CA Owner Name:

Dubai Electronic Security Center (DESC) was founded in 2014. Pursuant to Law No. 11 and with the aim to develop and implement information security practices, it has been setting good-practice criteria for cyber security across the Emirate of Dubai.

As part of DESC’s strategic plan, DESC had an initiative to establish a Public Key Infrastructure (PKI) referred to as the “Dubai PKI”. The Dubai PKI comprises the Dubai Root CA that is the trust anchor of this PKI, which comes at the first level of the PKI hierarchy. In order to ensure seamless user experience across UAE, DESC has agreed with the UAE federal government on a standard naming conversion for the UAT public root CAs, accordingly the Dubai Root CA was formally names as “UAE Global Root CA G4 E2”.

CA Email Alias 1: ahmed.alali@desc.gov.ae

CA Email Alias 2: afra.ibrahim@desc.gov.ae

CA Email Alias 3: khawla.hassan@desc.gov.ae

Company Website: http://desc.dubai.ae/

Organizational Type: Government Agency

Geographic Focus: United Arab Emirates.

Primary Market / Customer Base:

Certification services provided by Dubai PKI enable citizens, residents and entities/organizations in Dubai and other emirates in the UAE to conduct secure electronic transactions in addition to signing/encryption of documents and emails. One major initiative supported by Dubai PKI is the nation-wide digitalization initiative which is planned to be open to foreign individuals and companies running businesses in UAE. Dubai PKI also issue certificates to non-natural persons (devices) to secure Machine-to-Machine communication where devices can transact securely leveraging the PKI signing and encryption capabilities.

Impact to Mozilla Users:

Given that, a wide range to Dubai PKI certificate users are using Mozilla products, embedding of the Dubai Root CA in the NSS trust store will facilitate seamless trust and security services offered to end-users and relaying parties.

**-- Required and Recommended Practices --**

Recommended Practices: https://wiki.mozilla.org/CA/Required\_or\_Recommended\_Practices

Do You, as an official representative of this CA agree to the following 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:

**-- Required Practices –**

Publicly Available CP and CPS

* The [CP/CPS](https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DubaiRootCA-CertificationPracticeStatement_v1.1.pdf) is publicly available from the CA's official web site (https://ca-repository.desc.gov.ae/)
* Dubai PKI publishes the CP/CPS in PDF format structured as per the RFC3647 format in English.
* See the root CA [CP/CPS](https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DubaiRootCA-CertificationPracticeStatement_v1.1.pdf) Sections 2.2 and 2.3 for provisions regarding publication availability and frequency.

CP/CPS Revision Table

The Dubai PKI was newly established this year, however the document history section in the CP/CPS documents shows the document revision history.

Audit Criteria

* See CP/CPS Section 8 for audit criteria
* Dubai PKI was audited by Auren, the audit was done according to the following:
	+ WebTrust Principles and Criteria for Certification Authorities v2.1, see <https://cert.webtrust.org/ViewSeal?id=2467>
	+ WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, see <https://cert.webtrust.org/ViewSeal?id=2468>

Revocation of Compromised Certificates

See CP/CPS Section 4.9 for revocation criteria and processing.

Verifying Domain Name Ownership

DESC issues only OV certificates, for that a reasonable measures are followed to identify the entity submitting the request and to authenticate the request as well. See CP/CPS Section 3.2.2, 3.2.3, 3.2.4 for relevant provisions.

Further, the detailed verification procedure are specified as part of DESC internal vetting manual that was covered by the WebTrust audit. DESC verification covers the following mains steps:

* Blacklist check (DESC has its own internally maintained Blacklist)
* Establish requesting entity existence & authorized representatives
* Identify authorized certificate requestors from the requesting entity
* In case of Wildcard certificates, perform Wildcard domain validation
* Check for valid domain TLD
* Check for high-profile certificate requests
* Check CAA records for the domain
* Check ownership of the domain (Email validation, website change, DNS record validation)

Baseline Requirements

Baseline requirements are fulfilled as described in the above answer.

WHOIS

DESC relies on direct commands and tools to establish the domain ownership/control. The results are cross-checked and verified against the submitted application details and its related governmental records.

Email Challenge-Response

Email Challenge response is one of the validation method that DESC is using, see the answer to “Verifying Domain Name Ownership”.

