure as for a new Certificate request in Section 4.1.

4.6.1 Circumstances for Certificate Renewal

DarkMatter may renew a Certificate if:

a. the associated Public Key has not reached the end of its validity period,
b. the Subscriber and attributes are consistent, and
c. the associated Private Key remains uncompromised.

DarkMatter may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. DarkMatter may notify Subscribers prior to a Certificate’s expiration date. Certificate renewal requires payment of additional fees.

4.6.2 Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber’s Certificates. For Certificates cross-certified with Bridge CAs, renewal requests are only accepted from certificate subjects, PKI sponsors, or RAs. DarkMatter may renew a Certificate without a corresponding request if the signing Certificate is re-keyed.

4.6.3 Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate’s original issuance. DarkMatter may elect to reuse previously verified information in its sole discretion but will refresh any information that is older than the periods specified in Section 3.3.1. DarkMatter may refuse to renew a Certificate if it cannot verify any rechecked information. If an individual is renewing a client Certificate and the relevant information has not changed, then DarkMatter does not require any additional identity vetting. Some device platforms, e.g. Apache, allow renewed use of the Private Key. If the Private Key and domain information have not changed, the Subscriber may renew the SSL Certificate using a previously issued Certificate or provided CSR.

4.6.4 Notification of New Certificate Issuance to Subscriber

DarkMatter may deliver the Certificate in any secure fashion, typically by email or by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and download the Certificate.
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate
Renewed Certificates are considered accepted 5 days after the Certificate’s renewal, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.6.6 Publication of the Renewal Certificate by the CA
DarkMatter publishes a renewed Certificate by delivering it to the Subscriber. All renewed CA Certificates are published in DarkMatter’s repository.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities
RAs may receive notification of a Certificate’s renewal if the RA was involved in the issuance process.

4.7 Certificate Re-Key
For the UAENRCA there is no Certificate re-keying specific procedure, any Entity CA should follow the same procedure as for a new Certificate in Section 4.1.

4.7.1 Circumstances for Certificate Rekey
Re-keying a Certificate consists of creating a new Certificate with a new Public Key and serial number while keeping the subject information the same. The new Certificate may have a different validity date, key identifiers, CRL and OCSP distribution points, and signing key. After re-keying a Certificate, DarkMatter may revoke the old Certificate but may not further re-key, renew, or modify the previous Certificate. Subscribers requesting re-key should identify and authenticate themselves as permitted by section 3.3.1.

4.7.2 Who May Request Certificate Rekey
DarkMatter will only accept re-key requests from the subject of the Certificate or the PKI sponsor. DarkMatter may initiate a certificate re-key at the request of the certificate subject or in DarkMatter’s own discretion.

4.7.3 Processing Certificate Rekey Requests
DarkMatter will only accept re-key requests from the subject of the Certificate or the PKI sponsor. If the Private Key and any identity and domain information in a Certificate have not changed, then DarkMatter can issue a replacement Certificate using a previously issued Certificate or previously provided CSR. DarkMatter re-uses existing verification information unless re-verification and authentication is required under section 3.3.1 or if DarkMatter believes that the information has become inaccurate.

4.7.4 Notification of Certificate Rekey to Subscriber
DarkMatter notifies the Subscriber within a reasonable time after the Certificate issues.

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate
Issued Certificates are considered accepted 5 days after the Certificate is rekeyed, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.
4.7.6 Publication of the Issued Certificate by the CA
DarkMatter publishes rekeyed Certificates by delivering them to Subscribers.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities
RAs may receive notification of a Certificate’s rekey if the RA was involved in the issuance process.

4.8 Certificate Modification
For the UAENRCA there is no Certificate modification specific procedure, any Entity CA should follow the same procedure as for Certificate Renewal in Section 4.1.

4.8.1 Circumstances for Certificate Modification
Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CPS. The new Certificate may have the same or a different subject Public Key. After modifying a Certificate that is cross-certified with a Bridge CA, DarkMatter may revoke the old Certificate but will not further re-key, renew, or modify the old Certificate.

4.8.2 Who May Request Certificate Modification
DarkMatter modifies Certificates at the request of certain certificate subjects or in its own discretion. DarkMatter does not make certificate modification services available to all Subscribers.

4.8.3 Processing Certificate Modification Requests
After receiving a request for modification, DarkMatter verifies any information that will change in the modified Certificate. DarkMatter will only issue the modified Certificate after completing the verification process on all modified information. DarkMatter will not issue a modified Certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.4 Notification of Certificate Modification to Subscriber
DarkMatter notifies the Subscriber within a reasonable time after the Certificate issues.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate
Modified Certificates are considered accepted 5 days after the Certificate is modified, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.8.6 Publication of the Modified Certificate by the CA
DarkMatter publishes modified Certificates by delivering them to Subscribers.

4.8.7 Notification of Certificate Modification by the CA to Other Entities
RAs may receive notification of a Certificate’s modification if the RA was involved in the issuance process.
4.9 Certificate Revocation and Suspension

Requests to revoke a certificate may be authenticated using the certificate's associated private key, regardless of whether or not the private key has been compromised. There is no provision for a suspension of certificates. Once a certificate has been revoked it can no longer be renewed or extended.

4.9.1 Circumstances for Revocation

Certificates must be revoked if at least one of the following circumstances applies:

- The Subscriber requested revocation of its Certificate
- A certificate contains information that is not valid or no longer valid
- The certificate has been illegally extended
- The certificate can no longer guarantee that a signature verification key can be assigned to a specific person
- The private key of the subscriber has been changed, lost, stolen, made public or otherwise compromised or misused
- The Subscriber is no longer entitled to hold the certificate (Refer to 1.3.3)
- The Subscriber does not comply with DarkMatter CA requirements
- The certificate in question is no longer needed (e.g. in the case of closing business, a new certificate was issued)
- A wildcard Certificate was used to authenticate a fraudulently misleading subordinate domain name
- The used algorithms and key sizes are not considered secure any more
- The Certificate was not issued in accordance with the CP, CPS, or applicable industry standards
- The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others
- For code-signing Certificates, the Certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content
- In the case of a cross-Certificate if the cross-certified entity no longer meets the stipulations of the corresponding policies, as indicated by policy OIDs listed in the policy mapping extension of the cross-Certificate.

4.9.2 Who can Request Revocation

Any appropriately authorized party, such as a recognized representative of a subscriber or cross-signed partner, may request revocation of a Certificate by the DarkMatter CA. Alternatively, the DarkMatter CA can revoke a certificate if an emergency has occurred that may impact the integrity of the certificate or the integrity of the DarkMatter CA operations. The DarkMatter CA may establish procedures that allow other entities to request certificate revocation for fraud or misuse. The DarkMatter CA may revoke a certificate of its own volition without reason, even if no other entity has requested revocation.

4.9.3 Procedure for Revocation Request

When the revocation request is not due to a perceived emergency, the revocation request, with an agreed time, can be done by a recognized representative of a subscriber, and executed immediately by the DarkMatter CA.
Revoked certificates are included on all new publications of the certificate status information until the expiration date of the certificate. The DarkMatter CA shall authenticate and log each revocation request.

In case of an emergency, the DarkMatter CA may revoke a certificate by executing the following activities:

- Notify all identified POCs related to the certificate for revocation by e-mail or phone,
- Revoke the certificate, and
- Post the new CRL

Once the incident has been investigated and documented, a new certificate is issued to replace the revoked certificate.

The DarkMatter CA will always revoke a certificate if the request is authenticated as originating from the Subscriber or the Affiliated Organization listed in the certificate. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, the DarkMatter CA shall investigate the alleged basis for the revocation request.

The DarkMatter CA shall maintain a continuous 24/7 ability to internally respond to any high priority certificate problem reports.

4.9.4 Revocation Request Grace Period

There is no revocation grace period for the DarkMatter CA. The DarkMatter CA will revoke certificates as quickly as practical upon receipt of a legitimate revocation request, or at a time agreed upon between DarkMatter CA and the Subscriber as long as the revocation is not due to a compromise. Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key.

4.9.5 Time Within which CA Must Process the Revocation Request

The DarkMatter CA should process a revocation request immediately after the request is received.

If the DarkMatter CA determines that immediate revocation is not practical, because the potential risks of revocation outweigh the risks caused by the compromise, then the DarkMatter CA and the DMPPA shall jointly determine the appropriate process to follow in order to promptly revoke the certificate. In all cases the DMPPA is the ultimate authority for making this decision.

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

1. Before the next CRL is published, if the request is received two or more hours before regular periodic CRL issuance,
2. By publishing it in the CRL following the next CRL, if the request is received within two hours of the regularly scheduled next CRL issuance,
3. Within seven days for a subCA meeting any of the Baseline Requirements reasons outlined in section 4.9.1.2, and
4. Regardless, within 18 hours after receipt.
4.9.6 Revocation Checking Requirement for Relying Parties
Prior to relying on the information listed in a certificate, a Relying Party is recommended to confirm the validity of each certificate in the certificate path in accordance with IETF PKIX standards, including checks for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each certificate in the chain.

4.9.7 CRL Issuance Frequency (if applicable)
DarkMatter uses its offline root CAs to publish CRLs for its intermediate CAs at least every 6 months. For an offline CA that has been cross-signed by a Bridge CA and only issues CA Certificates, certificatestatus-checking certificates, or internal administrative Certificates, DarkMatter issues a CRL at least every 31 days. All other CRLs are published at least every 24 hours. If a Certificate is revoked for reason of key compromise, an interim CRL is published as soon as feasible, but no later than 18 hours after receipt of the notice of key compromise. The Certificate Revocation list is published and is available 24 hours a day, 7 days a week, and 52 weeks of the year every year.

4.9.8 Maximum Latency for CRLs (if applicable)
CRLs for Certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Irregular, interim, or emergency CRLs and all CRLs for CAs chaining to Bridge CAs are posted within four hours after generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9 On-Line Revocation/Status Checking Availability
DarkMatter CA makes certificate status information available via OCSP. Where OCSP support is required, OCSP responses are provided within a commercially reasonable time.

