Print this page

# Mozilla - CA Program

## Case Information

| | | | |
|---|---|---|---|
| **Case Number** | 00000174 | **Case Record Type** | CA Owner/Root Inclusion Request |
| **CA Owner/Certificate Name** | Government of Tunisia, Agence National de Certification Electronique / National Digital Certification Agency (ANCE/NDCA) | **Request Status** | Need Information from CA |

## Additional Case Information

| | | | |
|---|---|---|---|
| **Subject** | Add Tunisia National Root CA (Tunisia's National PKI) | **Case Reason** | |

## Bugzilla Information

| | |
|---|---|
| **Link to Bugzilla Bug** | https://bugzilla.mozilla.org /show_bug.cgi?id=1402889 |

## General information about CA's associated organization

| | | | |
|---|---|---|---|
| **CA Email Alias 1** | ndca.pki@certification.tn | | |
| **CA Email Alias 2** | | | |
| **Company Website** | http://www.certification.tn | **Verified?** | Verified |
| **Organizational Type** | Government Agency | **Verified?** | Verified |
| **Organizational Type (Others)** | None | **Verified?** | Verified |
| **Geographic Focus** | Tunisia | **Verified?** | Verified |
| **Primary Market / Customer Base** | This is the Tunisian national certification authority. | **Verified?** | Verified |
| **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 | **Verified?** | Verified |

| | |
|---|---|
| | MTA, sending/receiving S/MIME email, etc. |

## 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** | NEED: The wiki page and your CP/CPS have changed, so please verify the answers below.<br>https://wiki.mozilla.org /CA/Required_or_Recommended_Practices<br>And in particular, see<br>https://wiki.mozilla.org /CA/Required_or_Recommended_Practices#Pre-Issuance_Linting<br><br>* Publicly Available CP and CPS: Yes<br>* Audit Criteria: Yes<br>* Revocation of Compromised Certificates: CP/CPS section 4.9<br>* Verifying Domain Name Ownership: CP/CPS section 3.2.2<br>* Verifying Email Address Control: CP/CPS section 3.2.3<br>* DNS names go in SAN: CP/CPS Appendix A1<br>* OCSP: CP/CPS section 2.2<br>* Network Security Controls: CP/CPS section 6.8<br>* CA Hierarchy: CP/CPS section 1.1<br>* Document Handling of IDNs in CP/CPS: CP/CPS section 3.2.2.2<br>* Usage of Appropriate Constraints: CP/CPS section 1.1<br>* Pre-Issuance Linting: ??? | **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** | NEED: The wiki page and your CP/CPS have changed, so please verify the answers below.<br>https://wiki.mozilla.org /CA/Forbidden_or_Problematic_Practices | **Verified?** | Need Response From CA |

* Long-lived Certificates: ??? Note the recent changes in BRs limiting max validity of SSL certs to 825 days.
* Non-Standard Email Address Prefixes for Domain Ownership Validation: ???
* Issuing End Entity Certificates Directly From Roots: No. CP/CPS section 1.1
* Distributing Generated Private Keys in PKCS#12 Files: No. CP/CPS section 3.2.1.1
* Certificates Referencing Local Names or Private IP Addresses: ???
* Issuing SSL Certificates for .int Domains: ???
* OCSP Responses Signed by a Certificate Under a Different Root: No
* Issuance of SHA-1 Certificates: No. CP/CPS section 7.1.3
* Delegation of Domain / Email Validation to Third Parties: Yes. It appears that there are Delegated Registration Authorities - CP/CPS section 1.3.3.
* Allowing External Entities to Operate Subordinate CAs: No. It appears that externally-operated subCAs are not allowed - CP/CPS section 1.3.1.2.
* Generic Names for CAs: No. CP/CPS section 1.1
* Lack of Communication With End Users: No. http://www.certification.tn/en/content/technical-support, support@certification.tn
* Backdating the notBefore Date: The notBefore date is the date of issuing the certificate by the Server CA. The timestamp is always set to 00:00:00 GMT.
* Issuer Encoding in CRL: ???

