Mozilla – CA Program

Required and Recommend	ed Practices	
Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices 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.	Publicly Available CP and CPS The Tunisian National Root CA supplied a complete Certification Policy (CP) and Certification Practice Statement (CPS) containing sufficient information to determine
		 whether and how the CA complies with the Mozilla policy requirements: The CP/CPS is publicly available from the NDCA's official web site (http://www.certification.tn/pub/CPCPS-TunisianNationalPKI.pdf). The format of the CP/CPS document is PDF. The CP/CPS is available in an English version. The Tunisian National Root CA provides references to the CP/CPS sections (e.g., by section number and/or page number) that address the requirements of the Mozilla policy.
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	
Forbidden and Potentially	Problematic Practices	1
Potentially	https://wiki.mozilla.org/CA/Forbidden or Problematic Practices	
Problematic	I have reviewed Mozilla's lists of Forbidden and Potentially Problematic	
Practices	Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.	
CA's Response	NEED: CA's response to each of the items listed in	
to Problematic	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	
Practices Root Case Record #1		
Root Case Record #1 Root Case Information		
Root Case Information Root Certificate Name	Tunisia National Root CA	
Request Status	Initial Request Received	
Certificate Data	1	
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:3 A:C0:55:45:33:67:D4:78:AF:9E	
Certificate Version	3	

Technical Information abo		
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	Microsoft	The Tunisian National Root CA is not yet included in Microsoft root store. An application
Treet steres merades m	Need Clarification From CA	has been submitted and the CA is waiting for the response.
Mozilla Applied	No constraints	The coordinate and the ciris waters for the response
Constraints	TVO CONSTRUINES	
Test Websites or Example	Cert	
Test Website - valid		The Tunisia National Root CA is a root CA which issue only:
Test website Expired		• CRL
Test website - revoked		OCSP certificate
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.	Intermediate CAs certificates.
Test Results (When Reques	sting the SSL/TLS Trust Bit)	
Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	The Tunisia National Root CA is a root CA which issue only: CRL
CA/Browser Forum Lint	NEED: The CA MUST check that they are not issuing	OCSP certificate
Test	certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs). BR Lint Test: https://github.com/awslabs/certlint	Intermediate CAs certificates.
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	
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	
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	List of the subordinate CAs that are signed by the Tunisia National Root CA are: Tunisia Gov CA: is an intermediate CA. There are two issuing CAs under this CA which are: TnTrust Gov CA: which issue these certificate profiles: OV SSL EV SSL OV Code Signing EV Code Signing VPN Timestamping TnTrust Qualified Gov CA: Qualified Signature Qualified Seal Tunisia Corporate CA: is an intermediate CA. There are two issuing CAs under this CA which are: TnTrust Corporate CA: which issue these certificate profiles: OV SSL OV SSL EV SSL
		which are: TnTrust Co

		EV Code Signing
		• VPN
		Timestamping
		TnTrust Qualified Corporate CA:
		Qualified signature
		Qualified Seal
Externally Operated	NEED: ¬ If this root has any subordinate CA certificates that are operated by	This root has no subordinate CA certificates that are operated by external third parties.
SubCAs	external third parties, then provide the information listed in the Subordinate CA	This foot has no supplement CA certificates that are operated by external third parties.
	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.	
Cross Signing	NEED: ¬ List all other root certificates for which this root certificate has issued	There are not any other root certificates for witch this root certificate has issued cross-
	cross¬signing certificates List all other root certificates that have issued	signing certificates.
	crosssigning certificates for this root certificate. ¬ If any such cross-signing	There are not any other root certificates that have issued crosssigning
	relationships exist, it is important to note whether the cross¬signing CAs'	certificates for this root certificate.
	certificates are already included in the Mozilla root store or not.	There are not any crosssigning relationships.
Technical Constraint on	NEED: CP/CPS documentation describing the technical and contractual controls	Section 1.3.3 of the CP/CPS describes the technical and contractual controls over any 3rd
3 rd party Issuer	over any 3rd party who may issue certs in this CA Hierarchy. This includes	party « Delegated Registration Authority (DRA) Delegated RAs have to abide by all the
	external RAs as well as External subCAs. References: - section 7.1.5 of the	requirements of the TN PKI CP/CPS. DRAs may, however implement more restrictive
	CA/Browser Forum's Baseline Requirements ¬ Mozilla's Root Store Policy	practices based on their internal requirements. Any DRA operating under this CP/CPS must
		adhere to the following rules: • The DRA must have a contractual agreement with the
		National Digital Certification Agency which indicates the authorization for their role as RA
		and clearly details the minimum requirements, processes and liabilities. • The registration
		process of any DRA must be provided by the National Digital Certification Agency. The
		latter has to audit and approve the process as meeting the quality requirements of this
		CP/CPS and therefore being equivalent to the registration process of the TN PKI RA. • The
		DRA must have an annual audit. All costs related to this audit are to be paid by the operator
		of the RA. Failure to pass the annual audit leads to the revocation of DRA privileges. »
		For the moment, the Tunisia National Root CA does not use external RAs. We have
Verification Policies and P		prepared a template of contract between NDCA and delegated RA.
Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	The CP/CPS is provided in English language.
CA Document Repository	NEED. Languages that the C1/C1 5 and other documents are provided in.	http://www.certification.tn/pub/CPCPS-TunisianNationalPKI.pdf
CP Doc Language		English
CPS Doc Language		English
Other Relevant		The relying parties agreement are made in French language.
Documents		The felying parties agreement are made in Flench language.
Auditor Name		Mr. Philippe Bouchet from the certification body LSTI
Auditor Website		http://lsti-certification.fr
Auditor Qualifications		LSTI has been accredited pursuant to the accreditation certificate of French Accreditation
Auditor Qualifications		Body COFRAC with registration number 5-0546 in accordance with NF EN ISO/IEC
		17065:2013 as a certification body for products, processes, and services in accordance with
		the Annex of the accreditation certificate and the ETSI EN 319 403.
Standard Audit	NEED: Audit statements meeting the requirements of Mozilla's Root Store	
Starrant of Taget	Policy.	
Standard Audit type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security
		requirements applicable to trust service providers issuing certificates - Part 1: General
		requirements
		EÑ 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security
		requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust
		service providers issuing EU qualified certificate
Standard Audit Statement		21 march 2017
Date		

BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	
RG Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
BR Audit Statement Date		21 march 2017
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	
EV SSL Audit		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
EV SSL Audit Statement Dare		21 march 2017
BR Commitment 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.	Tunisian National Root CA conform to the current version of the CA/Browser Forum (CABF) requirements including: Guidelines for the Issuance and Management of Extended Validation (EV) Certificates, Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Published at www.cabforum.org. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR SelfAssessment) to the Bugzilla Bug.	I have attached the BR Self Assessment two months ago.
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.	Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name. • To validate the name of the organization, the requester provides official documentation about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form.

<u> </u>		
		In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization. NDCA have also internal procedures that are guidelines for the operators to for validating
		the Applicant's ownership or control of the domain:
		The FQDN of the server to be used in the certificate; The name and surname of the CHN; The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the name of the requested domain; The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three months; A certificate of non-bankruptcy for private organizations.
ENGCLN 'C '	NEED ICEN . C C . 1 d 1 IIII . 1 /	• A power of attorney for requests of certificates filed by an agent.
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. 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	Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name. • To validate the name of the organization, the requester provides official documentation about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form.
		In addition, the TN PKI RA:

		Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain:
		The FQDN of the server to be used in the certificate; The name and surname of the CHN; The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the name of the requested domain; The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three months; A certificate of non-bankruptcy for private organizations.
		A power of attorney for requests of certificates filed by an agent.
Organisation Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name. • To validate the name of the organization, the requester provides official documentation about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form. In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing

		the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain:
		The FQDN of the server to be used in the certificate; The name and surname of the CHN; The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the name of the requested domain; The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three months; A certificate of non-bankruptcy for private organizations.
		A power of attorney for requests of certificates filed by an agent.
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.	Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name. • To validate the name of the organization, the requester provides official documentation about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form.
		In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information