4.9.10 On-Line Revocation Checking Requirements
A relying party must confirm the validity of a certificate prior to relying on the certificate.

4.9.11 Other Forms of Revocation Advertisements Available
The DarkMatter CA does not support any other forms of revocation advertisements.

4.9.12 Special Requirements Key Compromise
If one of the DarkMatter CA keys is compromised, the DarkMatter CA will make best efforts to notify the affected community. The compromised root certificate will be added to the CRL with the appropriate revocation reason. Additionally, if the DarkMatter CA key is compromised, all vendors with agreements to distribute the DarkMatter CA root certificate in their commercial trust stores will be notified.

In addition, a replacement root certificate and key pair will be generated and all related Entity CAs of the compromised CA will be issued new certificates. The new root certificate will be securely distributed to all Entity CAs.
If a certificate is revoked because of compromise or suspected compromise, the DarkMatter shall issue a CRL within 18 hours after it receives notice of the compromise or suspected compromise.

4.9.13 Circumstances for Suspension
Suspension is not used by the DarkMatter CA.

4.9.14 Who can Request Suspension
Suspension is not used by the DarkMatter CA.

4.9.15 Procedure for Suspension Request
Suspension is not used by the DarkMatter CA.

4.9.16 Limits on Suspension Period
Suspension is not used by the DarkMatter CA.

4.10 Certificate Status Services
Certificate status information is available via CRL and OCSP responder.

4.10.1 Operational Characteristics
Certificate status information is available via CRL and OCSP responder. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate’s validity period, except for revoked EV Code Signing Certificates, which remain on the CRL for at least 365 days following the Certificate’s validity period. OCSP information for subscriber Certificates is updated at least every four days. OCSP information for subordinate CA Certificates is updated at least every 12 months and within 24 hours after revoking the Certificate.

4.10.2 Service Availability
Certificate status services are available 24 hours a day, 7 days a week, 365 days of the year.

4.10.3 Optional Features
The DarkMatter CA does not support any other optional features.

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices
DarkMatter never escrows CA Private Keys.
DarkMatter may escrow Subscriber key management keys to provide key recovery services. DarkMatter encrypts and protects escrowed Private Keys using the same or a higher level of security as used to generate and deliver the Private Key.

DarkMatter allows Subscribers and other authorized entities to recover escrowed (decryption) Private Keys. DarkMatter uses multi-person controls during key recovery to prevent unauthorized access to a Subscriber’s escrowed Private Keys. DarkMatter accepts key recovery requests:

a. From the Subscriber or Subscriber’s organization, if the Subscriber has lost or damaged the Private Key token;
b. From the Subscriber’s organization, if the Subscriber is not available or is no longer part of the organization that contracted with DarkMatter for Private Key escrow;
c. From an authorized investigator or auditor, if the Private Key is part of a required investigation or audit;
d. From a requester authorized by a competent legal authority to access the communication that is encrypted using the key;
e. From a requester authorized by law or governmental regulation; or
f. From an entity contracting with DarkMatter for escrow of the Private Key when key recovery is mission critical or mission essential.

Entities using DarkMatter’s key escrow services are required to:

a. Notify Subscribers that their Private Keys are escrowed;
b. Protect escrowed keys from unauthorized disclosure;
c. Protect any authentication mechanisms that could be used to recover escrowed Private Keys;
d. Release an escrowed key only after making or receiving (as applicable) a properly authorized request for recovery; and

e. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key related information, or the facts concerning any key recovery request or process.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The DarkMatter CA does not perform any session key encapsulation recovery functions; no Entity CA keys are issued or used within the DarkMatter CA.

5 Facility, Management and Operational Controls

This section describes non-technical security controls used by the DarkMatter CA operator to perform the functions of subject authentication, certificate issuance, certificate revocation, audit, and archival. The DarkMatter CA implements an array of non-technical security controls in accordance with UAE Information Assurance Standards, in addition to other controls pertaining to this section.

During an initial transitional period some Public Trust CA operations are conducted in facilities of DarkMatter’s trust partner which is covered under a separate WebTrust Audit. These operations are also covered by the trust partner’s CPS. This CPS details only those operations specific to DarkMatter CA operations in the UAE.
5.1 **Physical Controls**

The DarkMatter CA sites adhere to the [UAE Information Assurance Standards], Physical and Environmental Security controls commensurate with the security level required for the systems and information they process or contain. The controls include the security of physical access points to the facility where the information system resides and the security of equipment against loss, damage, theft or compromise.

5.1.1 **Site Location and Construction**

The DarkMatter CA operations are conducted from sites within the UAE where information systems of the DarkMatter CA are located. The sites are consistent with facilities used to house high value, sensitive information. Multiple layers of security checkpoints are employed in these sites to only grant access to the authorized personnel.

Within the DarkMatter CA sites, the information systems are hosted in datacenters that is equipped with logical and physical controls. Moreover, information systems handling sensitive data are inside locked cages to provide additional security against unauthorized access. DarkMatter operates under a security policy designed to detect, deter, and prevent unauthorized access to DarkMatter’s operations.

5.1.2 **Physical Access**

Physical and environmental protection policy is developed in accordance with [UAE Information Assurance Standards] and with industry best practices. Refer to [UAE Information Assurance Standards], under “Physical and Environmental Security Policy” section.

The DarkMatter CA implements physical controls to reduce the risk of unauthorized access and equipment tampering. Security checkpoints of the DarkMatter CA site have security personnel 24 hours per day, 365 days per year. The secure parts of the DarkMatter CA hosting facilities are protected using physical access controls making them accessible only to appropriately authorized individuals via use of multi-level multi-party multi-factor authentication.

The DarkMatter CA site is constantly monitored using a CCTV system to detect any unusual activities and digital video recording is carried out covering at least one month period.

For RA personnel, controlled access and keyed-lock doors secure the support and vetting areas where identity vetting and other RA functions take place. Access card use is logged by the building security system.

5.1.3 **Power and Air Conditioning**

The DarkMatter CA datacenters (including the locked cage) have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and diesel generators provide redundant backup power in case the primary and secondary power supplies are interrupted. The backup power will keep the DarkMatter CA processing power and storage available until primary or secondary power is restored.
The DarkMatter CA datacenter use multiple load-balanced HVAC systems for cooling, and air ventilation through raised flooring to prevent overheating and to maintain an acceptable humidity level for all the information systems.

5.1.4 Water Exposures
All information systems are located in a datacenter configured with a raised platform and away from any water. In addition, the datacenter is equipped with monitoring systems to detect any excess moisture.

5.1.5 Fire Prevention and Protection
The datacenters are equipped with fire alarm systems and have smoke and heat detectors fitted in the ceilings and floors. The fire alarm system also responds to alarm pull boxes installed on the interior walls.
In the event of a fire, the datacenters are equipped with dry sprinkler pipes that are activated by the fire alarm system and all proper personnel are systematically notified. In addition, the datacenters are equipped with handheld fire extinguishers.

5.1.6 Media Storage
Media (such as CD-ROM, USB storage modules, Hardware Security Modules) is protected from accidental damage (such as water, fire, electromagnetic) and tempering. Media that contains security audit, archive, or backup information are secured and stored in a location separate from the datacenter.

5.1.7 Waste Disposal
Sensitive paper documents and materials are shredded on-site before disposal. Electronic media used to collect or transmit sensitive information are zeroized. If the zeroization procedure fails, the media is rendered unreadable before disposal. Any other waste is disposed of in accordance with the normal waste disposal requirements. Refer to [UAE Information Assurance Standards], under “Disposal of Media” section.

5.1.8 Off-Site Backup
The DarkMatter CA maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure. Backup media should be regularly tested to ensure that they can be relied upon when necessary. Refer to [UAE Information Assurance Standards], under “Information Backup” section.
Whenever a certificate is issued or revoked, the DarkMatter CA database is backed up on the next scheduled back-up. Two copies of the backup information are maintained, in the DarkMatter CA site and in another distant site. The backup media is stored with adequate protection in a safe.
5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role performs functions that can introduce security or operational incidents if not carried out properly, whether accidentally or maliciously. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot bypass security measures or subvert the security and trustworthiness of the DarkMatter CA operations. All personnel in trusted roles must be trained for assigned functions and free from conflicts of interest that might prejudice the impartiality of the DarkMatter CA operations. A list of personnel appointed to trusted roles is maintained and reviewed annually.

The following is the list of Trusted Roles:

- CA Administrator: to setup and maintain the CA information systems
- Officer: to perform activities along the certificate lifecycle
- Operator: to provide system administration/engineering functions of the infrastructure
- Auditor: to view and maintain audit logs

The separation provides a set of checks and balances over the DarkMatter CA operation.

5.2.1.1 CA Administrator

The CA Administrator role is responsible for:

- Installing, configuring, and maintaining the CA applications (including directory platform and certificate management system);
- Controlling and managing cryptographic modules;
- Performing systems backups and recovery;
- Establishing and maintaining systems accounts;
- Configuring audit parameters for the hardware equipment and CA applications; and
- Assisting with problem resolution and routine maintenance.

5.2.1.2 Officer

The Officer role is responsible for:

- Registering new Subscribers and requesting the issuance of certificates;
- Verifying the identity of Entity CA and the accuracy of information included in certificates;
- Approving and executing the issuance of certificates;
- Requesting, approving and executing the revocation of certificates;
- Configuring certificate profiles or templates and audit parameters for the DarkMatter CA software;
- Posting Certificates and CRLs; and
- Generating and backing up the DarkMatter CA keys.

5.2.1.3 Operator

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

### 5.2.1.4 Internal Auditor

The Internal Auditor role is responsible for:

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

### 5.2.2 Number of Persons Required per Task

The DarkMatter CA requires that at least two people acting in a trusted role (not necessarily exclusively dedicated to the trusted roles) to perform the following tasks:

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

Since a CA Administrator is required to gain access to the DarkMatter CA systems, at least one of the participants will always be a CA Administrator. The Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA systems but not logical access.

### 5.2.3 Identification and Authentication for Each Role

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

Trusted Roles are given role-based access control on the system enforced by the directory services.

