Print this page

Mozilla - CA Program

Case Information

Case Number	00000076	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Government of Tunisia	**Request Status**	Initial Request Received

Additional Case Information

Subject	Include Government of Tunisia Root	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1233645

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)		**Verified?**	Not Applicable
Geographic Focus	Tunisia	**Verified?**	Verified
Primary Market / Customer Base	This is the Tunisian national certification authority.	**Verified?**	Verified
Impact to Mozilla Users	National Digital Certification Agency (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.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	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.

CA's Response to Recommended Practices	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices 1) Publicly Available CP and CPS: Yes 2) CA Hierarchy: Yes 3) Audit Criteria: Yes 4) Document Handling of IDNs in CP/CPS: ??? 5) Revocation of Compromised Certificates: Server CPS section 4.9 6) Verifying Domain Name Ownership: Yes 7) Verifying Email Address Control: ??? 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. 9) DNS names go in SAN: ??? 10) Domain owned by a Natural Person: ??? 11) OCSP: ??? 12) Network Security Controls: ???	**Verified?**	Need Response From CA

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic 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	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices 1) Long-lived DV certificates: ??? 2) Wildcard DV SSL certificates: ??? 3) Email Address Prefixes for DV Certs: ??? 4) 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: ??? 8) Certificates referencing hostnames or private IP addresses: ??? 9) Issuing SSL Certificates for Internal Domains: ??? 10) OCSP Responses signed by a certificate under a different root: No 11) SHA-1 Certificates: ??? 12) Generic names for CAs: No 13) Lack of Communication With End Users: ??? 14) Backdating the notBefore date: ???	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	Tunisian Root Certificate Authority - TunRootCA2	**Root Case No**	R00000106
Request Status	Initial Request Received	**Case Number**	00000076

Additional Root Case Information

Subject	Include Tunisian Root Certificate Authority - TunRootCA2

Technical Information about Root Certificate

O From Issuer Field	National Digital Certification Agency	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This root has internally-operated subordinate CAs that sign certificates for TLS/SSL, S/MIME, and code signing.	**Verified?**	Verified
Root Certificate Download URL	http://www.certification.tn /pub/TunRootCA2.crt	**Verified?**	Verified
Valid From	2015 May 05	**Verified?**	Verified
Valid To	2027 May 05	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://webmail.ance.tn	**Verified?**	Verified
CRL URL(s)	http://crl.certification.tn/TunRootCA2.crl Server CP section 2.3: A new CRL is published every 24 hours	**Verified?**	Verified
OCSP URL(s)	http://ocsp.certification.tn	**Verified?**	Verified
Revocation Tested	NEED: Fix all errors listed here: https://certificate.revocationcheck.com /webmail.ance.tn	**Verified?**	Need Response From CA
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested	Not requesting EV treatment	**Verified?**	Not Applicable
Root Stores Included In		**Verified?**	Need Response From CA
Mozilla Applied Constraints	NEED: Please confirm that, if included, Mozilla may constrain this CA hierarchy to *.tn. Reference: Server CP section 1.1: ...only to servers for government agencies under the domain ".tn ".	**Verified?**	Need Response From CA

Digital Fingerprint Information

SHA-1 Fingerprint	96:38:63:3C:90:56:AE:88:14:A0:65:D2:3B:DC:60:A0:EE:70:2F:A7	**Verified?**	Verified
SHA-256 Fingerprint	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	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root will have internally-operated subordinate CAs: - Tunisian Personal Certificate Authority - TunServerCA2	**Verified?**	Verified

	- Tunisian Server Certificate Authority - TunServerCA2 - Tunisian Code Certificate Authority - TunServerCA2 - Tunisian Device Certificate Authority - TunServerCA2		
Externally Operated SubCAs	No Externally Operated SubCAs.	**Verified?**	Verified
Cross Signing	No Cross-Signing.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	NEED: Can external Registration Authorities directly cause the issuance of TLS/SSL certificates? If yes, what rules, constraints, auditing applies to them?	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	All the documents are in French. Root CP: http://www.certification.tn/sites/default/files/documents/politiqueRACINE-NG-01.pdf Server (TLS/SSL) CP: http://www.certification.tn/sites/default/files/documents/politiqueSERVEURS-PTC-BR-02.pdf Personal CP: http://www.certification.tn/sites/default/files/documents/politiquePERSONNES.pdf	**Verified?**	Verified
CA Document Repository	http://www.certification.tn/en/content/downloads	**Verified?**	Verified
CP Doc Language	French		
CP	http://www.certification.tn/en/content/certificate-policy	**Verified?**	Verified
CP Doc Language	French		
CPS	http://www.certification.tn/en/content/certificate-policy	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	LSTI	**Verified?**	Verified
Auditor Website	http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf	**Verified?**	Verified
Auditor Qualifications	https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	**Verified?**	Verified
Standard Audit	http://www.certification.tn/11140VA1_ANCE_AF_S.pdf	**Verified?**	Not Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	11/30/2015	**Verified?**	Verified
BR Audit	http://www.certification.tn/11140VA1_ANCE_AF_S.pdf	**Verified?**	Not Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	11/30/2015	**Verified?**	Verified
EV Audit	Not EV	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable

BR Commitment to Comply	Server CP section 1.1	**Verified?**	Verified
SSL Verification Procedures	NEED Correct translation: Section 4.2.1: For the purpose of verification of identity of applicants, EI, does the following: - check the consistency of the registration dossier and supporting documents submitted; - verify the accuracy of the purchase order and payment; - ensure that the organization owns the domain name by consulting the official database AFRINIC INTERNIC or type domain names. - ensure that the RCS has noted the detailed rules applicable to the use of the certificate. Once these steps, EI forwards the request to the components of the CA certificate loaded in production.	**Verified?**	Need Response From CA
EV SSL Verification Procedures	Not EV	**Verified?**	Not Applicable
Organization Verification Procedures	NEED Correct translation: Server CPS Section 3.2.2: The authentication of a client organization is through the verification of the following: - The certificate application form duly completed and signed by the applicant, making certificate request Office, containing including mailing address, email address and business telephone number to contact ANCE the future wearer; - A copy of the National Identity Card, passport or residence permit of the applicant and the RCS; - An extract from the trade register not exceeding three months; - The carrier must be informed that the personal information of identity he has indicated to the registration dossier will be retained. - The operations of verification and validation of the application are executed in accordance with the provisions described in section 4.2. Section 4.1.1: A certificate can be requested by a legal representative of the organization to which the server is implemented.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS (translated into English) that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	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.	**Verified?**	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.	**Verified?**	Verified
Network Security	Confirmed. CPS section 6.5-6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.certification.tn/en/content/root-certificates	**Verified?**	Verified