	Dubai Electronic Security Center	Dubai PKI
	DESC response on Mozilla's Comments on 24th July, 2019	

Comments raised by Mozilla	DESC response
The Devices intermediate is intended for TLS and the Corporate intermediate is intended for S/MIME, but neither is EKU constrained and their respective CPSes only cover one usage or the other. The binding from each certificate to the respective CPS is weak - as far as I can tell, only the name of the CPS is used to indicate the applicable certificate. This creates the possibility each issuing CA could claim to be adhering to whichever CPS is convenient.	There is a different policy identifier for each certificate type that is included in the CP Extension: - SSL: 2.16.784.1.2.2.100.1.2.2.3.2, that is referenced and described only in the Devices CA CPS, - S/MIME: 2.16.784.1.2.2.100.1.2.2.1.1 and 2.16.784.1.2.2.100.1.2.2.1.2, both are referenced and described only in the Corporate CA CPS Further, each CPS has its own separate OID that is also referenced in the certificate CP Extension: - In S/MIME certs, the Corporate CA CPS OID 2.16.784.1.2.2.100.1.2.1.1 is referenced - In SSL certs, the Devices CA CPS OID 2.16.784.1.2.2.100.1.2.1.2 is referenced Please note that DESC has technically configured each CA to issue only the certificates described in the corresponding CPS. Having said that, please let us know if we could answer your concern.
The BR audit statement lists policies applicable to each intermediate in the scope in Appendix A. From this, it's not 100% clear if the Corporate CA is in-scope for the BR audit.	All the CAs and the certificates mentioned in Appendix A are covered by the BR audit. The aspects specific to SSL certificates life cycle management have only been validated on the Devices CA which is the only CA issuing SSL certificates. Please note that while the corporate CA is not issuing SSL certificates, it complies where applicable with the BRs given that it shares common infrastructure components (with proper segregation) with the Devices CA. Also, the same CA management procedures and practices apply for both CAs.
The Corporate CA CPS, which does not cover TLS Certificates, states in section 1.6.3 that it complies with the BRs. Devices CA CPS section 3.2.4 contains an IP address validation method that is forbidden after July 31 due to ballot SC7.	Please refer to the above answer. The Devices CA CPS was updated and published on 31st July. https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DevicesCA-CertificationPracticeStatement_v1.5.pdf
Is the RKGC audit report available? If so, please provide it.	Added as an attachment to the bug record.
Root is valid from 6-Feb 2018 and intermediates are valid from 14-Feb 2018, but period for first period-of-time audit doesn't begin until 28-Feb 2018, leaving a 2-week audit gap.	The CA operations was frozen during those 2 weeks where final approval from DESC management was being granted to start the live operations and expose the CA services. That is why the first Period of Time covered the period from February 26th, 2018 where the actual operations started. Please also note that the auditor was still engaged from the 6th February till the 25th where the Point in Time reports were issued.

	Dubai Electronic Security Center	Dubai PKI
	DESC response on Mozilla's Comments on 24th July, 2019	