# Root Case Record # 1

## Root Case Information

| | | | |
|---|---|---|---|
| **Root Certificate Name** | Tunisia National Root CA | **Root Case No** | R00000315 |
| **Request Status** | Need Information from CA | **Case Number** | 00000174 |

## Certificate Data

| | |
|---|---|
| **Certificate Issuer Common Name** | Tunisia National Root CA |

| | |
|---|---|
| **O From Issuer Field** | National Digital Certification Agency |
| **OU From Issuer Field** | |
| **Valid From** | 2016 Nov 29 |
| **Valid To** | 2037 May 29 |
| **Certificate Serial Number** | 683e1155929c8e8e |
| **Subject** | CN=Tunisia National Root CA, OU=null, O=National Digital Certification Agency, C=TN |
| **Signature Hash Algorithm** | sha256WithRSAEncryption |
| **Public Key Algorithm** | RSA 4096 bits |
| **SHA-1 Fingerprint** | AF:29:06:F9:E6:9E:C1:86:36:AE:29:ED:5B:B4:08:91:7A:82:B5:07 |
| **SHA-256 Fingerprint** | 4F:BA:9F:8B:2B:F7:0D:94:7F:F8:47:C1:5F:BA:65:13:38:84:01:8A:9B:B2:B2:E2:09:B8:33:C9:3F:57:B6:7C |
| **Certificate Fingerprint** | 8A:10:B0:0B:AB:71:CC:2A:9C:64:27:C4:FA:69:78:11:A1:EF:1D:A5:3D:8F:3A:C0:55:45:33:67:D4:78:AF:9E |
| **Certificate Version** | 3 |

## Technical Information about Root Certificate

| | | | |
|---|---|---|---|
| **Certificate Summary** | This root certificate has two subordinate CAs, "Tunisia Gov CA" and "Tunisia Corporate CA". Both subCAs have two subordinate CAs, one for issuing Qualified signature certs, and the other for issuing SSL, Code Signing, VPN, and Timestamping certs. | **Verified?** | Verified |
| **Root Certificate Download URL** | www.certification.tn/pub /TunisianNationalRootCA.crt | **Verified?** | Verified |
| **CRL URL(s)** | http://crl.certification.tn /tntrustcorporateca.crl CPS section 4.9.7: CRL of the issuing CAs are issued every twenty four (24) hours or whenever a certificate is revoked. | **Verified?** | Verified |
| **OCSP URL(s)** | http://va.certification.tn CPS section 4.9.9 | **Verified?** | Verified |
| **Mozilla Trust Bits** | Email; Websites | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| **SSL Validation Type** | OV; EV | **Verified?** | Verified |
| **Mozilla EV Policy OID(s)** | 2.23.140.1.1 | **Verified?** | Verified |
| **Root Stores Included In** | | **Verified?** | Verified |
| **Mozilla Applied Constraints** | NEED: Mozilla has the ability to name constrain root certs; e.g. to *.tn. Shall we name constrain this root cert to *.tn? | **Verified?** | Need Response From CA |

## Test Websites or Example Cert

| | | | |
|---|---|---|---|
| **Test Website - Valid** | https://valid-corp-ev.certification.tn/ | **Verified?** | Verified |
| **Test Website - Expired** | https://expired-corp-ev.certification.tn | | |
| **Test Website - Revoked** | https://revoked-corp-ev.certification.tn | | |
| **Example Cert** | | | |
| **Test Notes** | The test website response times are extremely slow. | | |

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

| | | | |
|---|---|---|---|
| **Revocation Tested** | NEED: Fix or explain all errors here: https://certificate.revocationcheck.com/valid-corp-ev.certification.tn | **Verified?** | Need Response From CA |
| **CA/Browser Forum Lint Test** | NEED: BR Lint Test: https://github.com/awslabs/certlint<br><br>It would really help if at lest the test certs are logged to a CT log.<br>I can't even find the root cert in crt.sh to run the tests. | **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.<br>X.509 Lint Test: https://github.com/kroeckx/x509lint | **Verified?** | Need Response From CA |
| **EV Tested** | NEED: 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<br><br>I tried to run this test with the valid test website above, but it seems to time out. | **Verified?** | Need Response From CA |