Verifying Email Address Control

As part of the verification procedure, DESC is using Challenge-Response mechanism to verify an email to be included in issued certificates.

DNS names go in SAN

For SSL certificates, the Subject Alternative Name extension must be used to define the applicable domain and one or more additional domain names for the certificate. See section 3.1.5 of the Devices CA CPS (https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DevicesCA-CertificationPracticeStatement\_v1.1.pdf).

OCSP

* DESC OCSP responder is set up to listen on the standard HTTP port 80.
* DESC OCSP was tested with Firefox

Network Security Controls

The Dubai PKI was audited against WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, which covers the requirements stated by Mozilla.

CA Hierarchy

See CP/CPS Section 1.1.1 for a visual representation and description of the Dubai PKI hierarchy.

Document Handling of IDNs in CP/CPS

See CP/CPS section 3.1, DESC follows certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names RFC-822 names and X.400 names.

Usage of Appropriate Constraints

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.

For the Subordinate/issuing CAs that will be issued to other Dubai government entities, DESC will always apply appropriate technical constraints.

Pre-Issuance Linting

All certificate profiles are being validated using linting tools such as zlint. Once validation is done, the profiles are configured on the CA so that the tested profiles are enforced during issuance. Variables related to subscribed data is validated and signed off by at least RA officers before issuing the certificate, see CP/CPS section 4.3.1.

**-- Forbidden and Potentially Problematic Practices --**

Potentially Problematic Practices: https://wiki.mozilla.org/CA/Forbidden\_or\_Problematic\_Practices

Do You, as an official representative of this CA agree to the following 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 Practice:

Long-lived Certificates

DESC issues OV certificates for a maximum of 27 months, see section 7.1.2 of the Devices CA CPS.

Non-Standard Email Address Prefixes for Domain Ownership Validation

DESC restricts the email addresses that may be used for domain ownership validation to the following:

* admin@
* administrator@
* webmaster@
* hostmaster@
* postmaster@

Issuing End Entity Certificates Directly From Roots

See CP/CPS section 1.3.3. Dubai root CA only issues certificate to intermediate or issuing CAs with the only exception being the Root CA OCSP certificate that is issued by the Root CA.

Distributing Generated Private Keys in PKCS#12 Files

See CP/CPS section 6.1.2.2, DESC does not generate keys for subscribers.

Certificates Referencing Local Names or Private IP Addresses

See section 3.1.5 of the Devices CA CPS, DESC does not allow issuing certificates to private/internal IP addresses or domain names.

Issuing SSL Certificates for .int Domains:

See section 3.1.5 of the Devices CA CPS, DESC does not issue SSL certs with local names or reserved IP addresses. Further, the Subject Alternative Name extension must be used to define the applicable domain and one or more additional domain names for the certificate.

OCSP Responses Signed by a Certificate Under a Different Root

DESC OCSP response signing certificates are fully compliant with the RFC 2560.

Further, for all DESC CAs (Root and subordinates), each OCSP responder certificate is issued by the respective DESC CAs. Therefore, we do not sign OCSP responder certificates with foreign CAs.

Issuance of SHA-1 Certificates

See CP/CPS section 7.1, DESC does not issue any certificates with SHA-1.

Delegation of Domain / Email Validation to Third Parties

See section 1.3.2 of the Devices CA CPS, the RA for Device CA is restricted to DESC.

Allowing External Entities to Operate Subordinate CAs

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.

Generic Names for CAs

See CP/CPS section 1.1 and 3.1, DESC does not use generic names. Also DESC is following naming conventions for CAs agreed with the UAE PKI regulatory organization to further ensure uniqueness of CA names within the UAE.

Lack of Communication With End Users

See CP/CPS Section 1.5.2 and 9.11 for DESC PA contacts. Further, DESC is going to appoint representatives to participate in international PKI forums.

Backdating the notBefore Date

The time set in the “notBefore” date of the certificates issued by Dubai PKI is 30 minutes behind current time, which is applied for compatibility purposes.

Issuer Encoding in CRL

DESC maintains the same issuer encoding across all certificates and CRLs. See CP/CPS Section 7.1.

**- Policies and Practices -**

Policy Documentation:

The CP/CPS and other documents are provided in English.

