**General information about the CA’s associated organization**

|  |  |
| --- | --- |
| CA Company | National Digital Certification Agency (NDCA) |
| Website URL | http://www.certification.tn |
| Organizational type | Government Agency |
| Primark Market / Customer Base | Which types of customers does the CA serve? Any costumer who need to identify his enterprise website.  Are there particular vertical market segments in which it operates? No  Does the CA focus its activities on a particular country or other geographic region? No |
| Impact to Mozilla Users | The NDCA is the tunisian national certification authority. NDCA operates under Tunisia’s Electronic Signature Law 83-2000 (<http://www.certification.tn/sites/default/files/documents/loi_2000-83_fr.pdf>). All Mozilla users that would like to access Tunisian websites are likely to encounter the root certificate of the NDCA while web browsing, sending/receiving email to their own MTA, sending/receiving S/MIME email, etc. |
| Inclusion in other major browsers | NDCA has already included its root certificate in Microsoft Stores. |
| CA Primary Point of Contact (POC) | POC 1 :  Name : Olfa Kaddachi  Direct email : [olfa.kaddachi@certification.tn](mailto:olfa.kaddachi@certification.tn)  Email Alias : [ndca.pki@certification.tn](mailto:ndca.pki@certification.tn)  CA Phone Number : +216 99 207 378  POC 2 :  Name : Ramzi Khlif  Direct email : [ramzi.khlif@certification.tn](mailto:ramzi.khlif@certification.tn)  Email Alias : [ndca.pki@certification.tn](mailto:ndca.pki@certification.tn)  CA Phone Number : +216 99 207 352 |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Tunisian Root Certificate Authority – TunRootCA2 |
| Certificate Issuer Field | O=National Digital Certification Agency  CN=Tunisian Root Certificate Authority – TunRootCA2  C=TN |
| Certificate Summary | The main purpose of the Tunisian Root Certificate Authority is to issue the Subordinate Certification Authorities of the NDCA. |
| Mozilla Applied Constraints | Not applicable |
| Root Cert URL | <http://www.certification.tn/pub/TunRootCA2.crt> |
| SHA1 Fingerprint | 96:38:63:3C:90:56:AE:88:14:A0:65:D2:3B:DC:60:A0:EE:70:2F:A7 |
| Valid From | 2015-05-05 |
| Valid To | 2027-05-05 |
| Certificate Version | V3 |
| Certificate Signature Algorithm | sha256WithRSAEncryption |
| Signing key parameters | RSA 4096 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | <https://webmail.ance.tn> |
| CRL URL | <http://www.certification.tn/pub/TunRootCA2.crl> |
| OCSP URL (Required now for end-entity certs) | [ocsp.certification.tn](http://ocsp.certification.tn) |
| Requested Trust Bits | Websites; Email; Code Signing. |
| SSL Validation Type | OV |
| EV Policy OID(s) | Not applicable |
| Non-sequential serial numbers and entropy in cert | The serial number contains 16 random ASCII characters which corresponds to 8\*16 =128 bits that are random. |
| Response to Recent CA Communication(s) | Not applicable |

