Print this page

Mozilla - CA Program

Case Information

Case Number	00000318	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Dubai Electronic Security Center (DESC)	**Request Status**	Information Verification In Process

Additional Case Information

Subject	Include Dubai PKI root certificate	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1474556

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	http://desc.dubai.ae/	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Verified
Geographic Focus	United Arab Emirates	**Verified?**	Verified
Primary Market / Customer Base	Citizens, residents, and organizations in the UAE.	**Verified?**	Verified
Impact to Mozilla Users	Facilitate seamless trust with users in the UAE.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.

CA's Response to Recommended Practices

1. Publicly Available CP and CPS: CP/CPS sections 2.2, 2.3
1.1 Revision Table, updated annually: CP/CPS Document History section

1.2 CAA Domains listed in CP/CPS: SubCA and Devices CP section 4.2.1
NEED:
https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#CAA_Domains_listed_in_CP.2FCPS
Section 2.2 of the BRs states: "CA's Certificate Policy and/or Certification Practice Statement ... shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue.

1.3 BR Commitment to Comply statement in CP/CPS: CP/CPS section 1.6.3
2. Audit Criteria: CP/CPS section 8

NEED:
Clarify Government subCA, since things like BR Commitment to comply and audit criteria are different in that CPS.
e.g. Are the Government subCAs all technically constrained via EKU and name constraints?
Is that documented in the CPS?
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.

3. Revocation of Compromised Certificates: CP/CPS section 4.9

4. Verifying Domain Name Ownership: CP/CPS sections 3.2.2, 3.2.3, 3.2.4
NEED:
I did not find sufficient information about Domain Validation in the CP/CPS.
https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Domain_Name_Ownership

5. Verifying Email Address Control:
NEED:
Not found in CP/CPS
https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Email_Address_Control

6. DNS names go in SAN: Devices CP sections 3.1.5, 7.1.2
7. OCSP: SubCA and Devices CP section 4.9.9, CPS section 7.3

- OCSP SHALL NOT respond "Good" for unissued certs:
NEED: Certificate status is 'Revoked' expecting 'Unknown'
https://certificate.revocationcheck.com/good.pki.desc.gov.ae

8. Network Security Controls: CP/CPS section 6.7

Verified?

Need Response From CA

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices

https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices

Problematic Practices Statement

I have reviewed Mozilla's lists of Forbidden and Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and

			clarifications noted in the text box below.
CA's Response to Problematic Practices	1. Long-lived Certificates: Devices CP section 7.1.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: NEED: I did not find sufficient information about Domain Validation in the CP/CPS. https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Domain_Name_Ownership 3. Issuing End Entity Certificates Directly From Roots: CP/CPS sections 1.1.1, 1.3.3 4. Distributing Generated Private Keys in PKCS#12 Files: CPS section 6.1.2.2 5. Certificates Referencing Local Names or Private IP Addresses: Devices CP section 3.1.5 6. Issuing SSL Certificates for .int Domains: Devices CP section 3.1.5 7. OCSP Responses Signed by a Certificate Under a Different Root: SubCA and Devices CP section 4.9.9, CPS section 7.3 8. Issuance of SHA-1 Certificates: CP/CPS section 7.1 9. Delegation of Domain / Email Validation to Third Parties: CP/CPS section 1.3	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	UAE Global Root CA G4 E2	**Root Case No**	R00000625
Request Status	Information Verification In Process	**Case Number**	00000318