CA Document Repository:

CP: https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DubaiRootCA-CertificationPracticeStatement\_v1.1.pdf

CPS: https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DubaiRootCA-CertificationPracticeStatement\_v1.1.pdf

Other Relevant Documents:

<https://ca-repository.desc.gov.ae/>

Auditor Name: Auren

Auditor Website: www.auren.com

Auditor Qualifications: Auren is a licensed practitioner by the WebTrust organization to perform Webtrust Audits and it is qualified in accordance with chapter 8.2 of the CA/Browser Forum

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates version 1.4.1.

Standard Audit URL:

<https://cert.webtrust.org/ViewSeal?id=2467>

Standard Audit Type:

WebTrust Principles and Criteria for Certification Authorities v2.1 (Period-in-time)

Standard Audit Statement Date:

May 18th, 2018

BR Audit URL:

<https://cert.webtrust.org/ViewSeal?id=2468>

BR Audit Type:

WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3 (Period-in-time)

BR Audit Statement Date:

May 18th, 2018

EV SSL Audit URL:

*If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.*

EV SSL Audit Type:

EV SSL Audit Statement Date:

BR Commitment to Comply:

See CP/CPS section 1.6.3 and section 8.

BR Self Assessment:

See document attached to the Bugzilla Bug.

SSL Verification Procedures:

Verifying Domain Name Ownership: DESC issues only OV certificates, for that a reasonable measures are followed to identify the entity submitting the request and to authenticate the request as well. See CP/CPS Section 3.2.2, 3.2.3, 3.2.4 for relevant provisions.

Further, the detailed verification procedure are specified as part of DESC internal vetting manual that was covered by the WebTrust audit. DESC verification covers the following mains steps:

* Blacklist check (DESC has its own internally maintained Blacklist)
* Establish requesting entity existence & authorized representatives
* Identify authorized certificate requestors from the requesting entity
* In case of Wildcard certificates, perform Wildcard domain validation
* Check for valid domain TLD
* Check for high-profile certificate requests
* Check CAA records for the domain
* Check ownership of the domain (Email validation, website change, DNS record validation)

Baseline Requirements: Baseline requirements are fulfilled as described in the above answer.

WHOIS: DESC relies on direct commands and tools to establish the domain ownership/control. The results are cross-checked and verified against the submitted application details and its related governmental records.

Email Challenge-Response: Email Challenge response is one of the validation method that DESC is using, see the answer to “Verifying Domain Name Ownership”.

Verifying Email Address Control: DESC relies on LRA (Local Registration Authority) officers to enable organization to issue and manage certificates for their own communities through the LRAs. An organization needs to sign an LRA agreement with DESC. LRA obligations are documented in the LRA agreement which includes the obligation to verify email address control as and where applicable. At minimum, DESC will verify that the organization signing the LRA agreement will verify email control through a Challenge-Response mechanism.

DNS names go in SAN: For SSL certificates, the Subject Alternative Name extension must be used to define the applicable domain and one or more additional domain names for the certificate. See section 3.1.5 of the Devices CA CPS (https://ca-repository.desc.gov.ae/Repository/source/cps/DubaiPKI-DevicesCA-CertificationPracticeStatement\_v1.1.pdf).

EV SSL Verification Procedures:

*If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate.*

*The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.*

Organization Verification Procedures:

DESC issues only OV certificates, for that a reasonable measures are followed to identify the entity submitting the request and to authenticate the request as well. See CP/CPS Section 3.2.2, 3.2.3, 3.2.4 for relevant provisions.

Email Address Verification Procedures:

As part of the verification procedure, DESC is using Challenge-Response mechanism to verify an email to be included in issued certificates. See CP/CPS Section 3.2.2, 3.2.3, 3.2.4 for relevant provisions.

Multi-Factor Authentication:

See CP/CPS Sections 5.1.2, 5.2.1, 5.2.2, 5.2.3 for authentication requirements for certificate processing.

Network Security:

See CP/CPS Section 6.7.