Code Signing Subscriber	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	(employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization. NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain: • The FQDN of the server to be used in the certificate; • The name and surname of the CHN; • The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; • Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", " Hostmaster ", or" postmaster "@ the name of the requested domain; • The General Conditions of Use (GTC) signed by the legal representative; • An official extract from the trade register of the organization dating no longer than three months; • A certificate of non-bankruptcy for private organizations. • The CSR for the public key to be signed. • A power of attorney for requests of certificates filed by an agent. Yes. We need to activate Code Signing trust bit.
Pro		
Multi-factor Authentication	NEED section number of the CP/CPS that states that multifactor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)	Section 5.2.2 of the CP/CPS 5.2.2 Number of persons required per task Two or more persons are required for TN PKI CAs for the following tasks: (a) CA key generation = Three (3) persons (b) CA signing key activation = Three (3) persons (c) CA private key backup = Three (3) persons Where multiparty control for logical access is required, at least one of the participants is an administrator. All participants must serve in a trusted role as defined in Section 5.2.1 (Trusted Roles). Multiparty control for logical access are not achieved using personnel that serve in the Auditor Trusted Role. HSM Administrators uses HSM Smartcards for authentication. The HSM itself enforces dual control based on the HSM smartcards for the different functions. The number of needed HSMsmartcards (m) of the total number of produced HSM-smartcards (n) will be: (a) Key generation = 3 of 6 (b) Signing key activation = 3 of 8 (c) Private key backup and restore = 3 of 6 End-user certificate issuance requires the approval of at least two persons. End-user Certificate revocation requires the approval of at least two persons. Registration and Customer Services: Responsible Employees responsible for routine certification services such as customer services, document control, processes relating to certificate registration, generation and revocation. These employees are trusted roles. They access the RA system using a smart card and a PIN code.
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security	Section 6.8 of the CP/CPS: 6.8 Network security controls TN PKI's CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. TN PKI's customer support and vetting

Root Case Information Root Certificate Name			intermediate CAs Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. It is TN PKI's security policy to block all ports and protocols and open only necessary ports to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. All firewall configurations and changes thereto are documented, authorized, tested and implemented in accordance with change management procedures. TN PKI's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.
Root Certificate Name	Root Case Record # 2		
Request Status			
Certificate Issuer Commun			
Certificate Issuer Commun National Root CA		Initial Request Received	
Name			
OU From Issuer Field		Tunisia National Root CA	
Valid From 2016 Nov 29		National digital Certification Agency	
Valid To			
Certificate Serial Number 782c1009830a4bee			
Subject			
C=TN Signature Hash Algorithm Sha256WithRSAEncryption			
Public Key Algorithm	J.	C=TN	
SHA1 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:F2:8 5:B4:5F:45:52:57:57:13:FC:FE Certificate Version 3 Technical Information about Root Certificate Certificate Summary Need response from CA The Tunisia Gov CA issue : CRL			
37:A7:0C:F1:69:76:0A:64			
S:B4:5F:45:52:57:57:13:FC:FE	SHA-256 Fingerprint		
Technical Information about Root Certificate Certificate Summary Need response from CA The Tunisia Gov CA issue: CRL OCSP Certificate Certificate of issuing Authority. There are two issuing authorities under this CA which are: Thurst Gov CA Thirtust Go	Certificate Fingerprint		
Certificate Summary	Certificate Version	3	
CRL OCSP Certificate Certificate of issuing Authority. There are two issuing authorities under this CA which are: TnTrust Gov CA TnTrust Qualified Gov CA Root Certificate Download URL CRL URL(s) Need response from CA OCSP URL(s) Need response from CA Mozilla Trust Bits Need response from CA Mozilla Trust Bits Need response from CA SSL Validation Type Need response from CA Mozilla EV Policy OID(s) Need response from CA OV, EV Mozilla EV Policy OID(s) Need response from CA 2.16.788.1.2.6.1.9.1.2	Technical Information abo	ut Root Certificate	
Root Certificate Download URL Need response from CA http://crl.certification.tn/tunrootca.crl CRL URL(s) Need response from CA http://crl.certification.tn/tunisiagovca.crl OCSP URL(s) Need response from CA http://va.vertification.tn Mozilla Trust Bits Need response from CA Email, website SSL Validation Type Need response from CA OV, EV Mozilla EV Policy OID(s) Need response from CA 2.16.788.1.2.6.1.9.1.2	Certificate Summary	Need response from CA	 CRL OCSP Certificate Certificate of issuing Authority. There are two issuing authorities under this CA which are: TnTrust Gov CA
URL CRL URL(s) Need response from CA OCSP URL(s) Need response from CA Mozilla Trust Bits Need response from CA SSL Validation Type Need response from CA Mozilla EV Policy OID(s) Need response from CA Mozilla EV Policy OID(s) Need response from CA OV, EV 2.16.788.1.2.6.1.9.1.2			
OCSP URL(s) Need response from CA http://va.vertification.tn Mozilla Trust Bits Need response from CA Email, website SSL Validation Type Need response from CA OV, EV Mozilla EV Policy OID(s) Need response from CA 2.16.788.1.2.6.1.9.1.2			http://crl.certification.tn/tunrootca.crl
OCSP URL(s) Need response from CA http://va.vertification.tn Mozilla Trust Bits Need response from CA Email, website SSL Validation Type Need response from CA OV, EV Mozilla EV Policy OID(s) Need response from CA 2.16.788.1.2.6.1.9.1.2			
SSL Validation Type Need response from CA OV, EV Mozilla EV Policy OID(s) Need response from CA 2.16.788.1.2.6.1.9.1.2		Need response from CA	
Mozilla EV Policy OID(s) Need response from CA 2.16.788.1.2.6.1.9.1.2	Mozilla Trust Bits	Need response from CA	Email, website
D-4 C4 In-daddin N-4 C4	Mozilla EV Policy OID(s)		
Root Stores Included in Need response from CA The Tunisian National Root CA is not yet included in Microsoft root store. An apple has been submitted and the CA is waiting for the response.	Root Stores Included in	Need response from CA	The Tunisian National Root CA is not yet included in Microsoft root store. An application has been submitted and the CA is waiting for the response.
Mozilla Applied Need response from CA No contraints		Need response from CA	
Test Websites or Example Cert		Cert	
Test Website - valid The Tunisia Gov CA is an intermediateCA which issue only:			The Tunisia Gov CA is an intermediateCA which issue only:

Test website Expired		• CRL
Test website - revoked		
	NEED 10 (1 W.1.)	OCSP certificate
Test notes	NEED: - If requesting Websites trust	Issuing CAs certificates.
	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 Requ	esting the SSL/TLS trust Bit)	•
Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/	The Tunisia Gov CA is an intermediateCA which issue only:
	make sure there aren't any errors.	• CRL
CA/Browser Forum Lint	NEED: The CA MUST check that they are not issuing	OCSP certificate
Test	certificates that violate any of the CA/Browser Forum	Issuing CAs certificates.
1650	Baseline Requirements (BRs). BR Lint Test: https://github.com/awslabs/certlint	Issuing CAS certificates.
Test Website Lint Test	NEED: The CA MUST check that they are not issuing	
Test Website Lint Test	certificates that violate any of the X.509 rules.	
	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	
CA Hierarchy Informatio	on .	
CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated	The Tunisia Gov CA is an intermediate CA. This CA issue two issuing CA:
	with this root CA certificate List and/or describe all of the subordinate CAs	TnTrust Gov CA: which issue these certificate profiles:
	that are signed by this root Identify which of the subordinate CAs are	OV SSL
	internally operated; e.g. list the subordinate CAs that operated by the CA	EV SSL
	organization associated with the root CA. For example, this might include	OV Code Signing
	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.	EV Code Signing
	non-qualified certificates, EV certificates vs. non-EV certificates, SSL	• VPN
		Timestamping
	certificates vs. email certificates, and so on. ¬ It might also include subordinate	TnTrust Qualified Gov CA:
	CAs operated for the benefit of specific third parties. In this case note that we do	Qualified signature
	not require that the CA submit a complete customer list; rather we are interested	Qualified Seal
	in the general type and nature of the third party arrangements	Quantita san
Externally Operated	NEED: ¬ If this root has any subordinate CA certificates that are operated by	This CA has no subordinate CA certificates that are operated by external third parties.
SubCAs	external third parties, then provide the information listed in the Subordinate CA	This critical is substantice criticales that are operated by external time parties.
BubCAs	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	
G G: :	themselves as separate trust anchors.	
Cross Signing	NEED: ¬ List all other root certificates for which this root certificate has issued	There are not any other root certificates for witch this root certificate has issued cross-
	cross-signing certificates List all other root certificates that have issued	signing certificates.
	crosssigning certificates for this root certificate. ¬ If any such cross-signing	There are not any other root certificates that have issued crosssigning
	relationships exist, it is important to note whether the cross¬signing CAs'	certificates for this root certificate.
	certificates are already included in the Mozilla root store or not.	There are not any crosssigning relationships.
Technical Constraint on	NEED: CP/CPS documentation describing the technical and contractual controls	Section 1.3.3 of the CP/CPS describes the technical and contractual controls over any 3rd
3 rd party Issuer	over any 3rd party who may issue certs in this CA Hierarchy. This includes	party « Delegated Registration Authority (DRA) Delegated RAs have to abide by all the
5 party issuer	external RAs as well as External subCAs. References: - section 7.1.5 of the	requirements of the TN PKI CP/CPS. DRAs may, however implement more restrictive
	CA/Browser Forum's Baseline Requirements - Mozilla's Root Store Policy	practices based on their internal requirements. Any DRA operating under this CP/CPS must
	Crabiowsci i orani s basenne requirements - wozina s reou store roney	adhere to the following rules: • The DRA must have a contractual agreement with the
		National Digital Certification Agency which indicates the authorization for their role as RA
		and clearly details the minimum requirements, processes and liabilities. • The registration
		process of any DRA must be provided by the National Digital Certification Agency. The
		latter has to audit and approve the process as meeting the quality requirements of this

