Print this page

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**	Initial Request Received

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

General information about CA's associated organization

CA Email Alias 1	olfa.kaddachi@certification.tn		
CA Email Alias 2	ramzi.khlif@certification.tn		
Company Website	http://www.certification.tn	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)	None	**Verified?**	Verified
Geographic Focus	NEED: Country or geographic region where CA typically sells certs.	**Verified?**	Verified
Primary Market / Customer Base	Are there particular vertical market segments in which it operates? No Does the CA focus its activities on a particular country or other geographic region? No	**Verified?**	Verified
Impact to Mozilla Users	The NDCA is the tunisian national certification authority. 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/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and 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: CAs response to each of the items listed in https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Verified?**	Need Response From CA

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	NEED: CA's response to each of the items listed in https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	Tunisia National Root CA	**Root Case No**	R00000315
Request Status	Initial Request Received	**Case Number**	00000174

Certificate Data

Certificate Issuer Common 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 May 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
SHA-1 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.	**Verified?**	Verified
Root Certificate Download URL	www.certification.tn/pub/TunisianNationalRootCA.crt	**Verified?**	Verified
CRL URL(s)	http://crl.certification.tn/tunrootca.crl	**Verified?**	Verified
OCSP URL(s)	va.certification.tn	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	2.16.788.1.2.6.1.10	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Need Clarification From CA
Mozilla Applied Constraints	No constraints.	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid		**Verified?**	Need Response From CA
Test Website - Expired			
Test Website - Revoked			
Example Cert			
Test Notes	NEED: - If requesting Websites trust bit provide 3 URLs to 3 test websites (valid, expired, revoked) whose TLS/SSL cert chains up to this root. - If only requesting the Email trust bit, then attach an example S/MIME cert to the bug.		

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

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs). BR Lint Test: https://github.com/awslabs/certlint	**Verified?**	Need Response From CA
Test Website Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the X.509 rules.	**Verified?**	Need Response From CA

	X.509 Lint Test: https://github.com/kroeckx/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	**Verified?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist, https://wiki.mozilla.org/CA/Subordinate_CA_Checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those subordinate CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of the CA/Browser Forum's Baseline Requirements - Mozilla's Root Store Policy	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Need Response From CA
CP Doc Language			
CP		**Verified?**	Need Response From CA
CP Doc Language			

CPS		**Verified?**	Need Response From CA
Other Relevant Documents		**Verified?**	Need Response From CA
Auditor Name		**Verified?**	Need Response From CA
Auditor Website		**Verified?**	Need Response From CA
Auditor Qualifications		**Verified?**	Need Response From CA
Standard Audit	NEED: Audit statements meeting the requirements of Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
EV SSL Audit Type		**Verified?**	Need Response From CA
EV SSL Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED: If requesting Websites trust bit, need section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_Self-Assessment) to the Bugzilla Bug.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. CP/CPS must clearly specify the procedures that the CA employs. Each documented procedure should state which subsection of BR section 3.2.2.4 it is complying with.	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED: If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate.	**Verified?**	Need Response From CA

	The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.		
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert.	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED section number of the CP/CPS that states that multi-factor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)	**Verified?**	Need Response From CA
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	**Verified?**	Need Response From CA

Root Case Record # 2

Root Case Information

Root Certificate Name	Tunisia Gov CA	**Root Case No**	R00000316
Request Status	Initial Request Received	**Case Number**	00000174

Certificate Data

Certificate Issuer Common Name	Tunisia National Root CA
O From Issuer Field	National Digital Certification Agency
OU From Issuer Field	
Valid From	2016 Nov 29
Valid To	2032 Feb 29
Certificate Serial Number	782c1009830a4bee
Subject	CN=Tunisia Gov CA, OU=null, O=National Digital Certification Agency, C=TN
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits

SHA-1 Fingerprint	9F:81:BE:87:33:2A:67:FC:93:71:1E:5B:FD:FF:6E:3B:7F:46:31:A4
SHA-256 Fingerprint	37:93:68:F7:8E:99:37:A8:B0:BB:72:3E:99:99:50:86:12:75:12:0D:67:75:32:4E:37:A7:0C:F1:69:76:0A:64
Certificate Fingerprint	EB:9F:AC:B7:DD:89:B2:62:1E:D1:31:99:80:31:A6:8F:A4:5E:DA:CF:CE:F2:85:B4:5F:45:52:57:57:13:FC:FE
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	The main purpose of the Tunisia Gov CA is signing issuing CA (level 3) for governmental organisms.	**Verified?**	Need Response From CA
Root Certificate Download URL	http://crl.certification.tn/tunrootca.crl	**Verified?**	Need Response From CA
CRL URL(s)	http://crl.certification.tn/tunisiagovca.crl	**Verified?**	Need Response From CA
OCSP URL(s)	va.certification.tn	**Verified?**	Need Response From CA
Mozilla Trust Bits	Email; Websites	**Verified?**	Need Response From CA
SSL Validation Type	OV; EV	**Verified?**	Need Response From CA
Mozilla EV Policy OID(s)		**Verified?**	Need Response From CA
Root Stores Included In		**Verified?**	Need Response From CA
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid		**Verified?**	Need Response From CA
Test Website - Expired			
Test Website - Revoked			
Example Cert			
Test Notes	NEED: - If requesting Websites trust bit provide 3 URLs to 3 test websites (valid, expired, revoked) whose TLS/SSL cert chains up to this root. - If only requesting the Email trust bit, then attach an example S/MIME cert to the bug.		

