**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? NoDoes 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 | Not yet. |
| CA Primary Point of Contact (POC) | POC 1 :Name : Olfa Kaddachi Direct email : olfa.kaddachi@certification.tnEmail Alias : ndca.pki@certification.tnCA Phone Number : +216 99 207 378POC 2 :Name : Ramzi Khlif Direct email : ramzi.khlif@certification.tnEmail Alias : ndca.pki@certification.tnCA Phone Number : +216 99 207 352  |

**Technical information about root CA certificate**

|  |  |
| --- | --- |
| Certificate Name | Tunisia National Root CA |
| Certificate Issuer Field | CN = Tunisia National Root CAO = National Digital Certification AgencyL = TunisC = TN |
| Certificate Summary | The main purpose of the Tunisian National Root Certificate Authority is to issue the Subordinate Certification Authorities of the NDCA.  |
| Mozilla Applied Constraints | Not applicable |
| Root Cert URL | www.certification.tn/pub/TunisianNationalRootCA.crt |
| SHA1 Fingerprint | ‎AF:29:06:F9:E6:9E:C1:86:36:AE:29:ED:5B:B4:08:91:7A:82:B5:07 |
| Valid From | 29 November 2016 |
| Valid To | 29 May 2037 |
| Certificate Version | V3 |
| Certificate Signature Algorithm | sha256WithRSAEncryption |
| Signing key parameters | RSA 4096 |
| CRL URL | http://crl.certification.tn/tunrootca.crl |
| OCSP URL (Required now for end-entity certs) | [va.certification.tn](http://ocsp.certification.tn) |
| Requested Trust Bits | Websites; Email; Code Signing. |
| SSL Validation Type | OV, EV |
| EV Policy OID(s) | 2.16.788.1.2.6.1.10 |
| Non-sequential serial numbers and entropy in cert | Random numbers are generated with Java’s Secure Random, SHA1PRNG.The default length of the certificate serial number is 64-bit |
| Response to Recent CA Communication(s) | Not applicable |

**Technical information about intermediate CA certificate**

|  |  |
| --- | --- |
| Certificate Name | Tunisia Gov CA |
| Certificate DN | CN = Tunisia Gov CAO = National Digital Certification AgencyL = TunisC = TN |
| Certificate Issuer Field | CN = Tunisia National Root CAO = National Digital Certification AgencyL = TunisC = TN |
| Certificate Summary | The main purpose of the Tunisia Gov CA is signing issuing CA (level 3) for governmental organisms. |
| Mozilla Applied Constraints | No constraints.  |
| Root Cert URL | http://crl.certification.tn/tunrootca.crl |
| SHA1 Fingerprint | 9F:81:BE:87:33:2A:67:FC:93:71:1E:5B:FD:FF:6E:3B:7F:46:31:A4 |
| Valid From | 29 November 2016 |
| Valid To | 29 February 2032  |
| Certificate Version | V3 |
| Certificate Signature Algorithm | sha256WithRSAEncryption |
| Signing key parameters | RSA 4096 |
| CRL URL | http://crl.certification.tn/tunisiagovca.crl |
| OCSP URL (Required now for end-entity certs) | [va.certification.tn](http://ocsp.certification.tn) |
| Requested Trust Bits | Websites; Email; Code Signing |
| SSL Validation Type | OV, EV  |
| Non-sequential serial numbers and entropy in cert | Random numbers are generated with Java’s Secure Random, SHA1PRNG.The default length of the certificate serial number is 64-bit |
| Response to Recent CA Communication(s) | N/A |

|  |  |
| --- | --- |
| Certificate Name | Tunisia Corporate CA |
| Certificate DN | CN = Tunisia Corporate CAO = National Digital Certification AgencyL = TunisC = TN |
| Certificate Issuer Field | CN = Tunisia National Root CAO = National Digital Certification AgencyL = TunisC = TN |
| Certificate Summary | The main purpose of the Tunisia Gov CA is signing issuing CA (level 3) for private organisms. |
| Mozilla Applied Constraints | No constraints.  |
| Root Cert URL | http://crl.certification.tn/tunrootca.crl |
| SHA1 Fingerprint | EC:3C:48:68:3A:65:A9:A1:B3:64:2C:F3:D1:B1:1A:17:BC:52:D5:D6 |
| Valid From | 29 November 2016 |
| Valid To | 29 February 2032  |
| Certificate Version | V3 |
| Certificate Signature Algorithm | sha256WithRSAEncryption |
| Signing key parameters | RSA 4096 |
| CRL URL | http://crl.certification.tn/tunisiacorpca.crl |
| OCSP URL (Required now for end-entity certs) | [va.certification.tn](http://ocsp.certification.tn) |
| Requested Trust Bits | Websites; Email; Code Signing |
| Non-sequential serial numbers and entropy in cert | Random numbers are generated with Java’s Secure Random, SHA1PRNG.The default length of the certificate serial number is 64-bit |
| Response to Recent CA Communication(s) | N/A |