		CP/CPS and therefore being equivalent to the registration process of the TN PKI RA. • The DRA must have an annual audit. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit leads to the revocation of DRA privileges. » For the moment, the Tunisia National Root CA does not use external RAs. We have prepared a template of contract between NDCA and delegated RA.
Verification Policies and P	Practices	prepared a template of contract between NDCA and delegated RA.
Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	The CP/CPS is provided in English language.
CA Document Repository	11222. Earlightages that the C17C15 and other documents are provided in:	http://www.certification.tn/pub/CPCPS-TunisianNationalPKI.pdf
CP Doc Language		English
CPS Doc Language		English
Other Relevant		The relying parties agreement are made in French language.
Documents		The ferring parties agreement are made in French language.
Auditor Name		Mr. Philippe Bouchet from the certification body LSTI
Auditor Website		http://lsti-certification.fr
Auditor Qualifications		LSTI has been accredited pursuant to the accreditation certificate of French Accreditation
Traditor Qualifications		Body COFRAC with registration number 5-0546 in accordance with NF EN ISO/IEC 17065:2013 as a certification body for products, processes, and services in accordance with the Annex of the accreditation certificate and the ETSI EN 319 403.
Standard Audit	NEED: Audit statements meeting the requirements of Mozilla's Root Store Policy.	
Standard Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
Standard Audit Statement		21 march 2017
Date		21 match 2017
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	
BR Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
BR Audit Statement Date		21 march 2017
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	
EV SSL Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
EV SSL Audit Statement Date		21 march 2017
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.	Tunisian National Root CA conform to the current version of the CA/Browser Forum (CABF) requirements including: • Guidelines for the Issuance and Management of Extended Validation (EV) Certificates, • Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and, • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,

		Published at www.cabforum.org. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR SelfAssessment) to the Bugzilla Bug.	I have attached the BR Self Assessment two months ago.
SSL verification Procedures	(https://wiki.mozilla.org/CA/BR_SclfAssessment) to the Bugzilla Bug. 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.	Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name. • To validate the name of the organization, the requester provides official documentation about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures required on the registration form. In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in

		• The CSR for the public key to be signed.
		A power of attorney for requests of certificates filed by an agent.
EV SSL Verification	NEED: If EV verification is performed, then provide URLs and section/page	Section 3.2.2 of the CP/CPS
Procedures	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. The EV verification documentation	 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory.
	must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.	• The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name.
		 To validate the name of the organization, the requester provides official documentation about the organization. The use of the organization's name is authorized by one or more legal representatives of
		the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its
		representatives. The domain owner may be determined through the WHOIS information
		provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is
		present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form.
		In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain:
		 The FQDN of the server to be used in the certificate; The name and surname of the CHN; The personal identification data of the RCS as well as the legal representative including a
		valid official document of identity, including a photograph of identity; • Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the
		case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", " Hostmaster ", or" postmaster "@ the name of the requested domain;
		 The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three months;
		A certificate of non-bankruptcy for private organizations. The CSR for the public key to be signed.
		A power of attorney for requests of certificates filed by an agent.

	I	
Organization Verification	NEED: CP/CPS sections that describe identity and organization	Section 3.2.2 of the CP/CPS
Procedures	verification procedures for cert issuance.	3.2.2 Authentication of organization identity The DN of a certificate issued by one of the
		issuing CAs of TN PKI may contain one instance of the organization field. Should the
		requester decide to make the organization field part of the DN, the following rules are
		adhered to:
		• The use of the organization field means that the use of the country field is mandatory.
		The registration process of any registration authority operating under this CP/CPS
		contains provisions to determine the identity of an organization and to authorize the use of
		its name.
		• To validate the name of the organization, the requester provides official documentation
		about the organization.
		• The use of the organization's name is authorized by one or more legal representatives of
		the organization, and handwritten personal signatures is included on the registration form.
		The use of a domain name in a FQDN is authorized by the domain owner or its
		representatives. The domain owner may be determined through the WHOIS information
		provided by the domain registrar. Should an organization be listed as the domain owner,
		authorization is given by one or more legal representatives of the organization with
		handwritten personal signatures on the registration form. Should an individual be listed as
		the owner, this individual personally signs the registration form. The RA will create a copy
		of all required supporting documentation. Alternatively and only if an organization name is
		present in the certificate subject, domain validation according to section 3.1 may be used to
		obtain authorization of the use of the domain name in a FQDN. In this case the handwritten
		signatures of the authorization of the organizational name are the only authorization
		signatures required on the registration form.
		In addition, the TN PKI RA:
		Determines that the Organization exists by using at least one third party identity proofing
		service or database, or alternatively, organizational documentation issued by or filed with
		the applicable government that confirms the existence of the organization, and
		• Uses information contained in the business records or databases of business information
		(employee or customer directories) of an RA approving certificates to its own affiliated
		individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to
		the organization, the employment with the Organization of the individual submitting the
		Certificate Application and, when appropriate, his/her authority to act on behalf of the
		Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating
		the Applicant's ownership or control of the domain:
		the Applicant's ownership of control of the dollarin.
		• The FQDN of the server to be used in the certificate;
		The name and surname of the CHN;
		• The personal identification data of the RCS as well as the legal representative including a
		valid official document of identity, including a photograph of identity;
		• Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a
		minimum, an e-mail address as contained in the WHOIS must be used. If this is not the
		case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or
		in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the
		name of the requested domain;
		The General Conditions of Use (GTC) signed by the legal representative;
		• An official extract from the trade register of the organization dating no longer than three
		months;
		A certificate of non-bankruptcy for private organizations. The GOD is a second structure of the control o
		• The CSR for the public key to be signed.
		A power of attorney for requests of certificates filed by an agent.
Email Address	NEED if Email trust bit requested Sections of CP/CPS that sufficiently	Section 3.2.2 of the CP/CPS
Verification Procedures	describe the verification steps that are taken to confirm the	3.2.2 Authentication of organization identity The DN of a certificate issued by one of the

	ownership/control of the email address to be included in the cert.	issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory.
		• The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name.
		To validate the name of the organization, the requester provides official documentation about the organization. The use of the organization's name is authorized by one or more legal representatives of
		the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its
		representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with
		handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization
		signatures required on the registration form.
		In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain:
		The FQDN of the server to be used in the certificate; The name and surname of the CHN; The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the name of the requested domain; The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three months; A certificate of non-bankruptcy for private organizations.
		• A power of attorney for requests of certificates filed by an agent.
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	Yes. We need to activate Code Signing trust bit.
Multi-factor	NEED section number of the CP/CPS that states that multifactor	Section 5.2.2 of the CP/CPS
Authentication	authentication is enforced for all accounts capable of directly causing	5.2.2 Number of persons required per task

Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	Two or more persons are required for TN PKI CAs for the following tasks: (a) CA key generation = Three (3) persons (b) CA signing key activation = Three (3) persons (c) CA private key backup = Three (3) persons Where multiparty control for logical access is required, at least one of the participants is an administrator. All participants must serve in a trusted role as defined in Section 5.2.1 (Trusted Roles). Multiparty control for logical access are not achieved using personnel that serve in the Auditor Trusted Role. HSM Administrators uses HSM Smartcards for authentication. The HSM itself enforces dual control based on the HSM smartcards for the different functions. The number of needed HSMsmartcards (m) of the total number of produced HSM-smartcards (n) will be: (a) Key generation = 3 of 6 (b) Signing key activation = 3 of 8 (c) Private key backup and restore = 3 of 6 End-user certificate issuance requires the approval of at least two persons. End-user Certificate revocation requires the approval of at least two persons. Registration and Customer Services : Responsible Employees responsible for routine certification services such as customer services, document control, processes relating to certificate registration, generation and revocation. These employees are trusted roles. They access the RA system using a smart card and a PIN code. Section 6.8 of the CP/CPS: 6.8 Network security controls TN PKI's CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. TN PKI's customer support and vetting workstations are also protected by firewalls, and only use internal IP addresses. Root and intermediate CAs Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of
		changes thereto are documented, authorized, tested and implemented in accordance with
		change management procedures. TN PKI's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.
Root Case Record # 3		
Root Case Information		
Root Certificate Name	TnTrust Gov CA	
Request Status	Initial Request Received	
Certificate Data		
Certificate Issuer Commun Name	TnTrust Gov CA	
O From Issuer Field	National Digital Certification Agency	
OU From Issuer Field		
Valid From	2016 Nov 29	
Valid To	2026 Nov 29	
Certificate Serial Number	36716fa436ecc2d2	
Subject	CN = TnTrust Gov CA, O = National Digital Certification Agency, L = Tunis,	C = TN
Signature Hash Algorithm	Sha256WithRSAEncryption	
Public Key Algorithm	RSA 3072 bits	
SHA1 Fingerprint	A1:6B:C7:76:BE:65:1E:5E:1A:A1:09:D7:E1:42:6E:F0:42:59:B2:C4	