### 5.2.4 Roles Requiring Separation of Duties

Individuals serving as Auditors shall not perform or hold any other trusted role.

Only an individual serving in an Auditor role may perform internal auditing functions, with the exception of audit functions that require multi-person control (e.g., configuring, archiving, deleting).

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

5.3.1 Qualifications, Experience, and Clearance Requirements

Any individuals appointed to a trusted role shall meet the following:

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

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

5.3.2 Background Check Procedures

Individuals fulfilling Trusted Roles pass an extensive background check conducted by the DarkMatter CA, or a trusted 3rd party. The background check should include at least the following:

- Confirmation of previous employment;
- Confirmation of previous residence;
- Check of professional reference;
- Confirmation of the highest or most relevant educational degree obtained;
- Search of criminal records;
- Search of driver’s license records; and
- Identification verification.

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

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the DarkMatter CA receive comprehensive trainings based on the assigned duties. Training (including on the job and class based trainings) is conducted in the following areas:
- Basic Public Key Infrastructure knowledge;
- CA security principles and mechanisms;
- All PKI software versions in use for the CA;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures;
- Common threats to validation processes, including phishing and other social engineering tactics; and
- The EV guidelines.

The training curriculum and schedule will be provided by the management of the appropriate functional teams. In addition, personnel are required to sign acknowledgements of the training they have received.

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

5.3.4 Retraining Frequency and Requirements

The DarkMatter CA employees must maintain skill levels in order to continue acting in trusted roles. For any significant change to the operations, the change is documented, and the DarkMatter CA will provide documented training, in accordance with an executed training plan, to all employees acting in Trusted Roles.

5.3.5 Job Rotation Frequency and Sequence

Any rotation of the DarkMatter CA personnel shall not impact the continuity and integrity of the provided services.

5.3.6 Sanctions for Unauthorized Actions

The DarkMatter CA takes appropriate administrative and disciplinary actions against employees and agents failing to comply with this CPS, whether through negligence or malicious intent.

If management cited an employee in a trusted role for unauthorized or inappropriate actions, the employee will be immediately removed from the trusted role pending management review. After investigation, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7 Independent Contractor Requirements

Independent contractors’ employment is subject to the DarkMatter CA HR policies.

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated in Section 5.3.6.
5.3.8 Documentation Supplied to Personnel

The DarkMatter CA makes available to all its personnel the documentation necessary to perform their duties, including a copy of the CP, this CPS, and other technical and operational documentation needed to maintain the integrity of the DarkMatter CA operations.

5.4 Audit Logging Procedures

The DarkMatter CA systems require identification and authentication at system logon with a unique identity. The DarkMatter CA generates audit log files for all events relating to security to establish the accountability of the operators who initiate such actions. In addition to the audit logs detailed below, information relevant to certificate issuance and certificate revocation events is captured on certificate issuance and certificate revocation forms.

Formal audit and accountability procedures have been developed and documented in accordance with [UAE Information Assurance Standards]. Refer to [UAE Information Assurance Standards], under “Information Systems Audit Considerations” section.

5.4.1 Types of Events Recorded

The DarkMatter CA enables all essential event auditing capabilities of its systems in order to record the events listed below. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used, depending on the audited event. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

At a minimum, each audit record includes the following, in no particular order:

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

All event records are available to auditors as proof of the DarkMatter CA practices.

The audit records of the DarkMatter CA include:

SECURITY AUDIT
- Any changes to the audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the audit logs

AUTHENTICATION TO SYSTEMS
- Successful and unsuccessful attempts to assume a role
- The value of maximum number of authentication attempts is changed
- Maximum number of authentication attempts occur during user login
- An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- An administrator changes the type of authenticator, e.g., from a password to a biometric
- Attempts to set passwords
- Attempts to modify passwords
- Logon attempts to applications
- Escalation of privilege

**LOCAL DATA ENTRY**
- All security-relevant data that is entered in the system

**REMOTE DATA ENTRY**
- All security-relevant messages that are received by the system

**DATA EXPORT AND OUTPUT**
- All successful and unsuccessful requests for confidential and security-relevant information

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

**PRIVATE KEY LOAD AND STORAGE**
- The loading of component private Keys
- All access to certificate subject Private Keys retained within the CA for key recovery purposes

**TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE**
- All changes to the trusted public keys, including additions and deletions

**SECRET KEY STORAGE**
- The manual entry of secret keys used for authentication

**PRIVATE AND SECRET KEY EXPORT**
- The export of private and secret keys (keys used for a single session or message are excluded)

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

**CERTIFICATE REVOCATION**
- All certificate revocation requests

**CERTIFICATE STATUS CHANGE APPROVAL**
- The approval or rejection of a certificate status change request

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

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

**CERTIFICATE PROFILE MANAGEMENT**
- All changes to the certificate profile

**REVOCATION PROFILE MANAGEMENT**
- All changes to the revocation profile

**CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT**
- All changes to the certificate revocation list profile

**TIME STAMPING**
- Clock synchronization

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

**CONFIGURATION CHANGES**
- Hardware
- Software
- Operating System
- Patches
- Security Profiles

**PHYSICAL ACCESS / SITE SECURITY**
- Personnel access to secure area housing CA component
- Access to a CA component
- Known or suspected violations of physical security
- Firewall and router activities

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

### 5.4.2 Frequency of Processing Log
Audit logs are collected and processed in an automated continuous process, and checked for anomalies at least once per month. The automatic logger creates alerts if anomalies are encountered.
The DarkMatter CA ensures that designated Auditor reviews log files at regular intervals and detects and reports anomalous events. The Auditor reviews include verifying that the log has not been tampered with, and inspecting entries for any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

5.4.3 Retention Period for Audit Log
The DarkMatter CA retains audit logs on-site until after they are reviewed. The individuals who remove audit logs from the CA systems are different than the individuals who control the DarkMatter CA signature keys.

5.4.4 Protection of Audit Log
Audit log information is retained on equipment until after it is copied by an administrator. The DarkMatter CA systems are configured to ensure that:
- Only authorized people have read access to logs;
- Only authorized people may archive audit logs; and
- Audit logs are not modified.

Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. The DarkMatter CA off-site storage location is a safe and secure location that is separate from the location where the data was generated.

The DarkMatter CA makes time-stamping records available when required to prove in a legal proceeding that the DarkMatter CA time-stamping services are operating correctly. Audit logs are made available to auditors upon request.

5.4.5 Audit Log Backup Procedures
The DarkMatter CA makes regular onsite backup copies of audit logs and audit log summaries daily, and sends a copy of the audit log off-site weekly.

5.4.6 Audit Collection System (Internal vs. External)
The audit log collection system is internal to the DarkMatter CA components. Automatic audit processes begin on 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, the DarkMatter CA Administrators will determine whether to suspend its operation until the problem is remedied.

5.4.7 Notification to Event-Causing Subject
No notice that an event was audited is provided to the individual, organization, device, or application that caused the event.
5.4.8 Vulnerability Assessments

The DarkMatter CA performs self-assessments of the security controls at the time of initial installation and configuration of the technology components. Vulnerability assessments are performed monthly or following a system configuration change with potential effect on system security (i.e., hardware, software, or network changes or upgrades).

The DarkMatter CA Auditors review the security audit data checks for continuity and will alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

External penetration assessments are conducted on a quarterly basis.

5.5 Records Archival

The DarkMatter CA includes sufficient detail in all archived records to show that a certificate was issued in accordance with this CPS.

5.5.1 Types of Records Archived

The DarkMatter CA retains the following information in its archives during its operations:

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

5.5.2 Retention Period for Archive
Archive records must be kept for a minimum of 10 years without any loss of data.

5.5.3 Protection of Archive
The DarkMatter CA stores the archive records at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Moreover, the DarkMatter CA maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

5.5.4 Archive Backup Procedures
The DarkMatter CA creates an archive disk of the data listed in section 5.5.1 every six (6) months and stores it in a secure off-site location for the duration of the set retention period. The DarkMatter CA maintains an archive backup and restoration procedures document.

5.5.5 Requirements for Time-Stamping of Records
Records are clearly labeled with date and time period information of the data contained in the record. System clocks are kept synchronized via NTP and system logs are automatically time stamped.

5.5.6 Archive Collection System (Internal or External)
An Auditor from the DarkMatter CA collects the archive information and assures that all records required for archive are correctly filed.

5.5.7 Procedures to Obtain and Verify Archive Information
Individual records pertaining to a specific Entity can be released to the authorized POC for that Entity upon Entity POC request.

5.6 Key Changeover
Key changeover procedures enable the smooth transition from the DarkMatter CA expiring certificates to new certificates. Prior the end of a Private Key’s lifetime, the DarkMatter CA ceases using the expiring Private Key to sign certificates and uses the Private Key only to sign CRLs and OCSP responder certificates. A new signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active for a period of time. The corresponding new Public Key certificate is provided to Sub CAs and relying parties through the delivery methods detailed in Section 6.1.4.
5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures
The DarkMatter CA maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. The DarkMatter CA reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

5.7.2 Computing Resources, Software, and/or Data are Corrupted
In the event of any of the DarkMatter CA computing resources, software, or data operations have been compromised, the DarkMatter CA assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If the DarkMatter CA determines that a continued operation could pose a significant risk to Relying Parties or Sub CAs, the DarkMatter CA suspends such operation until it determines that the risk is mitigated.

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

5.7.3 Entity Private Key Compromise Procedures
If the DarkMatter CA suspects that one of its Private Keys has been comprised or lost (such that compromise is possible even though not certain) the following procedure is executed:

1. The DarkMatter CA and all Sub CAs will be securely notified via telephone (via callback and challenge-response) to the designated POCs.

2. The self-signed certificate of the compromised key will be revoked. A compromised key can be used to sign the new CRL.

3. The Entity CAs that have issued certificates to the DarkMatter CA will revoke the certificate issued to the DarkMatter CA.

4. The DarkMatter CA will generate a new key pair and self-signed certificate in accordance with procedures set forth in Section 6.1.