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

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum	**Verified?**	Need Response From CA

	Baseline Requirements (BRs). BR Lint Test: https://github.com/awslabs/certlint		
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	**Verified?**	Need Response From CA
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	**Verified?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist, https://wiki.mozilla.org/CA/Subordinate_CA_Checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those subordinate CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of the CA/Browser Forum's Baseline Requirements - Mozilla's Root Store Policy	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Need Response From CA

CP Doc Language			
CP		**Verified?**	Need Response From CA
CP Doc Language			
CPS		**Verified?**	Need Response From CA
Other Relevant Documents		**Verified?**	Need Response From CA
Auditor Name		**Verified?**	Need Response From CA
Auditor Website		**Verified?**	Need Response From CA
Auditor Qualifications		**Verified?**	Need Response From CA
Standard Audit	NEED: Audit statements meeting the requirements of Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
EV SSL Audit Type		**Verified?**	Need Response From CA
EV SSL Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED: If requesting Websites trust bit, need section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_Self-Assessment) to the Bugzilla Bug.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. CP/CPS must clearly specify the procedures that the CA employs. Each documented procedure should state which subsection of BR section 3.2.2.4 it is complying with.	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED: If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain	**Verified?**	Need Response From CA

	name, and the verification of identity, existence, and authority of the organization to request the EV certificate. The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.		
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert.	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED section number of the CP/CPS that states that multi-factor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)	**Verified?**	Need Response From CA
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	**Verified?**	Need Response From CA

Root Case Record # 3

Root Case Information

Root Certificate Name	Tunisia Corporate CA	**Root Case No**	R00000317
Request Status	Initial Request Received	**Case Number**	00000174

Certificate Data

Certificate Issuer Common Name	Tunisia National Root CA
O From Issuer Field	National Digital Certification Agency
OU From Issuer Field	
Valid From	2016 Nov 29
Valid To	2032 Feb 29
Certificate Serial Number	35d821ddca93b331
Subject	CN=Tunisia Corporate CA, OU=null, O=National Digital Certification Agency, C=TN
Signature Hash	sha256WithRSAEncryption

Algorithm	
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	EC:3C:48:68:3A:65:A9:A1:B3:64:2C:F3:D1:B1:1A:17:BC:52:D5:D6
SHA-256 Fingerprint	BB:79:2E:A9:FD:06:48:56:97:0A:F9:A7:25:8A:EE:A6:0D:7E:3A:22:44:7D:EE:EB:6A:EB:F3:E9:14:F2:FD:1A
Certificate Fingerprint	6D:87:8A:B5:7B:85:B4:67:D3:B8:88:4C:75:11:36:A8:65:00:E3:9A:47:EF:EC:CD:A6:7A:52:2F:BC:5A:6A:85
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	NEED: CA's input	**Verified?**	Need Response From CA
Root Certificate Download URL	http://crl.certification.tn/tunrootca.crl	**Verified?**	Need Response From CA
CRL URL(s)	http://crl.certification.tn/tunisiacorpca.crl	**Verified?**	Need Response From CA
OCSP URL(s)	va.certification.tn	**Verified?**	Need Response From CA
Mozilla Trust Bits	Email; Websites	**Verified?**	Need Response From CA
SSL Validation Type		**Verified?**	Need Response From CA
Mozilla EV Policy OID(s)		**Verified?**	Need Response From CA
Root Stores Included In		**Verified?**	Need Response From CA
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid		**Verified?**	Need Response From CA
Test Website - Expired			
Test Website - Revoked			
Example Cert			
Test Notes	NEED: - If requesting Websites trust bit provide 3 URLs to 3 test websites (valid, expired, revoked) whose TLS/SSL cert chains up to this root. - If only requesting the Email trust bit, then attach an example S/MIME cert to the bug.		