SHA-256 Fingerprint	55:17:5F:1C:24:C2:58:0E:0C:29:4B:9B:BE:86:D0:AE:C0:9B:43:B8:62:AF:B3:EC:81:27:06:1A:CC:E7:FB:06	
Certificate Fingerprint	a16bc776be651e5e1aa109d7e1426ef04259b2c4	
Certificate Version	3	
Technical Information abo		
Certificate Summary	Need Response From CA	The TnTrust Gov CA is an issuing CA. This CA issue these profiles fo certificates: OV SSL EV SSL OV Code Signing EV Code Signing VPN Timestamping
Root Certificate Download URL	Need Response From CA	http://crl.certification.tn/tunisiagovca.crl
CRL URL(s)	Need Response From CA	http://crl.certification.tn/tntrustgovca.crl
OCSP URL(s)	Need Response From CA	http://va.certification.tn
Mozilla Trust Bits	Need Response From CA	Emai, websites
SSL Validation Type	Need Response From CA	OV; EV
Mozilla EV Policy OID(s)	Need Response From CA	2.16.788.1.2.6.1.9.1.2
Root Stores Included In	Need Response From CA	The Tunisian National Root CA is not yet included in Microsoft root store. An application has been submitted and the CA is waiting for the response.
Mozilla Applied Constraints	Need Response From CA	No contraints
Test Websites or Example		
Test Website - valid	Need Response From CA	 OV certificate: https://valid-gov-ov.certification.tn
Test website Expired	Need Response From CA	OV certificate: https://expired-gov-ov.certification.tn EV certificate: https://expired-gov-ev.certification.tn
Test website - revoked	Need Response From CA	OV certificate: https://revoked-gov-ov.certification.tn EV certificate: https://revoked-gov-ev.certification.tn
Test notes	NEED: - If requesting Websites trust bit provide 3 URLs to 3 test webs trust bit, then attach an example S/MIME cert to the bug.	sites (valid, expired, revoked) whose TLS/SSL cert chains up to this root If only requesting the Email
Test results (When Reques	ting the SSL/TLS Trust Bit)	
Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/make sure there aren't any errors.	I have checked with the https://crtificate.revocationcheck.com/ the URL of this web site: https://crtification.tn/tunrootca.crl CRL information Source: CRL Distribution Point listed in Certificate Location: http://crt.certification.tn/tunrootca.crl Size: 750 bytes (DER data) Response time: 370.602217ms This update: Nov 8, 2017 11:37:03 AM Next update: Nov 8, 2018 11:37:03 AM Revoked: No Revoked: No Revoked certificates in CRL: 0 Relevant server response headers Date: Nov 20, 2017 2:32:35 PM Last Modified: Nov 8, 2017 1:47:02 PM Expires: Jan 1, 1 1:00:00 AM

Server and network information

Server Software: Apache

- Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)'
- This CRL file is DER encoded
- Response is already valid
- Response is not expired
- 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 a root CA CRL which have a validity of 365 days

http://crl.certification.tn/tunisiagovca.crl

CRL information

Source: CRL Distribution Point listed in Certificate **Location:** http://crl.certification.tn/tunisiagovca.crl

Size: 740 bytes (DER data) Response time: 391.794843ms

This update: Nov 8, 2017 11:38:33 AM **Next update:** Nov 8, 2018 11:38:33 AM

Revoked: No

Revoked certificates in CRL: 0

Relevant server response headers

Date: Nov 20, 2017 2:48:01 PM

Last Modified: Nov 8, 2017 1:47:00 PM

Expires: Jan 1, 1 1:00:00 AM

Server and network information

Server Software: Apache

- Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)'
- This CRL file is DER encoded
- Response is already valid
- Response is not expired
- 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 an intermediate CA CRL which have a validity of 365 days as mentioned in the CABForum Base line requirements section 4.9.7 CRL Issuance Frequency: « For the status of Subordinate CA Certificates:

The CA SHALL update and reissue CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field MUST NOT be more than twelve months beyond the value of the

		thisUpdate field. »
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	I checked that the TnTrustGov CA does not issue certificates that violate any of the CA/Browser Forum.
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	I checked that TnTrust Gov CA does not issue certificates that violate any of the X.509 rules.
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 checked the URL https://tls-observatory.services.mozilla.com/static/ev-checker.html with these parameters:
		TLS Server : https://tms.certification.tn
		EV Policy OID: 2.16.788.1.2.6.1.9.1.2
		I have this error message: « ev-checker reported failure: ev-checker did not exit successfully. exit status 1, Stderr: BuildCertChain failed: SEC_ERROR_POLICY_VALIDATION_FAILED Cert chain fails policy validation It appears be the case that the end-entity certificate was issued directly by the root. There should be at least one intermediate in the certificate issuance chain." But the certificate of https://tms.certification.tn is not issued by a root CA bu issued by an
CA Hierarchy Informatio		issuing CA: TnTrust Gov CA.
CA Hierarchy 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 internallyoperated; 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	The TnTrust Gov CA is an issuing CA. this CA issue these types of certificate profiles: OV SSL EV SSL OV Code Signing EV Code Signing VPN Timestamping
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.	This CA has no subordinate CA certificates that are operated by external third parties.
Cross Signing	NEED: List all other root certificates for which this root certificate has issued crosssigning certificates List all other root certificates that have issued crosssigning certificates for this root certificate. If any such crosssigning relationships exist, it is important to note whether the crosssigning CAs' certificates are already included in the Mozilla root store or not.	There are not any other root certificates for witch this root certificate has issued cross-signing certificates. There are not any other root certificates that have issued crosssigning certificates for this root certificate. There are not any crosssigning relationships.
Technical Constraint on 3 rd 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 -	Section 1.3.3 of the CP/CPS describes the technical and contractual controls over any 3rd party « Delegated Registration Authority (DRA) Delegated RAs have to abide by all the requirements of the TN PKI CP/CPS. DRAs may, however implement more restrictive practices based on their internal requirements. Any DRA operating under this CP/CPS must adhere to the following rules: • The DRA must have a contractual agreement with the

	Mozilla's Root Store Policy	National Digital Certification Agency which indicates the authorization for their role as RA and clearly details the minimum requirements, processes and liabilities. • The registration process of any DRA must be provided by the National Digital Certification Agency. The latter has to audit and approve the process as meeting the quality requirements of this CP/CPS and therefore being equivalent to the registration process of the TN PKI RA. • The DRA must have an annual audit. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit leads to the revocation of DRA privileges. » For the moment, the Tunisia National Root CA does not use external RAs. We have prepared a template of contract between NDCA and delegated RA.
Verification Policies and I		
Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	The CP/CPS is provided in English language.
CA Document Repository		http://www.certification.tn/pub/CPCPS-TunisianNationalPKI.pdf
CP Doc Language		English
CPS Doc Language		English
Other Relevant		The relying parties agreement are made in French language.
Documents		
Auditor Name		Mr. Philippe Bouchet from the certification body LSTI
Auditor Website		http://lsti-certification.fr
Auditor Qualifications		LSTI has been accredited pursuant to the accreditation certificate of French Accreditation Body COFRAC with registration number 5-0546 in accordance with NF EN ISO/IEC 17065:2013 as a certification body for products, processes, and services in accordance with the Annex of the accreditation certificate and the ETSI EN 319 403.
Standard Audit	NEED: Audit statements meeting the requirements of Mozilla's Root Store Policy.	
Standard Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
Standard Audit Statement Date		21 march 2017
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	
BR Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
BR Audit Statement Date		21 march 2017
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	
EV SSL Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
EV SSL Audit Statement Date		21 march 2017
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.	Tunisian National Root CA conform to the current version of the CA/Browser Forum (CABF) requirements including: • Guidelines for the Issuance and Management of Extended Validation (EV) Certificates,

		Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Published at www.cabforum.org. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR SelfAssessment) to the Bugzilla Bug.	I have attached the BR Self Assessment two months ago.
BR Self Assessment 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.	Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name. • To validate the name of the organization, the requester provides official documentation about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form. In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable gove
		individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain:
		The FQDN of the server to be used in the certificate; The name and surname of the CHN; The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the name of the requested domain;

		 The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three months; A certificate of non-bankruptcy for private organizations. The CSR for the public key to be signed. A power of attorney for requests of certificates filed by an agent.
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. 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.	A power of attorney for requests of certificates filed by an agent. Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name. • To validate the name of the organization, the requester provides official documentation about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form. In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, or
		• An official extract from the trade register of the organization dating no longer than three

D: CP/CPS sections that describe identity and organization cation procedures for cert issuance.	A power of attorney for requests of certificates filed by an agent. Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name. • To validate the name of the organization, the requester provides official documentation
	about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a cop of all required supporting documentation. Alternatively and only if an organization name in present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritte signatures of the authorization of the organizational name are the only authorization signatures required on the registration form.
	In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
	NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain:
	 The FQDN of the server to be used in the certificate; The name and surname of the CHN; The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the name of the requested domain; The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three

• A certificate of non-bankruptcy for private organizations.