5. New certificates will be issued to all Sub CAs in accordance with Section 4.3.

6. New DarkMatter CA root certificates will be securely distributed along with the new certificates.
5.7.4 Business Continuity Capabilities after a Disaster

The DarkMatter CA systems are redundant for failover in the event of a disaster. Moreover, the DarkMatter CA implements data backup and recovery procedures as part of its Business Continuity Management Plan to maintain the integrity of its services. The BCMP ensures that certificate status services are only minimally affected by any disaster affecting the DarkMatter CA facilities, while resuming other services as quickly as possible following a disaster.

The DarkMatter CA reviews, tests, and updates the BCMP and supporting procedures at least annually.

5.8 CA or RA Termination

In the event of a termination of the DarkMatter CA, certificates signed by the DarkMatter CA will be revoked, following the standard procedures for revoking certificates. Using secure communication (callback and challenge response), the DarkMatter CA will advise all Sub CAs of its termination. All documentation and data will be archived using the archival procedures in section 5.5.3. The CRLs will remain to be issued until the latest expiration date of any issued certificates, or will issue a long-term CRL valid until the expiration date of the root certificate. Once the last CRL has been issued, the private signing key will be destroyed.

Sub CAs will be given as much advance notice as circumstances permit.

6 Technical Security Controls

This section defines the security measures the DarkMatter CA takes to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). The DarkMatter CA implements an array of technical security controls in accordance with UAE Information Assurance Standards, in addition to other controls pertaining to this section.

6.1 Key Pair Generation and Installation

The DarkMatter CA protects its private key(s) in accordance with this CPS. The DarkMatter CA uses private signing keys only for signing certificates, CRLs, delta CRLs and OCSP responses in accordance with the intended use of each of these keys.

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The DarkMatter CA key pairs are generated in a hardware security module (HSM) by at least two individuals acting in Trusted Roles as part of the key generation ceremony. The DarkMatter CA creates auditable evidence during the key generation process to prove that the key pair generation process was followed. DarkMatter requires that an external auditor witness the generation of any CA keys to be used as publicly trusted root Certificates or to sign EV Certificates. For other CA key pair generation ceremonies, an Internal Auditor, external auditor, or independent third party attends the ceremony, or an external auditor examines the signed and documented record of the key generation ceremony, as allowed by applicable policy.
6.1.1.2 Subscriber Key Pair Generation
Subscribers must generate their keys in a manner that is appropriate for the certificate type. Certificates issued at Level 4 must be generated on validated hardware cryptographic modules using a FIPS-approved method.

6.1.2 Private Key Delivery to Subscriber
If DarkMatter, or an RA generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. Keys may be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module. In all cases:

1. Except where escrow/backup services are authorized and permitted, the key generator must not retain access to the Subscriber’s Private Key after delivery,
2. The key generator must protect the Private Key from activation, compromise, or modification during the delivery process,
3. The Subscriber must acknowledge receipt of the Private Key(s), typically by having the Subscriber use the related Certificate, and
4. The key generator must deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
   a. For hardware modules, the key generator maintaining accountability for the location and state of the module until the Subscriber accepts possession of it and
   b. For electronic delivery of Private Keys, the key generator encrypting key material using a cryptographic algorithm and key size at least as strong as the Private Key. The key generator shall deliver activation data using a separate secure channel.

The entity assisting the Subscriber with key generation shall maintain a record of the Subscriber’s acknowledgement of receipt of the device containing the Subscriber’s Key Pair. An RA providing key delivery services is required to provide a copy of this record to DarkMatter.

6.1.3 Public Key Delivery to Certificate Issuer
Subscribers generate their key pairs and electronically submits the public Key to DarkMatter CA as part of the certificate request process described in Section 4. The delivery mechanism of the public Key binds the Subscriber verified identity to the public key. The Subscriber’s signature on the request is authenticated prior to issuing the certificate.

6.1.4 CA Public Key Delivery to Relying Parties
The DarkMatter CA posts all CA certificates it issues to its repositories. The DarkMatter CA public keys are transported in a secure mechanism via digitally-signed e-mail, SFTP, or CD delivered by registered mail or courier.

The DarkMatter CA root certificate may also be distributed via commercial product trust stores when the DarkMatter CA is able to reach agreement with respective vendors.
6.1.5 Key Sizes

Currently, the DarkMatter Root CAs make use of the RSA SHA-384 algorithm with a key length of 4096 bits and ECC p384 with SHA-384. The DarkMatter CA also uses the same key size and algorithms for subordinate Entity or Issuing CAs as it does for Roots. In addition to these, the DarkMatter CA also uses SHA-256 and SHA-384 with RSA 2048 bits for Entity or Issuing CAs.

DarkMatter requires end-entity Certificates to contain a key size that is at least 2048 bits for RSA, DSA, or Diffie-Hellman and 224 bits for elliptic curve algorithms. DarkMatter may require higher bit keys in its sole discretion.

6.1.6 Public Key Parameters Generation and Quality Checking

DarkMatter uses a cryptomodule that conforms to FIPS 186-2 and provides random number generation and onboard generation of up to 4096-bit RSA Public Keys and a wide range of ECC curves.

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

The DarkMatter CA certificates include key usage extension fields that specify the intended use of the certificate and technically limit the certificate’s functionality in X.509v3 compliant software. Key usage bits and extended key usages are specified in the certificate profile for each type of certificate as set forth in Section 7.1.

The key of DarkMatter CA will be used for:
- The issuance of certificates to the Certification Authorities
- Issuance of Certificate Revocation Lists

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The DarkMatter CA uses appropriate cryptographic devices, known as Hardware Security Modules (HSMs), to perform its key management tasks.

These cryptographic devices meet the requirements of FIPS 140-2 Level 3 or higher, which guarantees, amongst other things, that any device tampering is immediately detected and private asymmetric cryptographic keys are never output in plaintext.

Activation of the HSM is described in Section 6.2.8. Physical access to the HSM requires two-party control.
6.2.2 Private Key (n out of m) Multi-Person Control
Use of the DarkMatter CA private key for signing will require the authorizations of at least two persons within the DarkMatter CA as explained in Section 5.2.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of CA Private Signature Key
The DarkMatter CA signature and encryption keys are not escrowed.

6.2.3.2 Escrow of Subscribers Private Signature Key
The DarkMatter CA is never in possession of Subscribers private signature keys. Subscribers may not escrow their private signature keys. Private keys associated with public trust TLS certificates are an example of private signature keys – these are never escrowed by the DarkMatter CA. DarkMatter may provide escrow services for other types of Certificates in order to provide key recovery as described in section 4.12.1.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key
The DarkMatter CA private signature keys are generated and stored inside DarkMatter CA cryptographic module, which has been evaluated to at least FIPS 140 Level 3. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. The DarkMatter CA key pairs are backed up by multiple individuals with Trusted Roles using a cryptographic hardware device as part of scripted and videotaped key backup process.

6.2.4.2 Backup of Subscribers Private Signature Key
The DarkMatter CA is never in possession of Subscribers private signing keys.

6.2.5 Private Key Archival
The DarkMatter CA does not archive its own Private Keys and is never in possession of Subscribers private signing keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module
All DarkMatter CA private keys are generated by and remain in a cryptographic module. Private Keys are exported from the cryptographic module only for backup purposes. The private keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, private keys are encrypted and protected from disclosure. Private Keys used to encrypt backups are securely stored and require two-person access.
6.2.7 Private Key Storage on Cryptographic Module
The DarkMatter CA private keys are generated and stored only inside cryptographic modules which are protected from unauthorized access and has been evaluated to at least FIPS 140 Level 3.

6.2.8 Method of Activating Private Key
The DarkMatter CA private keys are activated according to the specifications of the cryptographic module manufacturer. Activation data is split into two parts where the parts distributed by two different persons are required for activation.

Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber’s Private Key.

6.2.9 Method of Deactivating Private Key
Cryptographic modules, which have been activated, must not be left unattended or otherwise open to unauthorized access. After use, DarkMatter CA private keys are deactivated via logout procedures on the applicable HSM device. DarkMatter CA never leaves its HSM devices in an active unlocked or unattended state.

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10 Method of Destroying Private Key
Private keys will be destroyed when the certificates to which they correspond expire or are revoked, or when they are no longer needed, typically after:
- The services associated with the keys are disabled
- The associated CA is being decommissioned

To destroy a DarkMatter CA private key, the key will be deleted from all known storage media and all backup tokens will be zeroized. If the zeroization procedure fails, the Hardware cryptographic modules will be physically destroyed to eliminate the ability to extract any Private Key.

The key destruction process is documented and any associated records are archived.

6.2.11 Cryptographic Module Rating
Refer to Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival
Public keys of DarkMatter CA are archived as part of the certificate archival in accordance with Section 5.5.
6.3.2 Certificate Operational Periods and Key Pair Usage Periods

DarkMatter CA private signing keys are used to sign certificates for one-half of the certificate lifetime (e.g. for 10 years with a certificate lifetime of 20 years). New Certificate will be issued at 10 years.

The maximum validity period for end entity Digital Certificates issued within the UAE PKI (which contains both private and public trust profiles) is 1 to 3 years. The operational periods for keys are contained in the corresponding certificate profiles. NOTE: all publicly trusted TLS certificates conform to the key operational periods outlined in the Baseline Requirements and EV Guidelines.

6.4 Activation Data

Activation data refers to data values that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme.

6.4.1 Activation Data Generation and Installation

The DarkMatter CA activates the cryptographic module containing its CA private keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2.

Activation data will be transmitted via an adequately protected channel different from the delivery (time and location) of the associated cryptographic module.

All DarkMatter personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. DarkMatter employees are required to create non-dictionary, alphanumeric passwords with a minimum length and to change their passwords on a regular basis.

6.4.2 Activation Data Protection

The DarkMatter CA protects data used to unlock private keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. Activation data for cryptographic modules should be:

1. Memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.
2. biometric in nature, or
3. recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module

The DarkMatter CA is configured to temporarily lock out access following three unsuccessful login attempts.
6.4.3 Other Aspects of Activation Data

Activation PINs and passwords are required to be hard to guess, and to be changed regularly or upon rekey of the associated CA certificate.

