

# Mozilla - CA Program

## Case Information

<b>Case Number</b>	00000076	<b>Case Record Type</b>	CA Owner/Root Inclusion Request
<b>CA Owner/Certificate Name</b>	Government of Tunisia, Agence National de Certification Electronique / National Digital Certification Agency (ANCE/NDCA)	<b>Request Status</b>	Ready for Public Discussion

## Additional Case Information

<b>Subject</b>	Include Government of Tunisia Root	<b>Case Reason</b>	
----------------	------------------------------------	--------------------	--

## Bugzilla Information

<b>Link to Bugzilla Bug</b>	<a href="https://bugzilla.mozilla.org/show_bug.cgi?id=1233645">https://bugzilla.mozilla.org/show_bug.cgi?id=1233645</a>
-----------------------------	---

## General information about CA's associated organization

<b>CA Email Alias 1</b>	ndca.pki@certification.tn		
<b>CA Email Alias 2</b>			
<b>Company Website</b>	<a href="http://www.certification.tn/">http://www.certification.tn/</a>	<b>Verified?</b>	Verified
<b>Organizational Type</b>	Government Agency	<b>Verified?</b>	Verified
<b>Organizational Type (Others)</b>		<b>Verified?</b>	Not Applicable
<b>Geographic Focus</b>	Tunisia	<b>Verified?</b>	Verified
<b>Primary Market / Customer Base</b>	This is the Tunisian national certification authority.	<b>Verified?</b>	Verified
<b>Impact to Mozilla Users</b>	National Digital Certification Agency (NDCA) operates under Tunisia's Electronic Signature Law 83-2000 ( <a href="http://www.certification.tn/sites/default/files/documents/loi_2000-83_fr.pdf">http://www.certification.tn/sites/default/files/documents/loi_2000-83_fr.pdf</a> ). 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.	<b>Verified?</b>	Verified

## Required and Recommended Practices

<b>Recommended Practices</b>	<a href="https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices">https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices</a>	<b>Recommended Practices Statement</b>	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
<b>CA's Response to</b>	1) Publicly Available CP and CPS: Yes 2) CA Hierarchy: Yes	<b>Verified?</b>	Verified

**Recommended Practices**

- 3) Audit Criteria: Yes
- 4) Document Handling of IDNs in CP/CPS: Use of IDNs isn't allowed. The CA does not allow the use of a domain name containing non-ASCII characters in certificates.
- 5) Revocation of Compromised Certificates: Server CP section 4.9
- 6) Verifying Domain Name Ownership: Yes
- 7) Verifying Email Address Control: Not applicable, Email trust bit not requested.
- 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable.
- 9) DNS names go in SAN: Yes. This extension contains at least one entry. Each entry is either a DNS Name containing the FQDN or the IP address of a server.
- 10) Domain owned by a Natural Person: Not applicable. The CA does not issue certificates for Natural Person. See <http://www.certification.tn/rpa>
- 11) OCSP: Yes
- 12) Network Security Controls: Yes

**Forbidden and Potentially Problematic Practices**

**Potentially Problematic Practices**

[https://wiki.mozilla.org/CA:Problematic\\_Practices#Potentially\\_problematic\\_CA\\_practices](https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices)