|  |  |
| --- | --- |
| Certificate Name | Tunisian Server Certificate Authority – TunServerCA2 |
| Certificate Issuer Field | O=National Digital Certification Agency  CN=Tunisian Server Certificate Authority – TunServerCA2  C=TN |
| Certificate Summary | The main purpose of the Tunisian Server Certificate Authority is signing governmental SSL certificates. |
| Mozilla Applied Constraints | No constraints. TunServerCA2 CA will have his own constraints for ssl certificate issuance depending on information validation for ssl certificate request. |
| Root Cert URL | <http://www.certification.tn/pub/TunServerCA2.crt> |
| SHA1 Fingerprint | 82:71:03:B2:DA:52:9B:41:6E:14:9F:DF:22:5E:C8:86:44:9C:E7:46 |
| Valid From | 2015-05-07 |
| Valid To | 2025-05-08 |
| Certificate Version | V3 |
| Certificate Signature Algorithm | sha256WithRSAEncryption |
| Signing key parameters | RSA 4096 |
| Test Website URL (SSL)  Example Certificate (non-SSL) | <https://webmail.ance.tn> |
| CRL URL | <http://www.certification.tn/pub/TunServerCA2.crt> |
| OCSP URL (Required now for end-entity certs) | [ocsp.certification.tn](http://ocsp.certification.tn) |
| Requested Trust Bits | Websites; Email. |
| SSL Validation Type | OV |
| EV Policy OID(s) | Not applicable |
| Non-sequential serial numbers and entropy in cert | The serial number contains 16 random ASCII characters which corresponds to 8\*16 =128 bits that are random. |
| Response to Recent CA Communication(s) | N/A |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | Tunisian Server Certificate Authority – TunServerCA2 is an internally operated Subordinate CA. It issues OV SSL certificates. |
| Externally Operated SubCAs | No Externally Operated SubCAs |
| Cross-Signing | No Cross-Signing. |
| Technical Constraints on Third-party Issuers | No Third-party Issuers. |

**Verification Policies and Practices**

|  |  |
| --- | --- |
| Policy Documentation | All the documents are in French, including:  CP/ CPS: French.  Relying Party Agreement: French. |
| Audits | Audit Type: ETSI TS 102 042 V2.4.1 OVCP  Auditor: LSTI  Auditor Website: <http://www.lsti-certification.fr/>  URL to Audit Report and Management’s Assertions: <http://www.certification.tn/11140VA1_ANCE_AF_S.pdf> |
| Baseline Requirements (SSL) | URL to BR audit statement : <http://www.certification.tn/11140VA1_ANCE_AF_S.pdf> |
| SSL Verification Procedures | <http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf>  Page 21-section 3.2 and page 24-section 4.2. |
| Organization Verification Procedures | <http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf>  Page 21-section 3.2 |
| Email Address Verification Procedures | <http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf>  Page 21-section 3.2 |
| Code Signing Subscriber Verification Procedures | Not Applicable. |
| Multi-factor Authentication | All accounts that can cause the approval and/or issuance of end-entity certificates require biometric authentication, possession of the locks' keys and username/password authentication. In addition to that, there are technical controls that are implemented to restrict certificate issuance to a limited set of pre-approved static IP addresses. You can also see section 5.2.3 Page 35 of the CP/CPS :  <http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf> |
| Network Security | Confirmed.  <http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf>  Page 49-section 6.5.1 and Page 50-section 6.7 |

**Response to Mozilla’s CA Recommended Practices** (<https://wiki.mozilla.org/CA:Recommended_Practices>)

|  |  |
| --- | --- |
| Publicly Available CA and CPS |  |
| CA Hierarchy |  |
| Audit Criteria |  |
| Document Handing of IDNs in CP/CPS |  |
| Revocation of Compromised Certificates |  |
| Verifying Domain Name Ownership |  |
| Verifying Email Address Control |  |
| Verifying Identity of Code Signing Certificate Subscriber |  |
| DNS names go in SAN |  |
| Domain owned by Natural Person |  |
| OCSP |  |

**Response to Mozilla’s list of Potentially Problematic Practices** (<https://wiki.mozilla.org/CA:Problematic_Pratices>)

|  |  |
| --- | --- |
| Long-lived DV certificates |  |
| Wildcard DV SSL certificates |  |
| Email Address Prefixes for DV Certs |  |
| Delegation of Domain / Email validation to third parties |  |
| Issuing end entity certificates directly from roots |  |
| Allowing external entities to operate subordinate CAs |  |
| Distributing generated private keys in PKCS#12 files |  |
| Certificates referencing hostnames or private IP addresses |  |
| Issuing SSL Certificates for internal Domains |  |
| OCSP Responses signed by a certificate under a different root |  |
| SHA-1 Certificats |  |
| Generic names for CAs |  |
| Lack of Communications With End Users |  |
| Backdating the notBefore date |  |