All activation PINs, codes and passwords known to more than one person with a Trusted Role will be changed if any of the persons changed role or left the organization.

6.5 Computer Security Controls

The DarkMatter CA implements an array of technical security controls in accordance with [UAE Information Assurance Standards], in addition to other controls pertaining to this section.

6.5.1 Specific Computer Security Technical Requirements

Common systems configuration guidelines are developed and followed for all DarkMatter CA systems in accordance with [UAE Information Assurance Standards] and with industry best practices. Refer to [UAE Information Assurance Standards], under “Common Systems Configuration Guidelines” section.

The DarkMatter CA implements access controls to prevent unauthorized access to operating systems, using secure log-on procedures, suitable authentication techniques and user credentials management. Refer to [UAE Information Assurance Standards], under ”Operating System Access Control”, “Secure Log-on Procedures”, “User Identification and Authentication”, and “User Credentials Management System” sections.

Similarly, the DarkMatter CA implements access controls to prevent unauthorized access to information held in application systems by restricting access to information and isolating sensitive systems. Refer to [UAE Information Assurance Standards], under “Application and Information Access Control”, “Information Access Restriction”, and “Sensitive System Isolation” sections.

Relevant DarkMatter CA systems are scanned for malicious code and vulnerabilities, and protected against malwares. Refer to [UAE Information Assurance Standards], under “Technical vulnerability management”, and “Protection from Malware” sections.

In addition, the DarkMatter CA monitors the use of information systems, produces and keeps an audit log recording user activities, exceptions, and information security events. Refer to [UAE Information Assurance Standards], under “Monitoring System Use”, and “Audit Logging” section.

In case of an incident, an information security incident management and continuity management functions are implemented to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. Refer to [UAE Information Assurance Standards], under “Management of Information Security Incidents and Improvements” and “Information Systems Continuity Management” sections.

6.5.2 Computer Security Rating

Security measures are periodically examined in line with [UAE Information Assurance Standards] updates.
6.6 **Life Cycle Technical Controls**

The DarkMatter CA implements an array of technical security controls in accordance with [UAE Information Assurance Standards] that pertain to this section.

### 6.6.1 System Development Controls

The DarkMatter CA implements mechanisms to control and monitor the acquisition and development of its CA systems.

All DarkMatter CA software and systems are purchased using commercial-off-the-shelf products that have been developed under a formal development process that is well documented and selected based on rigorous selection process. Refer to [UAE Information Assurance Standards], under “Information Systems Acquisition, Development and Maintenance” section.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future to protect against supply chain threats and secure the supply of information systems. Refer to UAE Information Assurance Standards, under “Information Systems Acquisition, Development and Maintenance” section.

Updates of software and system are purchased in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel.

### 6.6.2 Security Management Controls

The configuration of the software and systems as well as any modifications and upgrades are documented and controlled as described in Section 6.5.1. A mechanism is implemented to detect unauthorized modification to the software or configuration in accordance with [UAE Information Assurance Standards] (Refer to “Correct Processing in Applications” section). The software, when first loaded, shall be verified as being supplied from the vendor, with no modifications, and be the version intended for use.

System and application level logging is enabled and reviewed weekly to maintain ongoing integrity of the software and configuration in accordance with UAE Information Assurance Standards (Refer to “Audit Logging” section).

### 6.6.3 Life Cycle Security Controls

The DarkMatter CA operates under standard maintenance. Upgrades, Information Assurance Vulnerability Alerts (IAVA), and patches to the software and hardware are applied as necessary in accordance with UAE Information Assurance Standards (Refer to “Technical vulnerability management” section).
6.7 Network Security Controls

The DarkMatter CA network is divided into different security zones which are isolated from one another by a firewall in accordance with [UAE Information Assurance Standards] (Refer to “Segregation in Networks” section). In addition, all unused network ports and services are turned off.

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are also employed to protect against known Internet and Intranet attacks.

Critical security incidents are investigated and processed immediately in collaboration with the national CERT (i.e. aeCERT). Refer to [UAE Information Assurance Standards], under “Incident Response Plan” and “Incident Response Assistance” sections.

6.8 Time-Stamping

The system time on DarkMatter’s computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours. All times are traceable to a real time value distributed by a UTC(k) laboratory or National Measurement Institute and are updated when a leap second occurs as notified by the appropriate body. DarkMatter maintains an internal NTP server that synchronizes with cellular telephone networks and maintains the accuracy of its clock within one second or less. For each timestamp request the internal NTP server is queried for the current time. However, Relying Parties should be aware that all times included in a time-stamp token are synchronized with UTC within the accuracy defined in the time-stamp token itself, if present.

7 Certificate, CRL, and OCSP Profiles

The DarkMatter CA uses the ITU X.509, version 3 standard to construct digital certificates for use within the DarkMatter CA PKI.

7.1 Certificate Profile


7.1.1 Version Number(s)

The DarkMatter CA issues X.509 v3 certificates.

7.1.2 Certificate Extensions

The DarkMatter CA issues certificates in conformance with [UAE Digital Certificate Interoperability Guidelines], using standard certificate extensions that comply with RFC 5280. IGTF Certificates comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.225
### 7.1.3 Algorithm Object Identifiers

The DarkMatter CA issues certificates using the following OIDs for signatures:

<table>
<thead>
<tr>
<th>OID Description</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>id-dsa-with-sha1</td>
<td>{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}</td>
</tr>
<tr>
<td>sha-1WithRSAEncryption</td>
<td>{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}</td>
</tr>
<tr>
<td>sha256WithRSAEncryption</td>
<td>{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}</td>
</tr>
<tr>
<td>sha384WithRSAEncryption</td>
<td>{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}</td>
</tr>
<tr>
<td>id-RSASSA-PSS</td>
<td>{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}</td>
</tr>
<tr>
<td>ecdsa-with-Sha256</td>
<td>{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}</td>
</tr>
<tr>
<td>ecdsa-with-Sha384</td>
<td>{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}</td>
</tr>
<tr>
<td>ecdsa-with-SHA512</td>
<td>{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4}</td>
</tr>
</tbody>
</table>

The DarkMatter CA issues certificates using the following OIDs to identify the algorithm associated with the subject key:

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

### 7.1.4 Name Forms

The DarkMatter CA issues certificates with the subject and issuer fields populated with an X.500 DN, with the attribute type as further constrained by RFC 5280. Optional subfields in the subject of a TLS Certificate must either contain information verified by DarkMatter or be left empty. DarkMatter logically restricts OU fields from containing Subscriber information that has not been verified in accordance with Section 3.

The Distinguished Name for each Certificate type is set forth in DarkMatter’s certificate profiles documents. The contents of the fields in EV Certificates must meet the requirements in Section 8.1 of the EV Guidelines.

### 7.1.5 Name Constraints

The DarkMatter CA may assert name constraints in certificates issued to Entity CAs appropriate for the PKI being certified using the nameConstraints extension.
7.1.6 Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs used by the DarkMatter CA are listed in Section 1.2 and in the DarkMatter CA Certificate Profiles document.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

The certificates issued by the DarkMatter CA do not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued by the DarkMatter CA do not contain a critical certificate policy extension.

7.2 CRL Profile

7.2.1 Version Number(s)

The DarkMatter CA issues X.509 version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

CRLs have at least the following extensions:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRL Number</td>
<td>Never repeated monotonically increasing integer</td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>Same as the Authority Key Identifier listed in the certificate</td>
</tr>
<tr>
<td>Invalidity Date</td>
<td>Optional date in UTC format</td>
</tr>
<tr>
<td>Reason Code</td>
<td>Optional reason for revocation</td>
</tr>
</tbody>
</table>

7.3 OCSP Profile

7.3.1 Version Number(s)

The DarkMatter CA OCSP responders conform to RFC 6960s.

7.3.2 OCSP Extensions

The DarkMatter CA does not use Critical OCSP extensions.
7.4 Lightweight Directory Access Protocol Profile

The DarkMatter CA may at its own discretion, host a repository in the form of a Lightweight Directory Access Protocol directory for the purpose of (i) storing and making available all X.509 v. 3 Digital Certificates issued under the UAE national PKI, (ii) facilitating public access to download these Digital Certificates for Certificate Holder and relying party requirements, and (iii) receiving, storing and making publicly available, regularly updated Certificate Revocation List v. 2 information, for the purpose of Digital Certificate validation.

7.4.1 Lightweight Directory Access Protocol Version Numbers

If deployed, LDAP V3 in accordance with RFC-4510

7.4.2 Lightweight Directory Access Protocol Extensions

No Stipulation.