Devices CPS section 4.9.1 enumerates reasons for revoking a certificate, but does not list all the reasons required by the BRs. The Subordinate CAs CP also lists revocation reasons without providing a complete set.	The CP and CPSs were updated to incorporate the reasons required by the BRs. https://ca-repository.desc.gov.ae/Repository/source/cp/DubaiPKI-DESCSubordinateCAs-CertificatePolicy_v1.3.pdf https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DevicesCA-CertificationPracticeStatement_v1.5.pdf https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-CorporateCA-CertificationPracticeStatement_v1.3.pdf
Section 4.9 of the Root CA CPS contains a subheading named "Subscribers" that contains no content.	"Subscribers" was meant to be parent heading for section 4.9.1. Anyway, a statement was added to clarify this point. https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DubaiRootCA-CertificationPracticeStatement_v1.3.pdf
Do any Dubai Government Entity Issuing CAs exist at this time? Are any currently planned?	No other issuing CAs existing now, and no any planned this year.
The Corporate CA CPS permits delegated RAs in section 1.3.3 but does not exclude email validation from delegation (section 3.2.3). Delegating email validation is listed as a Forbidden Practice [1].	The BRs stating that the CA may designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization. That is the case at least for the email protection certificates where DESC allows Local RA officer at a Dubai government entity to register the entity's own employees. If it would suffice, we can further specify in the CPS that the LRA can only issue certificate containing emails belonging to the LRA's entity. E.g. if the entity's verified domain name is "xyz.ae" then the LRA shall only issue certificates including emails under that domain such as personname@xyz.ae. Please note that there is no yet any delegation of email verification, this is planned in future once the practices are confirmed with you.
The Dubai Government Entity Issuing CAs CPS lacks a commitment to comply with the BRs.	The BRs along with other standards are indorsed by the Dubai Government Entity Issuing CAs CP as mentioned in section 1.6.3. Currently there is no CPSs since there is no such CAs established yet. In addition, these Issuing CAs will be all technically constrained, fall under the supervision of DESC (Dubai PKI PA) and will operate according to the contractual, audit and policy requirements applicable to Subordinate certification authorities (CA) as stated in the Root CA CPS section 1.3.3. Please let us know if we could answer your clarification.
Mozilla Policy section 5.2 forbids CA generation of Subscriber key pairs. Devices CPS section 6.1.1.2 permits local RAs to do this, which I believe violates the intent if not the letter of Mozilla policy. The Dubai Government Entity Issuing CAs CPS section 6.1.1.2 also grants the right to generate subscriber key pairs without restriction.	That was a typo error in the CPS. As mentioned at the first line under section 6.1.1.2; the CA does not perform Subscriber key generation. The typo was fixed in the CPS. https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DevicesCA-CertificationPracticeStatement_v1.5.pdf

	Although it is not foreseen that the government entities CAs will generate subscriber keys, we have explicitly added the exclusion endorsed by Mozilla Policy section 5.2. https://ca-repository.desc.gov.ae/Repository/source/cp/DubaiPKI-DubaiGovernmententityissuingCA-CertificatePolicy_v1.3.pdf
Section 1.4.1 of the Subordinate CAs CP and CPS' grants DESC the right to issue short-lived "test" certificates. The implication is that these certificates do no need to be validated in accordance with Mozilla policies.	The objective of issuing "test" certificates is to conduct pre-production testing on the production environments. Although such certificates are never exposed to any third-party and used only for DESC internal test, DESC decided to disclose this in the CPS for transparency reasons. Having said that, can you please clarify your concern here. Are you just declaring that you are not going to validate such certificates against Mozilla's policies?
Devices CPS section 7.1.3 describes the CN of a "VPN certificate" as "System unique common name or DNS name or IP address that are applicable, potentially linked to the Subject Alternative Name extension" This implies that certificates which are in-scope for the Bus and Mozilla policy may contain internal domain names in the CN field.	Please see section 3.1.5 where it is clearly mentioned that "The usage of internal domain names and reserved IP addresses is prohibited."
What is the purpose of the "Verification Response Signing Certificate" profile described in section 7.1.5, and why is there no EKU extension? This profile appears to be in scope for Mozilla policy and is clearly not BR compliant (36 month validity).	DESC is offering digital signature verification service to its relaying parties, this service is used by relaying parties to verify document signatures produced using certificates issued from DESC. The "Verification Response Signing Certificate" certificate is used to sign the response of the verification service to establish integrity of the verification response sent from the service. Please note that this certificate is used only by DESC for the service mentioned above.
Section 1.5.2 of these CP/CPSs does not provide the clear instructions for problem reporting required by BR 4.9.3	Sections 1.5.2 of the CPSs were updated with the contact and procedure for certificate problem reporting. https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DevicesCA-CertificationPracticeStatement_v1.5.pdf https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-CorporateCA-CertificationPracticeStatement_v1.3.pdf