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: **Use of IDNs isn't allowed. The CA does not allows the use of a domaine name containing non-ASCII character in certificates.** 5) Revocation of Compromised Certificates: Server CPS section 4.9 6) Verifying Domain Name Ownership: Yes 7) Verifying Email Address Control: **Not applicable (Trust bit email is not requested for this CA).** 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. 9) DNS names go in SAN: **The end user certificate contains only the Subject Alternative Name Extension.** **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 (Certificate Subscriber Agreement or Terms of Use).** 11) OCSP: **The OCSP responder is set up to listen on the 80 port. The OCSP URI is provided in the certificate (extension : Authority Information Access). The OCSP service for end-entity certificates is updated every four days and OCSP responses have a maximum expiration time of ten days. We have already test the OCSP service in Firefox. The OCSP responders functions without any error.** 12) Network SecurityControl: **The CA maintains network security controls (intrusion detection system, audit review, monitoring, user account management, access control, …) as described in sections 6.5 and 6.7 of Server CA CP/CPS. The CA has already implemented an information systems security policy.**	**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: **Not Applicable. The CA does not issue long-lived SSL certificates.** 2) Wildcard DV SSL certificates: **OV Certificates include a wildcard**	**Verified?**	Need Response From CA

asterisk character. Before issuing a Wildcard certificate, 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 CP/CPS).

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: **Not Applicable. 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 CA).**
10) OCSP Responses signed by a certificate under a different root: No
11) SHA-1 Certificates: **Not Applicable. 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.**

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	Nationale 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 **See the attached document (mozilla_check_error.pdf)**	**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	**Microsoft stores.**	**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

	No, this CA does not focus its activities only on Tunisia. The section 1.1 will nolonger be in effect since the Server CP will be updated.		

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
SHA256 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 Hirarchy	This root will have internally-operated subordinate CAs: ~~- Tunisian Personal Certificate Authority - TunServerCA2~~ - Tunisian Server Certificate Authority - TunServerCA2 ~~- Tunisian Code Certificate Authority - TunServerCA2~~ ~~- Tunisian Device Certificate Authority - TunServerCA2~~	**Verified ?**	Verified

Externally Operated SubCAs	No Externally Operated SubCAs	**Verified ?**	Verified
Cross Signing	No Cross-Signing.	**Verified ?**	Verified
Technical Contraint 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? **Not Applicable. No external Registration Authorities.**	**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 (corresponding to an other CA)**~~	**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

CPS 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. **The correct translation is below :** **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,**	**Verified ?**	Need Response From CA

	-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.**		
EV SSL Verification Procedures	Not EV	**Verified ?**	Not Applicable
Organization Verification Procedures	NEED Correct translation: Verified? Need Response From CA 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. **The correct translation is below :** **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 ?**	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 **For the time being, the Email trust bit is not requested.** **The Server CA issue only SSL certificates.**	**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