| | Dubai Electronic Security Center | Dubai PKI |
|---|---|---|
| | DESC response on Mozilla's Comment # 4 | |

| Comments raised by Mozilla | DESC response |
|---|---|
| **Required and Recommended Practices** | |
| 1.2 CAA Domains listed in CP/CPS: SubCA and Devices CP section 4.2.1<br>NEED:<br>https://wiki.mozilla.org /CA/Required_or_Recommended_Practices#CAA_Domains_listed_in_CP.2FCPS<br>Section 2.2 of the BRs states: "CA's Certificate Policy and/or Certification Practice<br>Statement ... shall clearly specify the set of Issuer Domain Names that the CA<br>recognises in CAA "issue" or "issuewild" records as permitting it to issue. | Section 4.2.1 of the Devices CA CPS was updated to address CAA records check requirements. |
| 2. Audit Criteria: CP/CPS section 8<br>NEED:<br>Clarify Government subCA, since things like BR Commitment to comply and audit criteria are different in that CPS.<br>e.g. Are the Government subCAs all technically constrained via EKU and name constraints?<br>Is that documented in the CPS?<br>CPS indicates that the Government subCAs or not constrained.<br>Mozilla trusts at the root cert level, such that all subCAs chaining up to that root cert are trusted, and so must fully comply with Mozilla's root store policy and the BRs. If the Government subCA is not able to fully comply with Mozilla requirements, then this CA will need to separate out the two hierarchies.<br>Another option is to change this request to be for inclusion of the Devices subCA as a trust anchor. | The Root CAs for Government entities will be operated by DESC and not by other entities. That is mentioned in the Root CA CPS at sections 1.1, 1.3.1 and 1.3.3. the Root CA CPS is published at the below link:<br>https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DubaiRootCA-CertificationPracticeStatement_v1.2.pdf<br><br>All the Subordinate CAs to be issued under the government Root CAs will be technically constrained as mentioned in the CPS as well, see sections 1.1, 1.3.1, 1.3.3.<br><br>On the mechanism of applying constraints, constraints will be applied via EKU and/or name constraints. |
| 4. Verifying Domain Name Ownership: CP/CPS sections 3.2.2, 3.2.3, 3.2.4<br>NEED:<br>I did not find sufficient information about Domain Validation in the CP/CPS.<br>https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Domain_Name_Ownership | Section 3.2.4 of the Devices CA CPS was updated with details on the domain validation. Please see updated version at the following link:<br>https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DevicesCA-CertificationPracticeStatement_v1.2.pdf |
| 5. Verifying Email Address Control:<br>NEED:<br>Not found in CP/CPS<br>https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Email_Address_Control | Sections 3.2.3 of the Corporate CA CPS was updated to address the validation of email ownership.<br>https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-CorporateCA-CertificationPracticeStatement_v1.2.pdf |
| 7. OCSP: SubCA and Devices CP section 4.9.9, CPS section 7.3<br>- OCSP SHALL NOT respond "Good" for unissued certs:<br>NEED: Certificate status is 'Revoked' expecting 'Unknown' | We are using "Revoked" as recommend in the RFC 6960. |