		• The CSR for the public key to be signed.
		• A power of attorney for requests of certificates filed by an agent.
Email Address	NEED if Email trust bit requested Sections of CP/CPS that sufficiently	Section 3.2.2 of the CP/CPS
Verification Procedures	describe the verification steps that are taken to confirm the	3.2.2 Authentication of organization identity The DN of a certificate issued by one of the
	ownership/control of the email address to be included in the cert.	issuing CAs of TN PKI may contain one instance of the organization field. Should the
		requester decide to make the organization field part of the DN, the following rules are
		adhered to:
		• The use of the organization field means that the use of the country field is mandatory.
		• The registration process of any registration authority operating under this CP/CPS
		contains provisions to determine the identity of an organization and to authorize the use of
		its name.
		• To validate the name of the organization, the requester provides official documentation
		about the organization.
		• The use of the organization's name is authorized by one or more legal representatives of
		the organization, and handwritten personal signatures is included on the registration form.
		• The use of a domain name in a FQDN is authorized by the domain owner or its
		representatives. The domain owner may be determined through the WHOIS information
		provided by the domain registrar. Should an organization be listed as the domain owner,
		authorization is given by one or more legal representatives of the organization with
		handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy
		of all required supporting documentation. Alternatively and only if an organization name is
		present in the certificate subject, domain validation according to section 3.1 may be used to
		obtain authorization of the use of the domain name in a FQDN. In this case the handwritten
		signatures of the authorization of the organizational name are the only authorization
		signatures required on the registration form.
		In addition, the TN PKI RA:
		• Determines that the Organization exists by using at least one third party identity proofing
		service or database, or alternatively, organizational documentation issued by or filed with
		the applicable government that confirms the existence of the organization, and
		• Uses information contained in the business records or databases of business information
		(employee or customer directories) of an RA approving certificates to its own affiliated
		individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to
		the organization, the employment with the Organization of the individual submitting the
		Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
		Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating
		the Applicant's ownership or control of the domain:
		• The FQDN of the server to be used in the certificate;
		• The name and surname of the CHN;
		• The personal identification data of the RCS as well as the legal representative including a
		valid official document of identity, including a photograph of identity;
		• Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a
		minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or
		in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the
		name of the requested domain;
		The General Conditions of Use (GTC) signed by the legal representative;
		• An official extract from the trade register of the organization dating no longer than three
		months;
		• A certificate of non-bankruptcy for private organizations.
		• The CSR for the public key to be signed.
		• A power of attorney for requests of certificates filed by an agent.

Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	Yes. We need to activate Code Signing trust bit.
Multi-factor Authentication	NEED section number of the CP/CPS that states that multifactor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)	Section 5.2.2 of the CP/CPS 5.2.2 Number of persons required per task Two or more persons are required for TN PKI CAs for the following tasks: (a) CA key generation = Three (3) persons (b) CA signing key activation = Three (3) persons (c) CA private key backup = Three (3) persons Where multiparty control for logical access is required, at least one of the participants is an administrator. All participants must serve in a trusted role as defined in Section 5.2.1 (Trusted Roles). Multiparty control for logical access are not achieved using personnel that serve in the Auditor Trusted Role. HSM Administrators uses HSM Smartcards for authentication. The HSM itself enforces dual control based on the HSM smartcards for the different functions. The number of needed HSMsmartcards (m) of the total number of produced HSM-smartcards (n) will be: (a) Key generation = 3 of 6 (b) Signing key activation = 3 of 8 (c) Private key backup and restore = 3 of 6 End-user certificate issuance requires the approval of at least two persons. End-user Certificate revocation requires the approval of at least two persons. Registration and Customer Services: Responsible Employees responsible for routine certification services such as customer services, document control, processes relating to certificate registration, generation and revocation. These employees are trusted roles. They access the RA system using a smart card and a PIN code.
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	Section 6.8 of the CP/CPS: 6.8 Network security controls TN PKI's CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. TN PKI's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root and intermediate CAs Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. It is TN PKI's security policy to block all ports and protocols and open only necessary ports to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. All firewall configurations and changes thereto are documented, authorized, tested and implemented in accordance with change management procedures. TN PKI's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

Root Case Record # 4	Root Case Record # 4		
Root Case Information			
Root Certificate Name	Tunisia Corporate CA		
Request Status	Initial Request Received		
Certificate Data			
Certificate Issuer Commun	Tunisia National Root CA		
Name			
O From Issuer Field	National Digital Certification Agency		
OU From Issuer Field			
Valid From	2016 Nov 29		
Valid To	2032 Feb 29		