**Problematic Practices Statement**

I have reviewed Mozilla's list of 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 DV certificates: No. The CA does not issue long-lived SSL certs.
- 2) Wildcard DV SSL certificates: OV certificates may include a wildcard asterisk character. Before issuing a Wildcard cert the RA verifies that the applicant has either the right to use or control the FQDN listed in the certificate, or is authorized by a person having such rights in order to obtain a certificate containing the FQDN (see section 4.2.1 of the CP)
- 3) Email Address Prefixes for DV Certs: For each FQDN to be included in a certificate, the Server CA confirms that the applicant is either the Domain Name Registrant or has control over the FQDN using the information listed in the "registrant", "technical", or "administrative" WHOIS records.
- 4) Delegation of Domain / Email validation to third parties: Not Applicable (No Delegation of domain/email validation to third parties.
- 5) Issuing end entity certificates directly from roots: No
- 6) Allowing external entities to operate subordinate CAs: No
- 7) Distributing generated private keys in PKCS#12 files: No. Subscribers generate their own key pairs. The CA does not issue the private key for the end-user (sections 6.1.2.2 and 6.1.3).
- 8) Certificates referencing hostnames or private IP addresses: No, the Server CA issues only SSL certificates which refer to domain names that are resolvable using the public DNS infrastructure.
- 9) Issuing SSL Certificates for Internal Domains: No, the Server CA issues only certificates to domain names recognized in the official database AFRINIC or INTERNIC (see section 4.2.1 of Server CP).
- 10) OCSP Responses signed by a certificate under a different root: No
- 11) SHA-1 Certificates: The CA issue only sha256 certificates (see sections 7.1.1 for AC certificate profile and section 7.1.2 for end-user Certificate Profile).
- 12) Generic names for CAs: No
- 13) Lack of Communication With End Users:  
<http://www.certification.tn/en/content/technical-support>
- 14) 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.

**Verified?**

Verified

**Root Case Record # 1**

**Root Case Information**

<b>Root Certificate Name</b>	Tunisian Root Certificate Authority - TunRootCA2	<b>Root Case No</b>	R00000106
<b>Request Status</b>	Ready for Public Discussion	<b>Case Number</b>	00000076

**Certificate Data**

<b>Certificate Issuer Common Name</b>	Tunisian Root Certificate Authority - TunRootCA2
<b>O From Issuer Field</b>	National Digital Certification Agency
<b>OU From Issuer Field</b>	
<b>Valid From</b>	2015 May 05
<b>Valid To</b>	2027 May 05
<b>Certificate Serial Number</b>	2166150505270505bc8ab01daf0abec4
<b>Subject</b>	CN=Tunisian Root Certificate Authority - TunRootCA2, OU=null, O=National Digital Certification Agency, C=TN
<b>Signature Hash Algorithm</b>	sha256WithRSAEncryption
<b>Public Key Algorithm</b>	RSA 4096 bits
<b>SHA-1 Fingerprint</b>	96:38:63:3C:90:56:AE:88:14:A0:65:D2:3B:DC:60:A0:EE:70:2F:A7
<b>SHA-256 Fingerprint</b>	C7:95:FF:8F:F2:0C:96:66:88:F0:64:A1:E0:91:42:1D:31:10:A3:45:6C:17:EC:24:04:B9:98:73:87:41:F6:22
<b>Certificate Fingerprint</b>	0F:31:0D:C7:29:9B:D0:C9:BB:62:F1:52:81:C3:BF:AB:10:AC:69:04:1D:C0:FE:49:4A:2F:83:D5:25:30:2A:FC
<b>Certificate Version</b>	3

**Technical Information about Root Certificate**

<b>Certificate Summary</b>	This root has internally-operated subordinate CAs.	<b>Verified?</b>	Verified
<b>Root Certificate Download URL</b>	<a href="http://www.certification.tn/pub/TunRootCA2.crt">http://www.certification.tn/pub/TunRootCA2.crt</a>	<b>Verified?</b>	Verified
<b>CRL URL(s)</b>	<a href="http://crl.certification.tn/TunRootCA2.crl">http://crl.certification.tn/TunRootCA2.crl</a> Server CP section 2.3: A new CRL is published every 24 hours	<b>Verified?</b>	Verified
<b>OCSP URL(s)</b>	<a href="http://ocsp.certification.tn">http://ocsp.certification.tn</a> OCSP responses have a maximum expiration time of 10 days.	<b>Verified?</b>	Verified
<b>Trust Bits</b>	Websites	<b>Verified?</b>	Verified
<b>SSL Validation Type</b>	OV	<b>Verified?</b>	Verified
<b>EV Policy OID(s)</b>	Not EV	<b>Verified?</b>	Not Applicable
<b>Root Stores Included In</b>	Microsoft	<b>Verified?</b>	Verified
<b>Mozilla Applied Constraints</b>	None	<b>Verified?</b>	Verified