**-- Technical Information about each Root Certificate --**

***Provide the following information for each root cert for which you are requesting inclusion or change.***

**-- Root Certificate #1 --**

Root Certificate Name: UAE Global Root CA G4 E2

**- Certificate Data -**

Root Certificate Download URL: <https://ca-repository.desc.gov.ae/Repository/source/certs/Dubai_Root_CA.crt>

Certificate Issuer Common Name: UAE Global Root CA G4 E2

O From Issuer Field: UAE Government

OU From Issuer Field:

SHA-256 Fingerprint: 51:A7:EC:B9:3A:CB:55:FF:0E:34:CD:0E:CF:D1:57:89:78:B3:7E:9E:DB:82:FD:06:F2:3F:6C:EC:00:5B:98:6D

CRL URL(s):

<http://ca-repository.desc.gov.ae/CRL/Root/uae_global_root_ca_g4_e2_uae_government_ae_crlfile.crl>

[*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/Root/uae_global_root_ca_g4_e2_uae_government_ae_crlfilea1.crl)

OCSP URL(s):

[*http://ca-services.desc.gov.ae/adss/ocsp/*](http://ca-services.desc.gov.ae/adss/ocsp/)

Mozilla Trust Bits:

*Email; Websites*

SSL Validation Type:

*DV; OV*

Mozilla EV Policy OID(s):

*2.23.140.1.2.2*

Root Stores Included In:

All Mozilla products relying on NSS.

Mozilla Applied Constraints

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

**- Test Websites or Example Cert -**

Test Website - Valid: https://good.pki.desc.gov.ae/

Test Website - Expired: https://expired.pki.desc.gov.ae/

Test Website - Revoked: https://revoked.pki.desc.gov.ae/

Example Cert:

*If requesting Websites trust bit provide 3 URLs to 3 test websites (valid, expired, revoked) whose TLS/SSL cert chains up to this root. - If only requesting the Email trust bit, then attach an example S/MIME cert to the bug.*

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

Revocation Tested: Done

*Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.*

CA/Browser Forum Lint Test: Done with zlint tool.

*The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs).*

BR Lint Test: Done with https://crt.sh/linttbscert.

*https://github.com/awslabs/certlint*

Test Website Lint Test: Done with https://crt.sh/linttbscert.

*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

EV Tested:

*If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV\_Testing\_Easy\_Version*

**- CA Hierarchy Information -**

CA Hierarchy:

See section CP/CPS section 1.1.1.

The Dubai PKI is currently comprises only two Subordinate CA that come at the second level within the PKI hierarchy. Those two CAs are operated by DESC and meant to issue the following certificates types:

Corporate CA:

|  |  |  |
| --- | --- | --- |
| **OID** | **Certificate type** | **Description** |
| 2.16.784.1.2.2.100.1.2.2.1.1 | Encryption certificates | Encryption certificates for corporate individuals and organizations (e.g., emails, documents) |
| 2.16.784.1.2.2.100.1.2.2.1.2 | Authentication certificates | Certificates for authentication and identification purposes |
| 2.16.784.1.2.2.100.1.2.2.1.3 | Digital signature certificates | Digital signing certificates for corporate individuals (e.g., emails, documents) |
| 2.16.784.1.2.2.100.1.2.2.2.1 | Digital signature certificates | Digital signing certificates for organizations (signing for legal persons) |
| 2.16.784.1.2.2.100.1.2.2.2.2 | Code signing certificates | Certificates for (software) code signing purposes |

Devices CA:

|  |  |  |
| --- | --- | --- |
|  **OID** | **Certificate Type** | **Description** |
| 2.16.784.1.2.2.100.1.2.2.3.1 | Device certificates | Certificates for general identification and authentication of devices |
| 2.16.784.1.2.2.100.1.2.2.3.3 | VPN certificates | Device identification and session data encryption for VPN (IPSec-based connections) |
| 2.16.784.1.2.2.100.1.2.2.3.2 | SSL certificates | SSL certificates used for server authentication and session data encryption |
| 2.16.784.1.2.2.100.1.3.1.1 | Time stamping certificates | Certificates intended for the Dubai PKI TSA (Time Stamping Authority) |

Externally Operated SubCAs:

No externally operated Sub CA has been established under DESC Root CA.

Cross Signing:

No Cross signing certificate issued by this root.

Technical Constraint on 3rd party Issuer:

See CP/CPS section 1.1, 1.3.1 and 1.3.3.

*References:*

*- section 7.1.5 of the CA/Browser Forum's Baseline Requirements*

*- Mozilla's Root Store Policy*

**-- End Root Certificate #1 --**