7.5 Digital Certificate Fields and Root CA Certificate Hashes

7.5.1 Digital Certificate Fields

<table>
<thead>
<tr>
<th>Standard Certificates</th>
<th>Qualified Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Authority Key Identifier</td>
</tr>
<tr>
<td>Serial number</td>
<td>Subject Key Identifier</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>Key Usage</td>
</tr>
<tr>
<td>Issuer</td>
<td>Private Key Usage</td>
</tr>
<tr>
<td>Validity</td>
<td>Certificate Policies</td>
</tr>
<tr>
<td>Subject</td>
<td>Policy Mappings</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>Subject Alternative Name</td>
</tr>
<tr>
<td>Place of Birth</td>
<td>Issuer Alternative Name</td>
</tr>
<tr>
<td>Title</td>
<td>Subject Directory Attributes</td>
</tr>
<tr>
<td>Residence</td>
<td>Subject Unique Identifier</td>
</tr>
<tr>
<td>Country</td>
<td>Basic Constraints</td>
</tr>
<tr>
<td>Subject Public Key Info</td>
<td></td>
</tr>
<tr>
<td>Issuer Unique Identifier</td>
<td></td>
</tr>
<tr>
<td>Subject Unique Identifier</td>
<td></td>
</tr>
</tbody>
</table>
7.5.2 DarkMatter CA Certificate Hashes

Note that all DarkMatter CA Certificates and CRLs are available for download from the DarkMatter CA Repository at:

http://ca.darkmatter.ae/

The following table provides all DarkMatter Publicly Trusted Root and Issuing CA Certificate information and hashes. (NOTE: None of the following CAs are Bridge CAs):

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>CN = UAE Global Root CA G3, O = UAE Government, C = AE</td>
</tr>
<tr>
<td>Serial Number</td>
<td>47 0e ff 0b 2e b3 83 40</td>
</tr>
<tr>
<td>Cert/Key Hashes</td>
<td>SKI: f8 77 be 28 15 ad e8 52 17 98 06 a7 b6 20 52 95 82 81 0e 65</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): a1 15 92 a2 13 7b 09 65 c4 ae 2b c3 6e d5 9f 95 61 d9 e3 63</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA25 6): 0A 9A 40 13 AF C0 56 50 94 5C CA 63 B9 2A 6B 26 58 57</td>
</tr>
<tr>
<td></td>
<td>CF 40 34 03 DE A5 2E 0E 68 CC 4E 1B F5 74</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>CN = UAE Global Root CA G4, O = UAE Government, C = AE</td>
</tr>
<tr>
<td>Serial Number</td>
<td>1e 86 4a 1c 01 b1 46 3f</td>
</tr>
<tr>
<td>Field</td>
<td>Certificate Profile</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>Cert/Key Hashes</strong></td>
<td>SKI: d5 2f 9a e9 e8 17 00 d9 57 52 d0 3f 07 2b 4f 66 08 eb f5 54</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): 21 a4 a2 79 22 b2 01 e7 cd 45 6d 12 a8 08 53 4b 16 e0 6e 46</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA256): 3E 83 A6 C7 80 B4 C5 B8 75 3B AD 2E 43 A2 03 70 8F F7 FF 29 BE DC 7B 20 62 6B F7 C0 09 19 9C 0A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>CN = DarkMatter Root CA G3, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>6a e6 cc d1 a8 29 7f eb</td>
</tr>
<tr>
<td><strong>Cert/Key Hashes</strong></td>
<td>SKI: ee 7d 9e fb 00 70 b0 fa 5c 0c 76 da a4 12 d1 1b d0 d1 1c a0</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): 14 fc c6 30 77 a7 c0 85 f5 e1 c3 74 20 81 25 ca 7a 21 5d d7</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA256): E6 87 29 01 3A 50 40 4D C1 BA F7 12 7B 3D 3C 9B A8 FF 39 2B 73 5D 0B 11 40 85 8D 5B 91 C3 BE 65</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>CN = DarkMatter Root CA G4, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>61 17 4d f7 2b ec 5f 84</td>
</tr>
<tr>
<td><strong>Cert/Key Hashes</strong></td>
<td>SKI: 89 01 3b cc 49 ba 96 2c 6d c7 84 84 99 13 4f 32 f1 b1 25 f4</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): 77 a9 2d f7 bc aa 14 1f 74 c7 4c 2b b7 65 cb c3 17 f5 49 0f</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA256): 51 58 69 A4 35 D6 D4 7D 3E B8 F3 8D 6F 91 9B EC 83 F2 A5 6A D3 1C C1 AE DE 4F 7B 89 DA 69 E4 BF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>CN = DarkMatter High Assurance CA, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td><strong>Issuer</strong></td>
<td>CN = QuoVadis Root CA 2 G3, O = QuoVadis Limited, C = BM</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>14 ed 7e 90 75 b6 ae 86 8e 1a 3b 02 4f 8a 94 af c8 f5 db ba</td>
</tr>
<tr>
<td><strong>Cert/Key Hashes</strong></td>
<td>SKI: 5d f1 fb 6a 67 81 e6 84 5b 57 37 5c 0f 99 b5 dc 9d 44 3b 55</td>
</tr>
<tr>
<td></td>
<td>AKI: ed e7 6f 76 5a bf 60 ec 49 5b c6 a5 77 bb 72 16 71 9b c4 3d</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): d3 fd 32 5d 0f 22 59 f6 93 dd 78 94 30 e3 a9 43 0b b5 9b 98</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA256):</td>
</tr>
<tr>
<td>Field</td>
<td>Certificate Profile</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>CN = DarkMatter Secure CA, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td><strong>Issuer</strong></td>
<td>CN = QuoVadis Root CA 2 G3, O = QuoVadis Limited, C = BM</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>62 7a 61 b1 0e 7f 5f 27 be 3b eb 5e 94 cf 7f f4 48 de e1 c5</td>
</tr>
<tr>
<td><strong>Cert/Key Hashes</strong></td>
<td>SKI: a2 50 a4 70 cb 3b b5 ca 61 94 27 13 96 3a 74 76 aa 9d ec 34</td>
</tr>
<tr>
<td></td>
<td>AKI: ed e7 6f 76 5a bf 60 ec 49 5b c6 a5 77 bb 72 16 71 9b c4 3d</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): 3a d0 10 24 7a 8f 1e 99 1f 8d de 5d 47 98 9c b5 20 2e 56 14</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA256): A2 5A 19 54 68 19 D0 48 00 0E F9 C6 57 7C 4B CD 8D 21 55 B1 E4 34 6A 45 99 D6 CB B7 97 99 D4 A1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>CN = DarkMatter Assured CA, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td><strong>Issuer</strong></td>
<td>CN = QuoVadis Root CA 3 G3, O = QuoVadis Limited, C = BM</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>19 ff 34 56 9d 36 6b a1 f6 6e 8d 95 32 ee 05 d0 55 b9 dd 1d</td>
</tr>
<tr>
<td><strong>Cert/Key Hashes</strong></td>
<td>SKI: 05 61 41 c6 3d 0d 28 be 62 9f 98 f3 af a3 33 ea c0 fd f0 e9</td>
</tr>
<tr>
<td></td>
<td>AKI: c6 17 d0 bc a8 ea 02 43 f2 1b 06 99 5d 2b 90 20 b9 d7 9c e4</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): 9f eb 09 1e 05 3d 1c 45 3c 78 9e 8e 9c 44 6d 31 cb 17 7e d9</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA256): D8 88 8F 4A 84 F7 4C 97 4D FF B5 73 A1 BF 5B BB AC D1 71 3B 90 50 96 F8 EB 01 50 62 BF 39 6C 4D</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>CN = DarkMatter Audit CA, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td><strong>Issuer</strong></td>
<td>CN = DarkMatter Root CA G4, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>7b 02 f9 f1 42 64 c1 42</td>
</tr>
<tr>
<td><strong>Cert/Key Hashes</strong></td>
<td>SKI: 67 b2 7d 71 d7 df 37 30 4b b6 ec a5 df 8a fe 88 7f cf af 64</td>
</tr>
<tr>
<td></td>
<td>AKI: 89 01 3b cc 49 ba 96 2c 6d c7 84 84 99 13 4f 32 f1 b1 25 f4</td>
</tr>
<tr>
<td>Field</td>
<td>Certificate Profile</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>CN = DigitalX1 High Assurance CA G3, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td><strong>Issuer</strong></td>
<td>CN = UAE Global Root CA G3, O = UAE Government, C = AE</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>75 50 d6 6f 78 b4 bd f5</td>
</tr>
<tr>
<td><strong>Cert/Key Hashes</strong></td>
<td></td>
</tr>
<tr>
<td>SKI: 21 74 d1 14 64 fd 9c c0 2d 51 c6 c4 b2 68 4c 83 e6 9d 6b 7d</td>
<td></td>
</tr>
<tr>
<td>AKI: f8 77 be 28 15 ad e8 52 17 98 06 a7 b6 20 52 95 82 81 0e 65</td>
<td></td>
</tr>
<tr>
<td><strong>Cert Hash(Sha1):</strong></td>
<td>6d 15 8f 5f 70 9b ab a8 07 67 7f d4 13 47 ba 72 58 e3 3c b3</td>
</tr>
<tr>
<td><strong>Cert Hash (SHA256):</strong></td>
<td>FD D7 C3 D8 9D 64 50 9E 00 83 60 40 2F CB 1B E1 C0 CB E2 20 D3 D2 82 AF 1F 9B 3D 8E 19 B3 E4 A4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>CN = DigitalX1 High Assurance CA G4, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td><strong>Issuer</strong></td>
<td>CN = UAE Global Root CA G4, O = UAE Government, C = AE</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>6e e0 2c 70 c9 43 17 16</td>
</tr>
<tr>
<td><strong>Cert/Key Hashes</strong></td>
<td></td>
</tr>
<tr>
<td>SKI: ba 0d c3 da ae 24 a7 38 d8 57 ba e6 87 69 18 f7 61 c9 0a 1a</td>
<td></td>
</tr>
<tr>
<td>AKI: d5 2f 9a e9 e8 17 00 d9 57 52 d0 3f 07 2b 4f 66 08 eb f5 54</td>
<td></td>
</tr>
<tr>
<td><strong>Cert Hash(Sha1):</strong></td>
<td>d3 bb a9 9e f6 ce 18 89 b8 73 8d 39 0e 13 40 5b 00 33 37 c5</td>
</tr>
<tr>
<td><strong>Cert Hash (SHA256):</strong></td>
<td>F2 B7 81 70 44 18 CC 6D 4F 20 0F 74 F5 42 CB 45 C9 1A C7 7C 82 F0 88 91 2A A1 A3 D3 B3 07 F6 1F</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>CN = DM X1 High Assurance CA G3, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td><strong>Issuer</strong></td>
<td>CN = DarkMatter Root CA G3, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td>Serial Number</td>
<td>7d de fe 2d 9f 05 7d 4e</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Cert/Key Hashes</td>
<td>SKI: ba ae ca 30 76 bf b7 69 64 6d 3f bd 06 5c 6d 3b 28 a3 af 9c</td>
</tr>
<tr>
<td></td>
<td>AKI: ee 7d 9e fb 00 70 b0 fa 5c 0c 76 da a4 12 d1 1b d0 d1 1c a0</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): c4 71 ba 59 df 85 b2 64 ad 3d 58 3f be 90 5b d6 48 cb 40 8b</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA256): 89 D3 BF 92 91 48 27 AF EC 62 16 DE 97 70 AC 43 7E E8 C5 F2 27 B3 B2 98 20 A9 EF 33 55 1D BF C6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>CN = DM X1 High Assurance CA G4, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td>Issuer</td>
<td>CN = DarkMatter Root CA G4, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td>Serial Number</td>
<td>40 17 d7 b9 dd ed 20 55</td>
</tr>
<tr>
<td>Cert/Key Hashes</td>
<td>SKI: 58 14 62 fe fe 8e cb 8b a4 1d e3 62 73 bd a9 32 81 99 6d 34</td>
</tr>
<tr>
<td></td>
<td>AKI: 89 01 3b cc 49 ba 96 2c 6d c7 84 84 99 13 4f 32 f1 b1 25 f4</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): 76 33 93 39 6b 4b f9 13 4f bf d2 a3 17 2e ea 1f 4f 90 3d 16</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA256): 27 44 26 9B B8 1D 48 0C 51 B2 1C 1C 26 B7 76 9A 90 56 4E 6D A0 AE 44 24 6D D7 79 CC AC 70 DA 34</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>CN=DigitalX1 Assured CA G4, O=DarkMatter LLC, C=AE</td>
</tr>
<tr>
<td>Issuer</td>
<td>CN = UAE Global Root CA G4, O = UAE Government, C = AE</td>
</tr>
<tr>
<td>Serial Number</td>
<td>6d 9f 01 8e 40 8e 5f 7f</td>
</tr>
<tr>
<td>Cert/Key Hashes</td>
<td>SKI: a6 74 8b d4 25 f6 2f f6 1f d0 95 ab b3 2a e1 f2 5e 35 f4 8a</td>
</tr>
<tr>
<td></td>
<td>AKI: d5 2f 9a e9 e8 17 00 d9 57 52 d0 3f 07 2b 4f 66 08 eb f5 54</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): 91 59 55 d9 99 34 35 aa 05 d8 40 58 d5 76 74 54 93 4c d0 4f</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA256): 35 7f 52 F8 1E 5D AF 02 A0 1A 50 A7 73 7B 50 2F 77 06 72 91 51 63 05 B0 ED 67 50 F2 A0 38 8C 32</td>
</tr>
</tbody>
</table>
### Field Certificate Profile

