

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


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	<p>NEED: The wiki page and your CP/CPS have changed, so please verify the answers below. https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices</p> <p>* 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,</p>	<p>* Long-lived Certificates: ???</p> <p>Note the recent changes in BRs limiting max validity of SSL certs to 825 days.</p> <p>→ The TnTrust Corp CA and TnTrust Gov CA issue certificates with a validity of a 1 year or 2 years only (see section 6.3.2).</p> <p>* Non-Standard Email Address Prefixes for Domain Ownership Validation: ???</p> <p>→ The RA controls the applicant over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at- sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response containing the Random Value.</p> <p>* Issuing End Entity Certificates Directly From Roots: No. CP/CPS section 1.1</p> <p>→ The root and intermediate CAs issue authority certificates, OCSP certificates and CRLs.</p> <p>* Distributing Generated Private Keys in PKCS#12 Files: No. CP/CPS section 3.2.1.1</p> <p>→ TN PKI does not issue PKCS#12 files. The private key is under the control of the applicant. The section 3.2.1.1 of the CP/CPS “The subscriber provides a digitally signed PKCS#10 CSR to establish that it holds the private key corresponding to the public key to be included in a certificate. TN PKI RA parses the PKCS#10 CSR submitted by the subscriber and</p>	

	<p>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: ???</p>	<p>verifies that the subscriber’s digital signature on the PKCS#10 was created by the private key corresponding to the public key in the PKCS#10 CSR.”</p> <p>* Certificates Referencing Local Names or Private IP Addresses: ??? → No, the TN PKI CAs issue only SSL certificates which refer to domain names that are resolvable using the public DNS infrastructure.</p> <p>* Issuing SSL Certificates for .int Domains: ??? → No, the TN PKI CAs do not issue certificates for internal names.</p> <p>* OSCP Responses Signed by a Certificate Under a Different Root: No → No.</p> <p>* Issuance of SHA-1 Certificates: No. CP/CPS section 7.1.3 → Not Applicable. The TN PKI CAs issue only sha256 certificates (see sections 6.1.5 and 7.1.3 of the CP/CPS)</p> <p>* Delegation of Domain / Email Validation to Third Parties: Yes. It appears that there are Delegated Registration Authorities - CP/CPS section 1.3.3. → Yes the TN PKI RA might have delegated registration parties but until now the TN PKI does not have a contractual agreement with any of those (see section 1.3.3 of the CP/CPS).</p> <p>* Allowing External Entities to Operate Subordinate CAs: No. It appears that externally-operated subCAs are not allowed - CP/CPS section 1.3.1.2. → Yes. Externally operated SubCAs are not allowed.</p> <p>* Generic Names for CAs: No. CP/CPS section 1.1 → No, there are no generic names for CAs.</p> <p>* Lack of Communication With End Users: No. http://www.certification.tn/en/content/technical-support, support@certification.tn → http://www.certification.tn/en/content/technical-support</p> <p>* 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. → The notBefore date is the date of issuing the certificate by the CA. The timestamp contains the time of issuing the certificate by the CA.</p> <p>* Issuer Encoding in CRL: ??? → Each CRL contains the Issuer DN and the Authority Key Identifier of the issuer.</p>
--	---	--

Root Case Record #1		
Root Case Information		
Root Certificate Name	Tunisia National Root CA	
Request Status	Initial Request Received	
Certificate Data		
Certificate Issuer Commun 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 Nov 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	
SHA1 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	The main purpose of the Tunisian National Root Certificate Authority is to issue the Subordinate Certification Authorities of the NDCA.	
Root Certificate Download URL	http://www.certification.tn/pub/TunisianNationalRootCA.crt	
CRL URL(s)	http://crl.certification.tn/tunrootca.crl	
OCSP URL(s)	http://va.certification.tn	
Mozilla Trust Bits	Email; website	
SSL Validation Type	OV, EV	
Mozilla EV Policy OID(s)	2.16.788.1.2.6.1.10	
Root Stores Included in		
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?	No, the TN PKI CAs does not focus its activities only on Tunisia.

Test Websites or Example Cert		
Test Website - valid	https://valid-corp-ov.certification.tn	This problem has been resolved. The reason of this slowness was that during the last two weeks, we migrated to our new backup site.
Test website Expired	https://expired-corp-ov.certification.tn	
Test website - revoked	https://revoked-corp-ov.certification.tn	
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	When I check the valid-corp-ev.certification.tn under the https://certificate.revocationcheck.com , I found these errors: <ol style="list-style-type: none"> OCSP: Unexpected HTTP response: 400 Bad Request. When we check over openssl command line, every thing is Okay. In our OCSP server I get this message error: Error processing OCSP request. Message; Request is missing last part of URL defined in RFC 2560 A.1.1. http://crl.certification.tn/tunrootca.crl: ThisUpdate is more than seven days old, CRLs must be updated and reissued at least every seven days (Mozilla Maintenance Policy section 3): this is the Root CA CRL for the status of Subordinate CA Certificates: The Root CA updates and reissue CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate (see section 4.9.7 of the CP/CPS and section 4.9.7 of the CAB/Forum Base Requirements).
CA/Browser Forum Lint Test	NEED: BR Lint Test: https://github.com/awslabs/certlint It would really help if at least the test certs are logged to a CT log. I can't even find the root cert in crt.sh to run the tests.	I applied the test certs in the certlint and I received this message: <pre>cablint INFO EV certificate identified cablint INFO TLS Server certificate identified x509lint INFO Subject has a deprecated CommonName zlint NOTICE Subscriber Certificate:</pre>

		<p>commonName is deprecated.</p>  <pre> cablint INFO EV certificate identified cablint INFO TLS Server certificate identified x509lint INFO Subject has a deprecated CommonName zlint NOTICE Subscriber Certificate: commonName is deprecated. </pre> <p>We don't know how to insert the root cert in crt.sh. Could you explain how and we will do so.</p>
Test Website Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the X.509 rules. X.509 Lint Test: https://github.com/kroeckx/x509lint	The issued certificates do not violate any of the X.509 rules. There are only Info and Notice messages after applying the x509lint.
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 I tried to run this test with the valid test website above, but it seems to time out.	<p>When I tried the https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version, I have this message: Error: TypeError: Cannot read property 'success' of undefined</p> <p>EV-Readiness Check</p> <p>Error: TypeError: Cannot read property 'success' of undefined</p> <p>TLS Server <input type="text" value="valid-corp-ev.certification.tn"/></p> <p>EV Policy OID <input type="text" value="2.16.788.1.2.6.1.9.2.2"/></p> <p>Root Certificate PEM</p>