| | |
|---|---|
| https://certificate.revocationcheck.com/good.pki.desc.gov.ae | Can you please clarify why are you suggesting to use "Unknown"? |
| **Forbidden and Potentially Problematic Practices** | |
| 2. Non-Standard Email Address Prefixes for Domain Ownership Validation:<br>NEED:<br>I did not find sufficient information about Domain Validation in the CP/CPS.<br>https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Domain_Name_Ownership | Section 3.2.4 of the Devices CA CPS was updated with details on the domain validation. |
| **Technical Information about Root Certificate** | |
| NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs.<br>https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551 | Although this CA was established to serve entities operating only in Dubai and other emirates within the UAE. Many of these entities are running websites with TLDs that are not ".ae" nor ".gov". Hence applying such constraints would limit the support of an essential part of the target community. We therefore prefer not to apply constrains on the root cert. |
| **Test Results (When Requesting the SSL/TLS Trust Bit)** | |
| NEED: Fix all errors listed here:<br>https://certificate.revocationcheck.com/good.pki.desc.gov.ae | There were two errors reported by the tool:<br><br>Frist was "ERROR: Response is not yet valid". That was fixed.<br><br>Second error is related to the OCSP response for non-issued certificate. We are using "Revoked" as recommend in the RFC 6960.<br>Can you please clarify why the tool is suggesting to use "Unknown"? |
| NEED: The CA MUST check that they<br>are not issuing certificates that violate any of the CA/Browser Forum Baseline<br>Requirements (BRs).<br>BR Lint Test: https://github.com/awslabs/certlint | Since we have not yet issued public certificates, we are using the tool https://crt.sh/linttbscert as advised in the following link https://wiki.mozilla.org/CA/Information_Checklist,<br><br>We test the TLS certificates and the CA certificates capable of issuing TLS certificates. As per the test results, the certificates are compliant with BRs. |
| NEED: The CA MUST check that they are not issuing certificates that violate<br>any of the X.509 rules.<br>X.509 Lint Test: https://github.com/kroeckx/x509lint | Since we have not yet issued public certificates, we are using the tool https://crt.sh/linttbscert as advised in the following link https://wiki.mozilla.org/CA/Information_Checklist,<br><br>We test the TLS certificates and the CA certificates capable of issuing TLS certificates. As per the test results, the certificates are compliant with X.509 rules. |
| **CA Hierarchy Information** | |

# DESC response on Mozilla's Comment # 4

| | |
|---|---|
| CP/CPS section 1.1.1, 1.3.3<br>While DESC aims to set both the SSL trust bit set and the Email trust bit, DESC operates two issuing CAs: the Devices CA issues SSL certificates and the Corporate CA issues email protection certificates, both CAs are operated by DESC and constrained by specific use cases.<br>NEED:<br>This root also issues Unconstrained Root CAs to Government entities. These may be externally-operated by the government entities, and do not appear to be required to follow the BRs and be annually audited. | As explained earlier, the Root CAs that will be issued under DESC root for Government entities will be operated by DESC. |
| DESC CP/CPS allows other Dubai entities to operate their own subordinate CAs certified by Dubai Root. Subordinate CAs operated by external entities will be technically constrained. It is also noted that other entities will be restrained to implement issuing CAs for SSL certificates and hence encouraged mostly to use DESC Devices CA for this service.<br>Further, DESC will continuously disclose their subordinate CAs in the Common CA Database, and maintain annual updates to the corresponding CP/CPS documents.<br>NEED<br>CPS indicates that the Government subCAs or not constrained. Mozilla trusts at the root cert level, such that all subCAs chaining up to that root cert are trusted, and so must fully comply with Mozilla's root store policy and the BRs. If the Government subCA is not able to fully comply with Mozilla requirements, then this CA will need to separate out the two hierarchies. Another option is to change this request to be for inclusion of the Devices subCA as a trust anchor. | As explained earlier, the Root CAs that will be issued under DESC root for Government entities will be operated by DESC.<br>Further, All the subordinate CAs (issuing CAs) that will be operated by other Dubai entities will be technically constrained. |
| NEED: Has this root been involved in cross-signing with any other root? | No |
| **Verification Policies and Practices** | |
| **SSL Verification Procedures**<br><br>CP/CPS sections 3.2.2, 3.2.3, 3.2.4<br>NEED:<br>I did not find sufficient information about Domain Validation in the CP/CPS.<br>https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Domain_Name_Ownership | Section 3.2.4 of the Devices CA CPS was updated with details on the domain validation. |
| **Email Address Verification Procedures**<br><br>NEED:<br>Not found in CP/CPS<br>https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Email_Address_Control | Sections 3.2.5 of the Corporate CA CPS was updated to address the validation of email ownership. |