Subject CN-Turnisa Corporate CA, Olf-mall, O-National Digital Cartification Agency, C-TN Signature Hath Algorithm Sha259 WithRSAILarception	Certificate Serial Number	35d821ddca93b331	
C-TN Signature Hadh Algorithm Sha250WinRSAEneryption R8A 4096 bits ShA17 Ingerprint ECC2486832A6549-D183-64-2CF3.D1.B1.Ta.17.BC.52.D5.D6 ShA17 Ingerprint ECC2486832A6549-D183-64-2CF3.D1.B1.Ta.17.BC.52.D5.D6 ShA17 Ingerprint ECC248683A6549-D183-64-2CF3.D1.B1.Ta.17.BC.52.D5.D6 ShA17 Ingerprint ECC248683A6549-D183-64-2CF3.D1.B1.Ta.17.BC.52.D5.D6 Sha17 Ingerprint ECC248683A6549-D183-64-2CF3.D1.B1.Ta.17.BC.52.D5.D6 Sha17 Ingerprint ECC248683A6549-D183-64-2CF3.D1.B1.Ta.17.BC.52.D5.D6 Sha17 Ingerprint ECC248683A6549-D184-52-D18-A7-2S.SA.FT-RA60D.FT-SA.47.DF ECC448-D18-D18-D18-D18-D18-D18-D18-D18-D18-D1			
Public Rey Algorithm RSA 4096 bits			
SHA-256 Fingerprint SHA-256 F	Signature Hash Algorithm	Sha256WithRSAEncryption	
SHA-256 Fingerprint EB6A-2ER-3FP-106-48S-6970A-179-A725-8A-EE-A6-0D-7E-3A-322-44-7D-EE (ER6A-EBF-3FP-14-17-EPT-1A Certificate Fingerprint Certificate Summary Certificate Summary Need response from CA The Tunisia Corporate CA issue: • CR1. • CR2 • CR3 • CR4 • CR5 • CR5 • CR5 • CR5 • CR5 • CR6 • CR6 • CR7 • CR			
Certificate Imagerprint ec-des883a659a9bi3642cfdbb1a17bc32d5d6 Certificate Version 3 Technical Information about Root Certificate Certificate Summary Need response from CA Root Certificate Summary Root Certificate Download URL CRI. URL (s) Need response from CA URL (a) Need response from CA URL (b) Root Response from CA URL (c) Root Response from CA Root Stores Included in Root Stores Included in Root Response from CA Root Response fr	SHA1 Fingerprint	EC:3C:48:68:3A:65:A9:A1:B3:64:2C:F3:D1:B1:1A:17:BC:52:D5:D6	
Certificate Fringerprint cscl-s46881a654a9a1b34d2e3d1b11a17bc52d5d6		BB:79:2E:A9:FD:06:48:56:97:0A:F9:A7:25:8A:EE:A6:0D:7E:3A:22:44:7D:EE	
Technical Information about Noot Certificate Certificate Summary	Certificate Fingerprint		
The Tunisia Corporate CA is size :			
CRL OCSP Certificate Certificate of issuing Authority.	Technical Information abo	ut Root Certificate	
Root Certificate Download Need response from CA http://crt.ecrtification.nr/tumrootea.crl http://crt.ecrtification.nr/tumrootea.crl http://crt.ecrtification.nr/tumrootea.crl http://crt.ecrtification.nr/tumrootea.crl http://crt.ecrtification.nr/tumsiacorporatea.crl http://crt.ecrt.ecrt.ecrt.ecrt.ecrt.ecrt.ecrt.e	Certificate Summary	Need response from CA	 CRL OCSP Certificate Certificate of issuing Authority. There are two issuing authorities under this CA which are:
Root Certificate Download Need response from CA http://crt.certification.tm/tunrootca.crl			
CRL URL(s) Need response from CA http://erl.certification.tn/tunisiacorporateca.crl	Post Cartificate Davim11	Need recogness from CA	
CRL URL(s) Need response from CA http://cr.certification.tm/unisiacorporateca.crl		Need response from CA	nup://cri.ceruncation.tn/tunrootca.cri
OCSP URL(s) Need response from CA http://wx.vertification.tn	1	Need response from CA	http://crl.certification.tp/tunisiacorporateca.crl
Mozilla Trust Bits Need response from CA Email, website SSL Validation Type Need response from CA OV, EV			
SSL Validation Type			1
Mozilla EV Policy OID(s) Need response from CA The Tunisian National Root CA is not yet included in Microsoft root store. An application has been submitted and the CA is waiting for the response.	1		
Root Stores Included in Need response from CA Mozilla Applied Constraints Need response from CA No contraints Test Website or Example Cert Test Website - railed Test website - revoked Test website - revoked 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. CA/Browser Forum Lint Test Baseline Requirements (BRs). BR Lint Test: https://github.com/rawslabs/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/rawslabs/certlint 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 The Tunisian National Root CA is an intermediate CA which issue only: **CRL** **OCSP certificate* **Issuing CAs certificates.* The Tunisia Corporate CA is an intermediate CA which issue only: **CRL** **OCSP certificates.* The Tunisia Corporate CA is an intermediate CA which issue only: **CRL** **OCSP certificates.* The Tunisia Corporate CA is an intermediate CA which issue only: **CRL** **OCSP certificates.* The Tunisia Corporate CA is an intermediate CA which issue only: **CRL** **OCSP certificates.* The Tunisia Corporate CA is an intermediate CA which issue only: **CRL** **OCSP certificates.* **Subject CA is an intermediate CA which issue only: **CRL** **OCSP certificates.* **In Tunisia Corporate CA is an intermediate CA which issue only: **CRL** **OCSP certificates.* **OCSP certificates.* **OCSP certificates.* **OCSP certificates.* **Subject CA is an intermediate CA which issue only: **CRL** **OCSP certificates.* **OC			
Mozilla Applied Need response from CA No contraints		1	
Test Website or Example Cert Test Website valid Test website Lypired Test website Expired Test website - revoked 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. CA/Browser Forum Lint Test Test Website 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 NEED: Test descend to the type of the X-509 rules. X.509 Lint Test: https://github.com/kroeckx/S509lint NEED: Test with rest violate any of the X-509 rules. X.509 Lint Test: https://github.com/kroeckx/S509lint 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			has been submitted and the CA is waiting for the response.
Test Website - valid Test Website - Valid Test website Expired Test website is Expired Test website - I 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. CA/Browser Forum Lint Test Test Website Lint Test NEED: The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Explain the State of the		Need response from CA	No contraints
Test Website - valid	1		
Test website Expired Test website - revoked 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. 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 Test Website Lint Test 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 **CRL** OCSP certificate* **Issuing CAs certificates* **OCSP certificate* **OCSP certificate* OCSP certificate* **Issuing CAs certificates* Issuing CAs certificates* **Issuing CAs certificates* **Is		Cert	
Test website - revoked 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. 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 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 EV Tested NEED: If EV treatment is being requested, then provide successful output from EV Testing Easy Version OCSP certificate Itsuing CAs certificates. The Tunisia Corporate CA is an intermediate CA which issue only: CRL OCSP certificate Itsuing CAs certificates.			
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)			4
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 SEL/TLS trust Bit) Revocation Tested NEED: Test with http://certificate.revocationcheck.com/ 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 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 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 Test Website Lint Test NEED: If EV treatment is being requested, then provide successful output from EV Testing Easy_Version Test Website Lint Test 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			4
Revocation Tested NEED: Test with http://certificate.revocationcheck.com/ 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 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 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 The Tunisia Corporate CA is an intermediate CA which issue only: CRL OCSP certificates Issuing CAs certificates.	Test notes	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	Issuing CAs certificates.
Revocation Tested NEED: Test with http://certificate.revocationcheck.com/ 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 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 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 The Tunisia Corporate CA is an intermediate CA which issue only: CRL OCSP certificates Issuing CAs certificates.	Test Results (When Reque	sting the SSL/TLS trust Bit)	
CA/Browser Forum Lint Test 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 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 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 OCSP certificate Issuing CAs certificates. Issuing CAs certificates.		NEED: Test with http://certificate.revocationcheck.com/	
Test certificates that violate any of the CA/Browser Forum 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 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 • Issuing CAs certificates.	CA/Browser Form Lint		1
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 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		certificates that violate any of the CA/Browser Forum	
https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version		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 NEED: If EV treatment is being requested, then	
	CA Hierarchy Information	https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	

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 internallyoperated; 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	The Tunisia Corporate CA is an intermediate CA. This CA issue two issuing CA: TnTrust Corporate CA: which issue these certificate profiles: OV SSL EV SSL OV Code Signing EV Code Signing VPN Timestamping TnTrust Qualified Corporate CA: Qualified signature Qualified Seal
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.	This CA has no subordinate CA certificates that are operated by external third parties.
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 crosssigning 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.	There are not any other root certificates for witch this root certificate has issued cross-signing certificates. There are not any other root certificates that have issued crosssigning certificates for this root certificate. There are not any crosssigning relationships.
Technical Constraint on 3 rd 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	Section 1.3.3 of the CP/CPS describes the technical and contractual controls over any 3rd party « Delegated Registration Authority (DRA) Delegated RAs have to abide by all the requirements of the TN PKI CP/CPS. DRAs may, however implement more restrictive practices based on their internal requirements. Any DRA operating under this CP/CPS must adhere to the following rules: • The DRA must have a contractual agreement with the National Digital Certification Agency which indicates the authorization for their role as RA and clearly details the minimum requirements, processes and liabilities. • The registration process of any DRA must be provided by the National Digital Certification Agency. The latter has to audit and approve the process as meeting the quality requirements of this CP/CPS and therefore being equivalent to the registration process of the TN PKI RA. • The DRA must have an annual audit. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit leads to the revocation of DRA privileges. » For the moment, the Tunisia National Root CA does not use external RAs. We have prepared a template of contract between NDCA and delegated RA.
Verification Policies and F	Practices	
Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	The CP/CPS is provided in English language.
CA Document Repository		http://www.certification.tn/pub/CPCPS-TunisianNationalPKI.pdf
CP Doc Language		English
CPS Doc Language		English
Other Relevant		The relying parties agreement are made in French language.
Documents		
Auditor Name		Mr. Philippe Bouchet from the certification body LSTI
Auditor Website		http://lsti-certification.fr
Auditor Qualifications		LSTI has been accredited pursuant to the accreditation certificate of French Accreditation Body COFRAC with registration number 5-0546 in accordance with NF EN ISO/IEC 17065:2013 as a certification body for products, processes, and services in accordance with the Annex of the accreditation certificate and the ETSI EN 319 403.
Standard Audit	NEED: Audit statements meeting the requirements of Mozilla's Root Store	