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

Revocation	NEED: Test with http://certificate.revocationcheck.com/	**Verified?**	Need Response From CA

Tested	make sure there aren't any errors.		
CA/Browser Forum Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs). BR Lint Test: https://github.com/awslabs/certlint	**Verified?**	Need Response From CA
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	**Verified?**	Need Response From CA
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	**Verified?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist, https://wiki.mozilla.org/CA/Subordinate_CA_Checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those subordinate CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of the CA/Browser Forum's Baseline Requirements - Mozilla's Root Store Policy	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA

CA Document Repository		**Verified?**	Need Response From CA
CP Doc Language			
CP		**Verified?**	Need Response From CA
CP Doc Language			
CPS		**Verified?**	Need Response From CA
Other Relevant Documents		**Verified?**	Need Response From CA
Auditor Name		**Verified?**	Need Response From CA
Auditor Website		**Verified?**	Need Response From CA
Auditor Qualifications		**Verified?**	Need Response From CA
Standard Audit	NEED: Audit statements meeting the requirements of Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
EV SSL Audit Type		**Verified?**	Need Response From CA
EV SSL Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED: If requesting Websites trust bit, need section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_Self-Assessment) to the Bugzilla Bug.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. CP/CPS must clearly specify the procedures that the CA employs. Each documented procedure should state which subsection of BR section 3.2.2.4 it is complying with.	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED: If EV verification is performed, then provide URLs and section/page number information pointing directly	**Verified?**	Need Response From CA

	to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate. The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.		
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert.	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED section number of the CP/CPS that states that multi-factor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)	**Verified?**	Need Response From CA
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	**Verified?**	Need Response From CA

Root Case Record # 4

Root Case Information

Root Certificate Name	TnTrust Gov CA	**Root Case No**	R00000318
Request Status	Initial Request Received	**Case Number**	00000174

Certificate Data

Certificate Issuer Common Name	
O From Issuer Field	
OU From Issuer Field	
Valid From	
Valid To	
Certificate Serial Number	
Subject	
Signature Hash	

Algorithm	
Public Key Algorithm	
SHA-1 Fingerprint	
SHA-256 Fingerprint	
Certificate Fingerprint	
Certificate Version	

Technical Information about Root Certificate

Certificate Summary	The main purpose of the TnTrust Gov CA is signing governmental SSL certificates (OV SSL).	Verified?	Need Response From CA
Root Certificate Download URL	http://crl.certification.tn/tunisiagovca.crl	Verified?	Need Response From CA
CRL URL(s)	http://crl.certification.tn/tntrustgovca.crl	Verified?	Need Response From CA
OCSP URL(s)	va.certification.tn	Verified?	Need Response From CA
Mozilla Trust Bits	Email; Websites	Verified?	Need Response From CA
SSL Validation Type	OV; EV	Verified?	Need Response From CA
Mozilla EV Policy OID(s)	2.16.788.1.2.6.1.9.1.2	Verified?	Need Response From CA
Root Stores Included In	Microsoft	Verified?	Need Response From CA
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	Verified?	Need Response From CA

Test Websites or Example Cert

Test Website - Valid		Verified?	Need Response From CA
Test Website - Expired			
Test Website - Revoked			
Example Cert			
Test Notes	NEED: - If requesting Websites trust bit provide 3 URLs to 3 test websites (valid, expired, revoked) whose TLS/SSL cert chains up to this root. - If only requesting the Email trust bit, then attach an example S/MIME cert to the bug.		

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

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	Verified?	Need Response From CA

CA/Browser Forum Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs). BR Lint Test: https://github.com/awslabs/certlint	**Verified?**	Need Response From CA
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	**Verified?**	Need Response From CA
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	**Verified?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist, https://wiki.mozilla.org/CA/Subordinate_CA_Checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those subordinate CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of the CA/Browser Forum's Baseline Requirements - Mozilla's Root Store Policy	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA
CA Document		**Verified?**	Need Response From CA

Repository			
CP Doc Language			
CP		**Verified?**	Need Response From CA
CP Doc Language			
CPS		**Verified?**	Need Response From CA
Other Relevant Documents		**Verified?**	Need Response From CA
Auditor Name		**Verified?**	Need Response From CA
Auditor Website		**Verified?**	Need Response From CA
Auditor Qualifications		**Verified?**	Need Response From CA
Standard Audit	NEED: Audit statements meeting the requirements of Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	**Verified?**	Need Response From CA
EV SSL Audit Type		**Verified?**	Need Response From CA
EV SSL Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED: If requesting Websites trust bit, need section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_Self-Assessment) to the Bugzilla Bug.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. CP/CPS must clearly specify the procedures that the CA employs. Each documented procedure should state which subsection of BR section 3.2.2.4 it is complying with.	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED: If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and	**Verified?**	Need Response From CA

	describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate. The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.		
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert.	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED section number of the CP/CPS that states that multi-factor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)	**Verified?**	Need Response From CA
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	**Verified?**	Need Response From CA