**Test Websites or Example Cert**

<b>Test Website - Valid</b>	<a href="https://valid-ov.certification.tn">https://valid-ov.certification.tn</a>	<b>Verified?</b>	Verified
<b>Test Website - Expired</b>	<a href="https://expired-ov.certification.tn">https://expired-ov.certification.tn</a>		
<b>Test Website - Revoked</b>	<a href="https://revoked-ov.certification.tn">https://revoked-ov.certification.tn</a>		
<b>Example Cert</b>	<a href="https://webmail.ance.tn">https://webmail.ance.tn</a>		
<b>Test Notes</b>			

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

<b>Revocation Tested</b>	<a href="https://certificate.revocationcheck.com/webmail.ance.tn">https://certificate.revocationcheck.com/webmail.ance.tn</a> no errors.	<b>Verified?</b>	Verified
<b>CA/Browser Forum Lint Test</b>	Tested. No errors.	<b>Verified?</b>	Verified
<b>Test Website Lint Test</b>	Tested. No errors.	<b>Verified?</b>	Verified
<b>EV Tested</b>	Not requesting EV treatment	<b>Verified?</b>	Not Applicable

## CA Hierarchy Information

<b>CA Hierarchy</b>	This root will have internally-operated subordinate CAs. Currently it has one internally-operated subordinate CA: - Tunisian Server Certificate Authority - TunServerCA2	<b>Verified?</b>	Verified
<b>Externally Operated SubCAs</b>	No Externally Operated SubCAs.	<b>Verified?</b>	Verified
<b>Cross Signing</b>	No Cross-Signing.	<b>Verified?</b>	Verified
<b>Technical Constraint on 3rd party Issuer</b>	No external Registration Authorities.	<b>Verified?</b>	Verified

## Verification Policies and Practices

<b>Policy Documentation</b>	Root CP: <a href="http://www.certification.tn/sites/default/files/documents/politiqueRACINE-NG-01.pdf">http://www.certification.tn/sites/default/files/documents/politiqueRACINE-NG-01.pdf</a>  Server (TLS/SSL) CP: <a href="http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf">http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf</a>  CP/CPS in English : <a href="http://www.certification.tn/sites/default/files/documents/CPCPS-PTC-BR-EN-05.pdf">http://www.certification.tn/sites/default/files/documents/CPCPS-PTC-BR-EN-05.pdf</a>	<b>Verified?</b>	Verified
<b>CA Document Repository</b>	<a href="http://www.certification.tn/en/content/downloads">http://www.certification.tn/en/content/downloads</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	French		
<b>CP</b>	<a href="http://www.certification.tn/sites/default/files/documents/PolitiqueSERVEURS-PTC-BR-05.pdf">http://www.certification.tn/sites/default/files/documents/PolitiqueSERVEURS-PTC-BR-05.pdf</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	French		
<b>CPS</b>	<a href="http://www.certification.tn/sites/default/files/documents/PolitiqueSERVEURS-PTC-BR-05.pdf">http://www.certification.tn/sites/default/files/documents/PolitiqueSERVEURS-PTC-BR-05.pdf</a>	<b>Verified?</b>	Verified
<b>Other Relevant Documents</b>	Certificate Subscriber Agreement or Terms of Use: <a href="http://www.certification.tn/sites/default/files/documents/CGUSSL.pdf">http://www.certification.tn/sites/default/files/documents/CGUSSL.pdf</a>  National Digital Certification Agency (NDCA) operates under Tunisia's Electronic Signature Law 83-2000: <a href="http://www.certification.tn/sites/default/files/documents/loi_2000-83_fr.pdf">http://www.certification.tn/sites/default/files/documents/loi_2000-83_fr.pdf</a>	<b>Verified?</b>	Verified
<b>Auditor Name</b>	LSTI	<b>Verified?</b>	Verified
<b>Auditor Website</b>	<a href="http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf">http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf</a>	<b>Verified?</b>	Verified
<b>Auditor Qualifications</b>	<a href="https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx">https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx</a>	<b>Verified?</b>	Verified
<b>Standard Audit</b>	<a href="https://bugzilla.mozilla.org/attachment.cgi?id=8879910">https://bugzilla.mozilla.org/attachment.cgi?id=8879910</a>	<b>Verified?</b>	Verified

