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, Agence National de Certification Electronique / National Digital Certification Agency (ANCE/NDCA)	**Request Status**	Ready for Public Discussion

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

Required and 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	1) Publicly Available CP and CPS: Yes 2) CA Hierarchy: Yes	**Verified?**	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	**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

Root Certificate Name	Tunisian Root Certificate Authority - TunRootCA2	**Root Case No**	R00000106
Request Status	Ready for Public Discussion	**Case Number**	00000076

Certificate Data

Certificate Issuer Common Name	Tunisian Root Certificate Authority - TunRootCA2
O From Issuer Field	National Digital Certification Agency
OU From Issuer Field	
Valid From	2015 May 05
Valid To	2027 May 05
Certificate Serial Number	2166150505270505bc8ab01daf0abec4
Subject	CN=Tunisian Root Certificate Authority - TunRootCA2, OU=null, O=National Digital Certification Agency, C=TN
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	96:38:63:3C:90:56:AE:88:14:A0:65:D2:3B:DC:60:A0:EE:70:2F:A7
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
Certificate Fingerprint	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
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This root has internally-operated subordinate CAs.	**Verified?**	Verified
Root Certificate Download URL	http://www.certification.tn/pub/TunRootCA2.crt	**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 OCSP responses have a maximum expiration time of 10 days.	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://webmail.ance.tn	**Verified?**	Verified
Test Website - Expired			
Test Website - Revoked			
Example Cert			
Test Notes			

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

Revocation Tested	https://certificate.revocationcheck.com/webmail.ance.tn no errors.	**Verified?**	Verified
CA/Browser Forum Lint Test	Tested. No errors.	**Verified?**	Verified
Test Website Lint Test	Tested. No errors.	**Verified?**	Verified
EV Tested	Not requesting EV treatment	**Verified?**	Not Applicable

CA Hierarchy Information

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

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	**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	Certificate Subscriber Agreement or Terms of Use: http://www.certification.tn/sites/default/files/documents/CGUSSL.pdf 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	**Verified?**	Verified
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?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit	11/30/2015	**Verified?**	Verified

Statement Date			
BR Audit	http://www.certification.tn/11140VA1_ANCE_AF_S.pdf	**Verified?**	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
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8865381	**Verified?**	Verified
SSL Verification Procedures	Server CP Section 4.2.1: For the purpose of verification of applicants' identities, the registration authority (RA) does the following operations : -check the accuracy of the registration file and all the credentials needed for submission, -check the accuracy of the purchase order and payment, -check that the organization owns the domain name by consulting the official databases of domain names such as AFRINIC or INTERNIC . -ensure that the subscriber has agreed to the terms specified in the Certificate Subscriber Agreement or Terms of Use. 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.	**Verified?**	Verified
EV SSL Verification Procedures	Not EV	**Verified?**	Not Applicable
Organization Verification Procedures	Server CP Section 3.2.2: The authentication of a client's organization is done through the verification of the following documents: • 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 • A copy of the National Identity Card, passport or residence permit of the applicant and the legal representative of the organization; • An extract from the trade register not exceeding three months; 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. Section 4.1.1 : A certificate can be requested by the legal representative of the organization to which the server is deployed.	**Verified?**	Verified
Email Address Verification Procedures	Not requesting the Email trust bit at this time.	**Verified?**	Not Applicable
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. CP section 6.5-6.7	**Verified?**	Verified