Certificate Data

Certificate Issuer Common Name	UAE Global Root CA G4 E2
O From Issuer Field	UAE Government
OU From Issuer Field	
Valid From	2018 Feb 06
Valid To	2043 Feb 06
Certificate Serial Number	1FD880704BC71C38000000005A79686B
Subject	CN=UAE Global Root CA G4 E2; OU=; O=UAE Government; C=AE
Signature Hash Algorithm	SHA256WithRSA
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	097AE284F58D0ABBC39AC671F48CE683F86DCB2F
SHA-256 Fingerprint	51A7ECB93ACB55FF0E34CD0ECFD1578978B37E9EDB82FD06F23F6CEC005B986D
Subject + SPKI SHA256	B1F55190ED1B31A51AFF6F1461DB4D4C695E0133ED7749A673BAFDCE80666B36
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This root issues internally and externally (and not-technically-constrained) subCAs.	**Verified?**	Verified
Root Certificate Download URL	https://ca-repository.desc.gov.ae/Repository/source/certs/Dubai_Root_CA.crt	**Verified?**	Verified
CRL URL(s)	http://ca-repository.desc.gov.ae/CRL/Root/uae_global_root_ca_g4_e2_uae_government_ae_crlfilea1.crl http://ca-repository.desc.gov.ae/CRL/Devices/devices_certification_authority_uae_government_ae_crlfilec1.crl	**Verified?**	Verified
OCSP URL(s)	http://ca-services.desc.gov.ae/adss/ocsp	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Verified
Root Stores Included In		**Verified?**	Not Applicable
Mozilla Applied Constraints	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. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid	https://good.pki.desc.gov.ae/	**Verified?**	Verified
Test Website - Expired	https://expired.pki.desc.gov.ae/		
Test Website - Revoked	https://revoked.pki.desc.gov.ae/		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	NEED: Fix all errors listed here: https://certificate.revocationcheck.com/good.pki.desc.gov.ae	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs). BR Lint Test: https://github.com/awslabs/certlint	**Verified?**	Need Response From CA
Test Website Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the X.509 rules. X.509 Lint Test: https://github.com/kroeckx/x509lint	**Verified?**	Need Response From CA

EV Tested		**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CP/CPS section 1.1.1, 1.3.3 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. NEED: 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.	**Verified?**	Need Response From CA
Externally Operated SubCAs	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. Further, DESC will continuously disclose their subordinate CAs in the Common CA Database, and maintain annual updates to the corresponding CP/CPS documents. NEED 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.	**Verified?**	Need Response From CA
Cross Signing	NEED: Has this root been involved in cross-signing with any other root?	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer		**Verified?**	Need Response From CA

Verification Policies and Practices

Policy	CP/CPS documents provided in English	**Verified?**	Verified

Documentation	Audit History: https://ca-repository.desc.gov.ae/		
CA Document Repository	https://ca-repository.desc.gov.ae/	**Verified?**	Verified
CP Doc Language	English		
CP	https://ca-repository.desc.gov.ae/Repository/source/cp/DubaiPKI-DESCSubordinateCAs-CertificatePolicy_v1.1.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DubaiRootCA-CertificationPracticeStatement_v1.1.pdf	**Verified?**	Verified
Other Relevant Documents	https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-CorporateCA-CertificationPracticeStatement_v1.1.pdf https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DevicesCA-CertificationPracticeStatement_v1.1.pdf https://ca-repository.desc.gov.ae/Repository/source/cp/DubaiPKI-DubaiGovernmententityissuingCA-CertificatePolicy_v1.1.pdf	**Verified?**	Verified
Auditor	Auren	**Verified?**	Verified
Auditor Location	Spain	**Verified?**	Verified
Standard Audit	https://www.cpacanada.ca/GenericHandlers/AptifyAttachmentHandler.ashx?AttachmentID=221263	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	5/18/2018	**Verified?**	Verified
BR Audit	https://www.cpacanada.ca/GenericHandlers/AptifyAttachmentHandler.ashx?AttachmentID=221262	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	5/18/2018	**Verified?**	Verified
EV SSL Audit		**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CP/CPS section 1.6.3	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8990948	**Verified?**	Verified
SSL Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.4 NEED: I did not find sufficient information about Domain Validation in the CP/CPS. https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA

EV SSL Verification Procedures	N/A	**Verified?**	Not Applicable
Organization Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.4	**Verified?**	Verified
Email Address Verification Procedures	NEED: Not found in CP/CPS https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CP/CPS Sections 5.1.2, 5.2.1, 5.2.2, 5.2.3	**Verified?**	Verified
Network Security	CP/CPS Section 6.7	**Verified?**	Verified