<b>Standard Audit Type</b>	ETSI TS 102 042	<b>Verified?</b>	Verified
<b>Standard Audit Statement Date</b>	9/30/2016	<b>Verified?</b>	Verified
<b>BR Audit</b>	<a href="https://bugzilla.mozilla.org/attachment.cgi?id=8879910">https://bugzilla.mozilla.org/attachment.cgi?id=8879910</a>	<b>Verified?</b>	Verified
<b>BR Audit Type</b>	ETSI TS 102 042	<b>Verified?</b>	Verified
<b>BR Audit Statement Date</b>	9/30/2016	<b>Verified?</b>	Verified
<b>EV Audit</b>	Not EV	<b>Verified?</b>	Not Applicable
<b>EV Audit Type</b>		<b>Verified?</b>	Not Applicable
<b>EV Audit Statement Date</b>		<b>Verified?</b>	Not Applicable
<b>BR Commitment to Comply</b>	Server CP section 1.1	<b>Verified?</b>	Verified
<b>BR Self Assessment</b>	<a href="https://bugzilla.mozilla.org/attachment.cgi?id=8865381">https://bugzilla.mozilla.org/attachment.cgi?id=8865381</a>	<b>Verified?</b>	Verified
<b>SSL Verification Procedures</b>	<p>Server CP Section 4.2.1: For the purpose of verification of applicants' identities, the registration authority (RA) does the following operations :</p> <ul style="list-style-type: none"> <li>-check the accuracy of the registration file and all the credentials needed for submission,</li> <li>-check the accuracy of the purchase order and payment,</li> <li>-check that the organization owns the domain name by consulting the official databases of domain names such as AFRINIC or INTERNIC .</li> <li>-ensure that the subscriber has agreed to the terms specified in the Certificate Subscriber Agreement or Terms of Use.</li> </ul> <p>Once these steps are accomplished, the RA transfers the request to the other components of the Certification Authority that are responsible of the issuance of the certificates.</p>	<b>Verified?</b>	Verified
<b>EV SSL Verification Procedures</b>	Not EV	<b>Verified?</b>	Not Applicable
<b>Organization Verification Procedures</b>	<p>Server CP Section 3.2.2: The authentication of a client's organization is done through the verification of the following documents:</p> <ul style="list-style-type: none"> <li>• The certificate application form, which contains the information needed to submit a certificate request such as the email address and the business phone number that will be used by the CA to contact the subscriber. The form must be duly completed and signed by the applicant</li> <li>• A copy of the National Identity Card, passport or residence permit of the applicant and the legal representative of the organization;</li> <li>• An extract from the trade register not exceeding three months;</li> </ul> <p>The registration authority notifies the subscriber that all the informations indicated in the registration file will be retained. The operations of verification and validation of the request are executed in accordance with section § 4.2.</p> <p>Section 4.1.1 : A certificate can be requested by the legal representative of the organization to which the server is deployed.</p>	<b>Verified?</b>	Verified
<b>Email Address Verification Procedures</b>	Not requesting the Email trust bit at this time.	<b>Verified?</b>	Not Applicable
<b>Code Signing Subscriber Verification Pro</b>	Mozilla is no longer accepting requests to enable the Code Signing trust bit, because we plan to remove the Code Signing trust bit in the next version of Mozilla's CA Certificate Policy.	<b>Verified?</b>	Not Applicable
<b>Multi-Factor Authentication</b>	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.	<b>Verified?</b>	Verified
<b>Network Security</b>	Confirmed. CP section 6.5-6.7	<b>Verified?</b>	Verified