	Policy.	
Standard Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
Standard Audit Statement Date		21 march 2017
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	
BR Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
BR Audit Statement Date		21 march 2017
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	
EV SSL Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
EV SSL Audit Statement Date		21 march 2017
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.	Tunisian National Root CA conform to the current version of the CA/Browser Forum (CABF) requirements including: • Guidelines for the Issuance and Management of Extended Validation (EV) Certificates, • Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and, • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Published at www.cabforum.org. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_SelfAssessment) to the Bugzilla Bug.	I have attached the BR Self Assessment two months ago.
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.	Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name. • To validate the name of the organization, the requester provides official documentation about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information

provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FODN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form. In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization. NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain: • The FODN of the server to be used in the certificate: • The name and surname of the CHN: • The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; • Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", "Hostmaster", or postmaster "@ the name of the requested domain; • The General Conditions of Use (GTC) signed by the legal representative; • An official extract from the trade register of the organization dating no longer than three • A certificate of non-bankruptcy for private organizations. • The CSR for the public key to be signed. • A power of attorney for requests of certificates filed by an agent. EV SSL Verification NEED: If EV verification is performed, then provide URLs and section/page Section 3.2.2 of the CP/CPS Procedures number information pointing directly to the sections of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the documents that pertain to EV and describe the procedures for verifying issuing CAs of TN PKI may contain one instance of the organization field. Should the the ownership/control of the domain requester decide to make the organization field part of the DN, the following rules are name, and the verification of identity, existence, and authority of the adhered to: organization to request the EV certificate. The EV verification documentation • The use of the organization field means that the use of the country field is mandatory. must meet the requirements of the CA/Browser Forum's EV Guidelines. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of and must also provide information specific to the CA's operations. its name. • To validate the name of the organization, the requester provides official documentation about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FODN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with

handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FODN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form. In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization. NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain: • The FODN of the server to be used in the certificate; • The name and surname of the CHN; • The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; • Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", "Hostmaster", or postmaster "@ the name of the requested domain; • The General Conditions of Use (GTC) signed by the legal representative; • An official extract from the trade register of the organization dating no longer than three · A certificate of non-bankruptcy for private organizations. • The CSR for the public key to be signed. • A power of attorney for requests of certificates filed by an agent. Organization Verification NEED: CP/CPS sections that describe identity and organization Section 3.2.2 of the CP/CPS Procedures verification procedures for cert issuance. 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name. • To validate the name of the organization, the requester provides official documentation about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner. authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy

		of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form.
		In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain:
		 The FQDN of the server to be used in the certificate; The name and surname of the CHN; The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the name of the requested domain; The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three months; A certificate of non-bankruptcy for private organizations. The CSR for the public key to be signed. A power of attorney for requests of certificates filed by an agent.
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.	Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are adhered to: • The use of the organization field means that the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of its name.
		 To validate the name of the organization, the requester provides official documentation about the organization. The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to

		obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form.
		In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain:
		 The FQDN of the server to be used in the certificate; The name and surname of the CHN; The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the name of the requested domain; The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three months; A certificate of non-bankruptcy for private organizations. The CSR for the public key to be signed. A power of attorney for requests of certificates filed by an agent.
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	Yes. We need to activate Code Signing trust bit.
Multi-factor Authentication	NEED section number of the CP/CPS that states that multifactor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)	Section 5.2.2 of the CP/CPS 5.2.2 Number of persons required per task Two or more persons are required for TN PKI CAs for the following tasks: (a) CA key generation = Three (3) persons (b) CA signing key activation = Three (3) persons (c) CA private key backup = Three (3) persons Where multiparty control for logical access is required, at least one of the participants is an administrator. All participants must serve in a trusted role as defined in Section 5.2.1 (Trusted Roles). Multiparty control for logical access are not achieved using personnel that serve in the Auditor Trusted Role. HSM Administrators uses HSM Smartcards for authentication. The HSM itself enforces dual control based on the HSM smartcards for the different functions. The number of needed HSMsmartcards (m) of the total number of produced HSM-smartcards (n) will be: (a) Key generation = 3 of 6 (b) Signing key activation = 3 of 8 (c) Private key backup and restore = 3 of 6 End-user certificate issuance requires the approval of at least two persons. End-user Certificate revocation requires the approval of at least two persons. Registration and Customer Services: Responsible Employees responsible for routine

		certification services such as customer services, document control, processes relating to certificate registration, generation and revocation. These employees are trusted roles. They access the RA system using a smart card and a PIN code.
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	Section 6.8 of the CP/CPS: 6.8 Network security controls TN PKI's CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. TN PKI's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root and intermediate CAs Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. It is TN PKI's security policy to block all ports and protocols and open only necessary ports to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. All firewall configurations and changes thereto are documented, authorized, tested and implemented in accordance with change management procedures. TN PKI's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.
Root Case Record # 5		
Root Case Information		
Root Certificate Name	TnTrust Corporate CA	
Request Status	Initial Request Received	
Certificate Data		
Certificate Issuer Commun	TnTrust Corporate CA	
Name	1	
O From Issuer Field	National Digital Certification Agency	
OU From Issuer Field	<u> </u>	
Valid From	2016 Nov 29	
Valid To	2026 Nov 29	
Certificate Serial Number	1aecc618f3d38cd1	
Subject	CN = TnTrust Corporate CA, O = National Digital Certification Agency, L = T	Tunis, C = TN
Signature Hash Algorithm	Sha256WithRSAEncryption	
Public Key Algorithm	RSA 3072 bits	
SHA1 Fingerprint	20:7E:3A:5E:F4:39:A2:99:AD:28:D2:C3:5A:F2:AD:4B:46:A5:9E:12	
SHA-256 Fingerprint	E7:4C:45:28:58:B8:AD:40:E3:6E:EF:17:B1:9E:E7:1E:65:55:B3:1D:47:76:58:	E4:08:42:5C:D6:C8:E7:31:AF
Certificate Fingerprint	207e3a5ef439a299ad28d2c35af2ad4b46a59e12	
Certificate Version	3	
Technical Information abo		
Certificate Summary	Need Response From CA	The TnTrust Corporate CA is an issuing CA. This CA issue these profiles fo certificates: OV SSL EV SSL OV Code Signing EV Code Signing VPN Timestamping
Root Certificate Download URL	Need Response From CA	http://crl.certification.tn/tunisiacorporateca.crl
CRL URL(s)	Need Response From CA	http://crl.certification.tn/tntruscorporateca.crl
OCSP URL(s)	Need Response From CA	http://va.certification.tn
Mozilla Trust Bits	Need Response From CA	Emai, websites
SSL Validation Type	Need Response From CA	OV; EV
Mozilla EV Policy OID(s)	Need Response From CA	2.16.788.1.2.6.1.9.2.2
Root Stores Included In	Need Response From CA	The Tunisian National Root CA is not yet included in Microsoft root store. An application has been submitted and the CA is waiting for the response.

Mozilla Applied Constraints	Need Response From CA	No contraints		
Test Websites or Examp	Test Websites or Example Cert			
Test Website - valid	Need Response From CA	OV certificate: https://valid-corp-ov.certification.tn EV certificate: https://valid-corp-ev.certification.tn		
Test website Expired	Need Response From CA	OV certificate: https://expired-corp-ov.certification.tn EV certificate: https://expired-corp-ev.certification.tn		
Test website - revoked	Need Response From CA	OV certificate: https://revoked-corp-ov.certification.tn EV certificate: https://revoked-corp-ev.certification.tn		
Test notes	NEED: - If requesting Websites trust bit provide 3 URLs to 3 test v trust bit, then attach an example S/MIME cert to the bug.	websites (valid, expired, revoked) whose TLS/SSL cert chains up to this root If only requesting the Email		
Test results (When Requ	esting the SSL/TLS Trust Bit)			
Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	I have checked with the https://certificate.revocationcheck.com/ the URL of this web site: https://valid-corp-ev.certification.tn and there two inexpliquable errors:		
		http://crl.certification.tn/tunrootca.crl		
		CRL information Source: CRL Distribution Point listed in Certificate Location: http://crl.certification.tn/tunrootca.crl Size: 750 bytes (DER data) Response time: 342.854827ms This update: Nov 8, 2017 11:37:03 AM Next update: Nov 8, 2018 11:37:03 AM Revoked: No Revoked certificates in CRL: 0 Relevant server response headers Date: Nov 20, 2017 2:32:35 PM Last Modified: Nov 8, 2017 1:47:02 PM Expires: Jan 1, 1 1:00:00 AM Server and network information Server Software: Apache Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)' This CRL file is DER encoded Response is already valid Response is not expired		
		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 a root CA CRL which have a validity of 365 days as mentioned in the CABForum Base line requirements section 4.9.7 CRL Issuance Frequency: « For the status of Subordinate CA Certificates:		
		The CA SHALL update and reissue CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field MUST NOT be more than twelve months beyond the value of		

	1	
		the thisUpdate field.»
		http://crl.certification.tn/tunisiacorporateca.crl
		CRL information Source: CRL Distribution Point listed in Certificate Location: http://crl.certification.tn/tunisiacorporateca.crl Size: 746 bytes (DER data) Response time: 325.925883ms This update: Nov 8, 2017 11:39:57 AM Next update: Nov 8, 2018 11:39:57 AM Revoked: No Revoked certificates in CRL: 0
		Relevant server response headers Date: Nov 20, 2017 2:32:35 PM Last Modified: Nov 8, 2017 1:46:59 PM Expires: Jan 1, 1 1:00:00 AM
		Server and network information Server Software: Apache
		Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)' This CDN Claim DEP.
		• This CRL file is DER encoded
		Response is already valid Response is not expired
		 Response is not expired 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 an intermediate CA CRL which have a validity of 365 days as mentioned in the CABForum Base line requirements section 4.9.7 CRL Issuance Frequency: « For the status of Subordinate CA Certificates:
		The CA SHALL update and reissue CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field MUST NOT be more than twelve months beyond the value of the thisUpdate field. »
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	I checked that the TnTrust Corporate CA does not issue certificates that violate any of the CA/Browser Forum.
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	I checked that TnTrust Corporate CA does not issue certificates that violate any of the X.509 rules.
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 checked the URL https://tls-observatory.services.mozilla.com/static/ev-checker.html with these parameters:
		TLS Server : https://valid-corp-ev.certification.tn