**Technical information about issuing CAs certificates**

|  |  |
| --- | --- |
| Certificate Name | TnTrust Gov CA |
| Certificate DN | CN = TnTrust Gov CAO = National Digital Certification AgencyL = TunisC = TN |
| Certificate Issuer Field | CN = Tunisia Gov CAO = National Digital Certification AgencyL = TunisC = TN |
| Certificate Summary | The main purpose of the TnTrust Gov CA is signing governmental SSL certificates (OV SSL). |
| Mozilla Applied Constraints | No constraints.  |
| Root Cert URL | http://crl.certification.tn/tunisiagovca.crl |
| SHA1 Fingerprint | A1:6B:C7:76:BE:65:1E:5E:1A:A1:09:D7:E1:42:6E:F0:42:59:B2:C4 |
| Valid From | 29 November 2016 |
| Valid To | 29 December 2026 |
| Certificate Version | V3 |
| Certificate Signature Algorithm | sha256WithRSAEncryption |
| Signing key parameters | RSA 4096 |
| Test Website URL (SSL)Example Certificate (non-SSL) | [https://tms.certification.tn](https://webmail.ance.tn) |
| CRL URL | http://crl.certification.tn/tntrustgovca.crl |
| OCSP URL (Required now for end-entity certs) | [va.certification.tn](http://ocsp.certification.tn) |
| Requested Trust Bits | Websites; Email; Code Signing |
| SSL Validation Type | EV , OV |
| EV Policy OID(s) | Organisation Validation SSL OVCP OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.1.1Wildcard SSL OVCP OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.1.1Extended Validation SSL EVCP OID: 0.4.0.2042.1.4 OID: 2.16.788.1.2.6.1.9.1.2Code Signing OVCP OID:0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.1.3Extended Validation Code Signing EVCP OID: 0..4.0.2042.1.4 OID: 2.16.788.1.2.6.1.9.1.4 |
| Non-sequential serial numbers and entropy in cert | Random numbers are generated with Java’s SecureRandom, SHA1PRNG.The default length of the certificate serial number is 64-bit |
| Response to Recent CA Communication(s) | N/A |
| Certificate Name | TnTrust Corporate CA |
| Certificate DN | CN = TnTrust Corporate CAO = National Digital Certification AgencyL = TunisC = TN |
| Certificate Issuer Field | CN = Tunisia Corporate CAO = National Digital Certification AgencyL = TunisC = TN |
| Certificate Summary | The main purpose of the TnTrust Gov CA is signing private SSL certificates (OV SSL). |
| Mozilla Applied Constraints | No constraints.  |
| Root Cert URL | http://crl.certification.tn/tunisiacorpca.crl |
| SHA1 Fingerprint | 20:7E:3A:5E:F4:39:A2:99:AD:28:D2:C3:5A:F2:AD:4B:46:A5:9E:12 |
| Valid From | 29 November 2016 |
| Valid To | 29 December 2026 |
| Certificate Version | V3 |
| Certificate Signature Algorithm | sha256WithRSAEncryption |
| Signing key parameters | RSA 4096 |
| CRL URL | http://crl.certification.tn/tntrustcorporateca.crl |
| OCSP URL (Required now for end-entity certs) | [va.certification.tn](http://ocsp.certification.tn) |
| Requested Trust Bits | Websites; Email; Code Signing |
| SSL Validation Type | OV , EV |
| EV Policy OID(s) | Organisation Validation SSL OVCP OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.2.1Wildcard SSL OVCP OID: 0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.2.1Extended Validation SSL EVCP OID: 0.4.0.2042.1.4 OID: 2.16.788.1.2.6.1.9.2.2Code Signing OVCP OID:0.4.0.2042.1.7 OID: 2.16.788.1.2.6.1.9.2.3Extended Validation Code Signing EVCP OID: 0..4.0.2042.1.4 OID: 2.16.788.1.2.6.1.9.2.4 |
| Non-sequential serial numbers and entropy in cert | Random numbers are generated with Java’s SecureRandom, SHA1PRNG.The default length of the certificate serial number is 64-bit |
| Response to Recent CA Communication(s) | N/A |

**CA Hierarchy information for root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | The CA hierarchy is composed by :* Root CA: Tunisian National Root CA
* Intermediate CAs: Tunisa Gov CA and Tunisia Corporate CA
* Issuing CAs:
* TnTrust Gov CA
* TnTrust Qualified Gov CA
* TnTrust Corporate CA
* TnTrust Qualified Gov CA

Only the issuing CAs TnTrust Gov CA and TnTrust Corporate CA issue :* OV and EV SSL certificates.
* OV and EV Code Signing 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 | CP/ CPS: English.Relying Party Agreement: French. |
| Audits | Audit Type: e-IDASAuditor: LSTIAuditor Website: <http://www.lsti-certification.fr/>URL to Audit Report and Management’s Assertions: http://lsti-certification.fr/index.php/eidas/lsti-s-eidas-trusted-list.html |
| Baseline Requirements (SSL) | URL to BR audit statement : http://lsti-certification.fr/index.php/eidas/lsti-s-eidas-trusted-list.html |
| SSL Verification Procedures | [http://www.certification.tn/sites/default/files/documents/](http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf)CP-CPS-Tunisian-National-PKI.pdfSections 3.2 and 4.2. |
| Organization Verification Procedures | [http://www.certification.tn/sites/default/files/documents/](http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf)CP-CPS-Tunisian-National-PKI.pdfSection 3.2 |
| Email Address Verification Procedures | [http://www.certification.tn/sites/default/files/documents/](http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf)CP-CPS-Tunisian-National-PKI.pdfSection 3.2 |
| Code Signing Subscriber Verification Procedures | [http://www.certification.tn/sites/default/files/documents/](http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf)CP-CPS-Tunisian-National-PKI.pdfSection 3.2 |
| 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 of the CP/CPS :[http://www.certification.tn/sites/default/files/documents/](http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf)CP-CPS-Tunisian-National-PKI.pdf |
| Network Security | Confirmed.[http://www.certification.tn/sites/default/files/documents/](http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf)CP-CPS-Tunisian-National-PKI.pdf Sections 6.5.1 and 6.7 |

**Response to Mozilla’s CA Recommended Practices** ([https://wiki.mozilla.org/CA:Recommended\_Practices](https://wiki.mozilla.org/CA%3ARecommended_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](https://wiki.mozilla.org/CA%3AProblematic_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 |  |