<table>
<thead>
<tr>
<th>Field</th>
<th>Certificate Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>CN = DM X1 Assured CA G4, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td>Issuer</td>
<td>CN = DarkMatter Root CA G4, O = DarkMatter LLC, C = AE</td>
</tr>
<tr>
<td>Serial Number</td>
<td>71 9c 24 e8 9a d9 44 ab</td>
</tr>
<tr>
<td>Cert/Key Hashes</td>
<td>SKI: 3a d4 91 de 3d 4a 92 7d a5 10 e3 6c 2d d6 51 88 f1 ef 03 94</td>
</tr>
<tr>
<td></td>
<td>AKI: 89 01 3b cc 49 ba 96 2c 6d c7 84 84 99 13 4f 32 f1 b1 25 f4</td>
</tr>
<tr>
<td></td>
<td>Cert Hash(Sha1): bf 46 78 b2 c7 4f d7 3e 93 1f 30 69 ce 88 42 a4 3a 7d 67 dc</td>
</tr>
<tr>
<td></td>
<td>Cert Hash (SHA256): 10 FE EE 3F 39 97 3D BF 0A 06 BE 65 35 78 29 7D 8A 87 5C 3A 5A 55 7F 28 59 8D 59 D2 67 14 B4</td>
</tr>
</tbody>
</table>

# 8 Compliance Audit and Other Assessments

## 8.1 Frequency or Circumstances of Assessment

The DarkMatter CA receives an annual audit by an independent external auditor to assess the DarkMatter CA's compliance with this CPS, any applicable CPs, and other criteria. The audit covers the DarkMatter CA CMSs, Sub CAs, RAs, and each status server that is specified in a certificate issued by the DarkMatter CA.

## 8.2 Identity/Qualifications of Assessor

The DarkMatter CA compliance audits are provided by an independent Auditor. Auditors must meet the following requirements:

**Qualifications and experience:** Auditing must be the auditor’s primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential.

**Expertise:** The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with Public Key infrastructures, certification systems, and Internet security issues.

**Rules and standards:** The auditor must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information
Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.

**Reputation**: The firm must have a reputation for conducting its auditing business competently and correctly.

**Insurance**: EV auditors must maintain Professional Liability/Errors and Omissions Insurance, with policy limits of at least $1 million in coverage.

### 8.3 Assessor’s Relationship to Assessed Entity

The DarkMatter CA auditor does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the DarkMatter CA.

### 8.4 Topics Covered by Assessment

The topics covered by an audit of an the DarkMatter CA will include but may not be limited to:

- the DarkMatter CA business practices disclosure;
- the integrity of the PKI operations;
- Security Policy and Planning;
- Physical Security;
- Technology Evaluation;
- Services Administration;
- Personnel Vetting;
- Contracts; and
- Privacy Considerations;
- the DarkMatter CA’s compliance with other guidelines.

### 8.5 Actions Taken as a Result of Deficiency

If the audit reports a material noncompliance with applicable law, this CPS, or any other contractual obligations related to the DarkMatter CA services, the following actions should be taken:

- The auditor will document the discrepancy,
- The auditor will promptly notify the DarkMatter CA, and
- The DarkMatter CA will develop a plan to treat the noncompliance.

If the deficiency relates to a UAENRCA then DarkMatter will submit the plan to the UAE CA Controller for approval and to any third party that the DarkMatter CA is legally obligated to satisfy. Otherwise the plan is submitted to the DMPPA.

If the DarkMatter CA receives a report of audit deficiency from an Entity CA, the DarkMatter CA may take additional actions to protect the DarkMatter CA level of trust by revoking cross-certificates issued to that Entity (this alternative will execute the revocation procedure described in Section 4.9.1), or take other actions it deems appropriate.
8.6 **Communication of Results**
The results of each audit are reported to the DarkMatter CA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results.

8.7 **Self Audits**
The DarkMatter CA shall perform regular internal audits of its operations, personnel, and compliance with the CP using a randomly selected sample of certificates issued since the last internal audit.

9 **Other Business and Legal Matters**

9.1 **Fees**
The DarkMatter CA reserves the right to charge a fee to each Subscriber in order to support its operations.

9.1.1 **Certificate Issuance or Renewal Fees**
The DarkMatter CA charges fees for certificate issuance and renewal. DarkMatter may change its fees at any time in accordance with the applicable customer agreement.

9.1.2 **Certificate Access Fees**
The DarkMatter CA may charge a reasonable fee for certificate access.

9.1.3 **Revocation or Status Information Access Fees**
The DarkMatter CA does not charge a fee for access to certificate revocation or status information.

9.1.4 **Fees for Other Services**
No stipulation.

9.1.5 **Refund Policy**
Subscribers must request refunds, in writing, within 30 days after a Certificate issues. After receiving the refund request, DarkMatter may revoke the Certificate and refund the amount paid by the Applicant, minus any applicable application processing fees.

9.2 **Financial Responsibility**
This CPS contains no financial limits on the use of certificates issued by the DarkMatter CA or Sub CAs under the policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.
9.2.1 Insurance Coverage
No stipulation.

9.2.2 Other Assets
No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities
No stipulation.

9.3 Confidentiality of Business Information
The DarkMatter CA information not requiring protection is publicly available in its Repositories.

9.3.1 Scope of Confidential Information
The following information is considered confidential and protected against disclosure using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by DarkMatter as private information in accordance with Section 9.4;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor’s letter confirming the effectiveness of the controls set forth in this CPS).

9.3.2 Information Not Within the Scope of Confidential Information
Any information not listed as confidential is considered public information. Published Certificate and revocation data is considered public information.

9.3.3 Responsibility to Protect Confidential Information
DarkMatter’s employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.
9.4 Privacy of Personal Information

9.4.1 Privacy Plan
The DarkMatter CA does not store any other data on certificates other than the data transferred to it and authorized by the Subscriber. Without consent of the data subject or explicit authorization by law, personal data processed by the DarkMatter CA will not be used for other purposes.

9.4.2 Information Treated as Private
DarkMatter treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. DarkMatter protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3 Information not Deemed Private
Private information does not include certificates, CRLs, or their contents.

9.4.4 Responsibility to Protect Private Information
DarkMatter employees and contractors are expected to handle personal information in strict confidence. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5 Notice and Consent to Use Private Information
Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. DarkMatter will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process
DarkMatter may disclose private information, without notice, if DarkMatter believes the disclosure is required by law or regulation.

9.4.7 Other Information Disclosure Circumstances
No stipulation.

9.5 Intellectual Property Rights
DarkMatter and/or its business partners own the intellectual property rights in DarkMatter’s services, including the Certificates, trademarks used in providing the services, and this CPS.
9.6 **Representations and Warranties**

9.6.1 **CA Representations and Warranties**

The DarkMatter CA certificates are issued and revoked at its sole discretion. The DarkMatter CA warrants that its operational procedures comply with this CPS.

For EV Certificates, DarkMatter represents to Subscribers, Subjects, Application Software Vendors that distribute DarkMatter’s root Certificates, and Relying Parties that use a DarkMatter Certificate while the Certificate is valid that DarkMatter followed the EV Guidelines when verifying information and issuing EV Certificates.

This representation is limited solely to DarkMatter’s compliance with the EV Guidelines (e.g., DarkMatter may rely on erroneous information provided in an attorney’s opinion or accountant’s letter that is checked in accordance with the Guidelines).

9.6.2 **RA Representations and Warranties**

RAs represent that:

1. The RA’s certificate issuance and management services conform to the corresponding CP and this CPS,
2. Information provided by the RA does not contain any false or misleading information,
3. Translations performed by the RA are an accurate translation of the original information, and
4. All Certificates requested by the RA meet the requirements of this CPS.

DarkMatter’s agreement with the RA may contain additional representations.