## CA Hierarchy Information

| | | | |
|---|---|---|---|
| **CA Hierarchy** | Section 1.1 of the CP/CPS: This root certificate has two subordinate CAs, "Tunisia Gov CA" and "Tunisia Corporate CA". Both subCAs have two subordinate CAs, one for issuing Qualified signature certs, and the other for issuing SSL, Code Signing, VPN, and Timestamping certs. | **Verified?** | Verified |
| **Externally Operated SubCAs** | Currently none, but the CP/CPS allows it, see section 3.2.6:<br>The requirements to be met by the authority are included but are not limited to:<br>- Signing a contractual agreement with the National Digital Certification Agency,<br>- Being compliant with the stipulations of this CP/CPS,<br>- Having passed and keeping current a WebTrust or ETSI audit,<br>- Publishing its own CP/CPS. | **Verified?** | Verified |
| **Cross Signing** | None | **Verified?** | Verified |
| **Technical Constraint on 3rd party Issuer** | Delegated Registration Authorities (DRAs) are allowed -- CP/CPS section 1.3.3. DRAs have contractual agreement to abide by the CP/CPS and have an annual audit. | **Verified?** | Verified |

## Verification Policies and Practices

| | | | |
|---|---|---|---|
| **Policy Documentation** | CP/CPS provided in English | **Verified?** | Verified |
| **CA Document Repository** | http://www.certification.tn/en/content/certificate-policy | **Verified?** | Verified |
| **CP Doc Language** | English | | |
| **CP** | http://www.certification.tn/pub/CPCPS-TunisianNationalPKI.pdf | **Verified?** | Verified |
| **CP Doc Language** | English | | |
| **CPS** | http://www.certification.tn/pub/CPCPS-TunisianNationalPKI.pdf | **Verified?** | Verified |
| **Other Relevant Documents** | http://www.certification.tn/en/content/downloads | **Verified?** | Verified |
| **Auditor (New)** | LSTI | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| **Auditor Location (New)** | France | **Verified?** | Verified |
| **Standard Audit** | https://bug1402889.bmoattachments.org/attachment.cgi?id=8951807 | **Verified?** | Verified |
| **Standard Audit Type** | ETSI EN 319 411 | **Verified?** | Verified |
| **Standard Audit Statement Date** | 9/13/2017 | **Verified?** | Verified |
| **BR Audit** | https://bug1402889.bmoattachments.org/attachment.cgi?id=8951807 | **Verified?** | Verified |
| **BR Audit Type** | ETSI EN 319 411 | **Verified?** | Verified |
| **BR Audit Statement Date** | 9/13/2017 | **Verified?** | Verified |
| **EV SSL Audit** | https://bug1402889.bmoattachments.org/attachment.cgi?id=8951807 | **Verified?** | Verified |
| **EV SSL Audit Type** | ETSI EN 319 411 | **Verified?** | Verified |
| **EV SSL Audit Statement Date** | 9/13/2017 | **Verified?** | Verified |
| **BR Commitment to Comply** | CP/CPS section 1 | **Verified?** | Verified |
| **BR Self Assessment** | https://bugzilla.mozilla.org/attachment.cgi?id=8911846 | **Verified?** | Verified |
| **SSL Verification Procedures** | CP/CPS section 3.2.2 | **Verified?** | Verified |
| **EV SSL Verification Procedures** | CP/CPS section 3.2.2.1 | **Verified?** | Verified |
| **Organization Verification Procedures** | CP/CPS section 3.2.3, 3.2.5 | **Verified?** | Verified |
| **Email Address Verification Procedures** | CP/CPS section 3.2.3 | **Verified?** | Verified |
| **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 section 5.2.3 | **Verified?** | Verified |
| **Network Security** | CP/CPS section 6.8 | **Verified?** | Verified |