9.6.3 **Subscriber Representations and Warranties**

Prior to being issued and receiving a Certificate, subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber’s Private Key, regardless of whether such use was authorized. Subscribers are required to notify DarkMatter and any applicable RA if a change occurs that could affect the status of the Certificate. Subscribers represent to DarkMatter, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with DarkMatter,
3. Confirm the accuracy of the certificate data prior to using the Certificate,
4. Promptly (i) request revocation of a Certificate, cease using it and its associated Private Key, and notify DarkMatter if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the certificate, and (ii) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
5. Ensure that individuals using Certificates on behalf of an organization have received security training appropriate to the Certificate,
6. Use the Certificate only for authorized and legal purposes, consistent with the certificate purpose, this CPS, any applicable CP, and the relevant Subscriber Agreement, including only installing TLS Certificates on servers accessible at the domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user’s consent, and
7. Promptly cease using the Certificate and related Private Key after the Certificate’s expiration.

9.6.4 Relying Party Representations and Warranties
The DarkMatter CA makes no representation or warranty about the use of certificates issued to any Relying Parties.

9.6.5 Representations and Warranties of Other Participants
The DarkMatter CA makes no representation or warranty for other participants.

9.7 Disclaimers of Warranties
Within the limits under UAE Law the DarkMatter CA does not warrant:

- The accuracy of any information contained in certificates except as it is warranted by the Entity CA that is the party responsible for the ultimate correctness and accuracy of all data transmitted to the DarkMatter CA with the intention to be included in a certificate
- The fitness of any certificate for a particular purpose
- The accuracy, authenticity, completeness or fitness of any information contained in, test prototype or demo certificates

9.8 Limitations of Liability
In no event (except for fraud or willful misconduct) will the DarkMatter CA be liable for:

- Any loss of profits
- Any loss of data
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures
- Any other damages

9.9 Indemnities
This CPS does not include any claims of indemnity.
9.10 Term and Termination

9.10.1 Term
This CPS has no specified term.

9.10.2 Termination
Termination of this CPS is at the discretion of the DMPPA.

9.10.3 Effect of Termination and Survival
The requirements of this CPS remain in effect through the end of the archive period for the last certificate issued.

9.11 Individual Notices and Communications with Participants
The DarkMatter CA use the POC information provided by Subscribers, and as updated by them, when communicating with Subscribers.

9.12 Amendments

9.12.1 Procedure for Amendment
The DMPPA shall review this CPS at least once every year, or when a change is made to the related CPs. If the DMPPA determines modifications to this CPS are required, the change, a change justification will be communicated.

9.12.2 Notification Mechanism and Period
The updated CPS and any subsequent changes shall be made publicly available.

9.12.3 Circumstances Under Which OID Must be Changed
If the DMPPA determines that there is a requirement to change the OIDs, the DarkMatter CA will amend the appropriate documents.

Parties are required to notify the DarkMatter CA and attempt to resolve disputes directly with the DarkMatter CA before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.
9.14 **Governing Law**
The construction, validity, performance and effect of certificates issued under this CPS for all purposes are governed by United Arab Emirates law.

9.15 **Compliance with Applicable Law**
The DarkMatter CA will comply with applicable law.

9.16 **Miscellaneous Provisions**

9.16.1 **Entire Agreement**
The DarkMatter CA shall contractually obligate each sub-CA and RA involved in Certificate issuance to comply with the UAE national CP and applicable industry guidelines.

9.16.2 **Assignment**
This CPS does not assign rights or responsibilities other than what is specified in this CPS.

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

9.16.4 **Enforcement (Attorneys' Fees and Waiver of Rights)**
Failure by any person to enforce a provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

9.16.5 **Force Majeure**
The DarkMatter CA is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond the DarkMatter CA reasonable control.

9.17 **Other Provisions**
No stipulation.
## Annex A: Acronyms

<table>
<thead>
<tr>
<th>Acronyms</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CP</td>
<td>Certificate Policy</td>
</tr>
<tr>
<td>CPS</td>
<td>Certification Practice Statement</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>DMPPA</td>
<td>DarkMatter PKI Policy Authority</td>
</tr>
<tr>
<td>DN</td>
<td>Distinguished Name</td>
</tr>
<tr>
<td>FIPS PUB</td>
<td>Federal Information Processing Standards Publication</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>NPPA</td>
<td>National PKI Policy Authority</td>
</tr>
<tr>
<td>OCSP</td>
<td>Online Certificate Status Protocol</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>RPS</td>
<td>Registration Practices Statement</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest-Shamir-Adleman (encryption algorithm)</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure/Multipurpose Internet Mail Extensions</td>
</tr>
<tr>
<td>UAENRCA</td>
<td>UAE National Root CA</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterrupted Power Supply</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
## Annex B: Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous</td>
<td>Having an unknown name</td>
</tr>
<tr>
<td>Applicant</td>
<td>The subscriber is sometimes also called an &quot;applicant&quot; after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.</td>
</tr>
<tr>
<td>Archive</td>
<td>Long-term, physically separate storage</td>
</tr>
<tr>
<td>Asset</td>
<td>Anything that has value to the organization such as software, information, documentation etc.</td>
</tr>
<tr>
<td>Audit</td>
<td>An independent review of event logs and related activities performed to determine the adequacy of current security measures, to identify the degree of conformance with established policy or to develop recommendations for improvements to the security measures currently applied</td>
</tr>
<tr>
<td>Authentication</td>
<td>Verifying the identity of an entity when that identity is presented</td>
</tr>
<tr>
<td>Authenticity</td>
<td>The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication</td>
</tr>
<tr>
<td>Availability</td>
<td>The property of being accessible and usable upon demand by an authorized entity</td>
</tr>
<tr>
<td>Backup</td>
<td>Copy of files and programs made to facilitate recovery if necessary</td>
</tr>
<tr>
<td>Biometric</td>
<td>A physical or behavioral characteristic of a human being</td>
</tr>
<tr>
<td>Certificate</td>
<td>A digital representation of information which at least identifies the certification authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certification authority issuing it</td>
</tr>
<tr>
<td>Certificate Revocation List</td>
<td>A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date</td>
</tr>
<tr>
<td>Compromise</td>
<td>Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>The property that information is not made available or disclosed to unauthorized individuals, entities, or processes</td>
</tr>
<tr>
<td>Control</td>
<td>Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature</td>
</tr>
<tr>
<td>Cryptographic Module</td>
<td>A related set of hardware or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates</td>
</tr>
<tr>
<td><strong>Cyber Security</strong></td>
<td>Security measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means</td>
</tr>
<tr>
<td><strong>Digital Signature</strong></td>
<td>The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: whether the transformation was created using the private key that corresponds to the public key in the signers digital certificate; and whether the message has been altered since the transformation was made</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>A network protection device that filters incoming and outgoing network data, based on a series of rules</td>
</tr>
<tr>
<td><strong>Guideline</strong></td>
<td>A description that clarifies what should be done and how, to achieve the objectives set out in policies</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td>A generic term for any physical component of information and communication technology</td>
</tr>
<tr>
<td><strong>Information Asset</strong></td>
<td>An Information Asset is a definable piece of information, stored in any manner which is recognized as valuable to the organization. In general, information assets have recognizable and manageable value, risk, content and lifecycles.</td>
</tr>
<tr>
<td><strong>Information Assurance</strong></td>
<td>Practice of protecting information and managing risks related to the use, processing, storage and transmission of information or data, and the systems and processes used for those purposes</td>
</tr>
<tr>
<td><strong>Information Security</strong></td>
<td>Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved</td>
</tr>
<tr>
<td><strong>Information Security Incident</strong></td>
<td>A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>The property of safeguarding the accuracy and completeness of assets</td>
</tr>
<tr>
<td><strong>Intrusion Detection System (IDS)</strong></td>
<td>A security device, resident on a specific host, which monitors system activities for malicious or unwanted behavior</td>
</tr>
<tr>
<td><strong>Key Escrow</strong></td>
<td>A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement</td>
</tr>
<tr>
<td><strong>Key Management</strong></td>
<td>The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction</td>
</tr>
<tr>
<td><strong>Key Pair</strong></td>
<td>Two mathematically related keys having the properties that one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and even knowing the public key, it is computationally infeasible to discover the private key</td>
</tr>
<tr>
<td><strong>Malicious Code or Malware</strong></td>
<td>Any software that attempts to subvert the confidentiality, integrity or availability of a system. Types of malicious code include logic bombs, trapdoors, Trojans, viruses and worms</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Media</strong></td>
<td>A generic term for hardware that is used to store information</td>
</tr>
<tr>
<td><strong>Network Device</strong></td>
<td>Any device designed to facilitate the communication of information destined for multiple system users. For example: cryptographic devices, firewalls, routers, switches and hubs</td>
</tr>
<tr>
<td><strong>Non-Repudiation</strong></td>
<td>Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.</td>
</tr>
<tr>
<td><strong>Online Certificate Status Protocol</strong></td>
<td>Protocol which provides on-line status information for certificates</td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td>Overall intention and direction as formally expressed by management</td>
</tr>
<tr>
<td><strong>Pseudonym</strong></td>
<td>A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing</td>
</tr>
<tr>
<td><strong>Regulator</strong></td>
<td>A government body that sets regulations and monitors compliance and behavior of regulated entities in a particular sector (or market)</td>
</tr>
<tr>
<td><strong>Re-key</strong></td>
<td>To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key</td>
</tr>
<tr>
<td><strong>Remote Access</strong></td>
<td>Access to a system from a location not under the physical control of the system owner</td>
</tr>
<tr>
<td><strong>Repository</strong></td>
<td>A database containing information and data relating to certificates</td>
</tr>
<tr>
<td><strong>Revoke a Certificate</strong></td>
<td>To prematurely end the operational period of a certificate effective at a specific date and time</td>
</tr>
<tr>
<td><strong>Third party</strong></td>
<td>That person or body that is recognized as being independent of the parties involved, as concerns the issue in question</td>
</tr>
<tr>
<td><strong>Zeroize</strong></td>
<td>A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.</td>
</tr>
</tbody>
</table>