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 Mozilla's Root Store Policy party « Delegated Registration Authority (DRA) Delegated RAs have to abide by all the requirements of the TN PKI CP/CPS. DRAs may, however implement more restrictive practices based on their internal requirements. Any DRA operating under this CP/CPS mu adhere to the following rules: The DRA must have a contractual agreement with the National Digital Certification Agency which indicates the authorization for their role as RA and clearly details the minimum requirements, processes and liabilities. The registration process of any DRA must be provided by the National Digital Certification Agency. The latter has to audit and approve the process as meeting the qualit requirements of this CP/CPS and therefore being equivalent to the registration process of the TN PKI RA. The DRA must have an annual audit. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit leads to the revocation of DRA privileges. » For the moment, the Tunisia National Root CA does not use external RAs. We have			
## CA Hierarchy Information CA Hierarchy Information CA Hierarchy Information CA Hierarchy Information WiED A description of the PK hierarchy rooted at or otherwise associated with the root closes of the property which of the subordinate CAs retain care large			EV Policy OID : 2.16.788.1.2.6.1.9.2.2
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 that are signed by this root. Identify which of the subordinate CAs retented to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified ecrificates, EV extificates vs. email certificates, large extinct that certificates, but his case note that we do not require that the CA submit a complete customer list; other we are interested in the general rulps and nature of the third party armagements Externally Operated SubCAs NEED: If this root bas any subordinate CA certificates we made that the CA submit a complete customer list; other we are interested in the general rulps and nature of the third party armagements NEED: If this root bas any subordinate CA certificates that are operated by external third parties, the provide the information listed in the Subordinate 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. Cross Signing NEED: Als all other root certificates that have issued crosssigning certificates in the sissued crosssigning certificates in the sissued crosssigning certificates are already included in the Mobilar root store or not. Technical Constraint on Significant to the sissued crosssigning certificates we already included in the Mobilar root store or not. Technical Constraint on Significant that have issued crosssigning certificates are already included in the Mobilar root store or not. Technical Constraint on Significant the CA benefit of the CABrowser Forum's Baseline Requirements - Mozilla's Root Store Policy The registration process of any DRA must be provided by the National Digital Certificates we already included in the			« ev-checker reported failure: ev-checker did not exit successfully. exit status 1, Stderr: GetFirstEVPolicyForCert failed: SEC_ERROR_EXTENSION_NOT_FOUND This may
CA Hierarchy Information CA Hierarchy NEED: A description of the PKI hierarchy noted at or otherwise associated with this root CA certificate. - List and/ord secrebs to the general public: Class 1 vs. class 2 certificates, gualified vs. non-guiletion desponding CAs trace to the general public: Class 1 vs. class 2 certificates, gualified vs. non-guiletide derificates, EV certificates, and so on. – It might also include subordinate CAs to more than the CAs and a complete customer into 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 subCAs Externally Operated SubCAs Externally Operated SubCAs NEED: A description of the PKI hierarchy noted at or other charges in the season of 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 in the vertical parties, then provide the information listed in the Subordinate CA. Checklist, https://wide.morall.no.gr/CAs/booklist, https://wide.morall.no.gr/CAs/booklist, https://wide.morall.no.gr/CAs/booklist, https://wide.morall.no.gr/CAs/booklist.pdf.CA checklist.pdf.pdf.case.p			
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 created to size different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified extritionates, PC over flower insight include subordinate CAs certificates vs. non-PC vertificates, such as a certificate, such as a constitution of 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 rulps and nature of the third party armagements NEED: If this root has any subordinate CA certificates vs. email certificates (Acklest) of the CA functions as a super CA such there CA policies and auditing don't apply to the subordinate CAs, tent has super case that are operated by external third parties, then provide the information listed in the Subordinate CA. Checklist, https://wki.kmozilla.org/CASbordinate CA, Checklist - If the CA functions as a super CA such there CA policies and auditing don't apply to the subordinate CAs, tent has super don't case and submit and the subordinate CAs must apply for inclusion themselves as separate trust anchors. NEED: List all other root certificates for which this root certificates for which this root certificates for which this root certificates is a super CA such there CA policies and auditing don't apply to the subordinate CAs, tent thouse subordinate CAs must apply for inclusion themselves as separate trust anchors. NEED: List all other root certificates for which this root certificates that have issued crosssigning certificates for his root certificates for which this root certificates for which the crossing in case of the province of	CA Hierarchy Information)n	,
list, rather we are interested in the general type and nature of the third party arrangements	CA Hierarchy	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	profiles:
Cross Signing Cross Signing NEED: List all other root certificates for which this root certificate has issued crosssigning certificates for this root certificate. If may such crosssigning certificates for this root certificate that have issued crosssigning certificates for this root certificates for which this root certificates for this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates. There are not any other root certificates for witch this root certificates for witch this root cer	· 1	list; rather we are interested in the general type and nature of the third-party arrangements NEED: ¬ If this root has any subordinate CA certificates that are operated by	This CA has no subordinate CA certificates that are operated by external third parties.
certificate has issued crosssigning certificates List all other root certificates that have issued crosssigning certificates for this root certificate. If any such crosssigning relationships exist, it is important to note whether the crosssigning CAs' certificates are already included in the Mozilla root store or not. 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 Mozilla's Root Store Policy Agency which indicates the authorization for their role as RA and clearly details the minimum requirements, or the TN PKI RA. There are not any other root certificates that have issued crosssigning certificates. There are not any crosssigning relationships. Section 1.3.3 of the CP/CPS describes 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 Mozilla's Root Store Policy The registration Authority (DRA) Delegated RAs have to abide by all the requirements of the TN PKI CP/CPS. DRAs may, however implement more restrictive practices based on their internal requirements. Any DRA operating under this CP/CPS mu adhere to the following rules: There are not any crosssigning relationships. There are not any crosssigning relationships. Section 1.3.3 of the CP/CPS describes the technical and contractual controls over any 3rd party who may issue certs in this CP/CPS under the requirements. Any DRA operating under this CP/CPS mu adhere to the following rules: The DRA must have a contractual agreement with the National Digital Certification Agency. The latter has to audit and approve the process of any DRA must be provided by t	SubCAs	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	
NEED: CP/CPS documentation describing the technical and contractual controls over any 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 Nozilla's Policy Root Root National And Contrac	Cross Signing	certificate has issued crosssigning certificates List all other root certificates that have issued crosssigning certificates for this root certificate. If any such cross- signing relationships exist, it is important to note whether the crosssigning CAs'	signing certificates. There are not any other root certificates that have issued crosssigning certificates for this root certificate.
	3 rd 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	requirements of the TN PKI CP/CPS. DRAs may, however implement more restrictive practices based on their internal requirements. Any DRA operating under this CP/CPS must adhere to the following rules: • The DRA must have a contractual agreement with the National Digital Certification Agency which indicates the authorization for their role as RA and clearly details the minimum requirements, processes and liabilities. • The registration process of any DRA must be provided by the National Digital Certification Agency. The latter has to audit and approve the process as meeting the quality requirements of this CP/CPS and therefore being equivalent to the registration process of the TN PKI RA. • The DRA must have an annual audit. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit leads to the revocation of DRA privileges. »
Verification Policies and Pratices			
Policy Documentation NEED: Languages that the CP/CPS and other documents are provided in. The CP/CPS is provided in English language.	Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	The CP/CPS is provided in English language.

CA Document Repository		http://www.certification.tn/pub/CPCPS-TunisianNationalPKI.pdf
CP Doc Language		English
CPS Doc Language		English
Other Relevant		The relying parties agreement are made in French language.
Documents		The retying parties agreement are made in French language.
Auditor Name		Mr. Philippe Bouchet from the certification body LSTI
Auditor Website		http://lsti-certification.fr
Auditor Qualifications		LSTI has been accredited pursuant to the accreditation certificate of French Accreditation
Auditor Qualifications		Body COFRAC with registration number 5-0546 in accordance with NF EN ISO/IEC 17065:2013 as a certification body for products, processes, and services in accordance with the Annex of the accreditation certificate and the ETSI EN 319 403.
Standard Audit	NEED: Audit statements meeting the requirements of Mozilla's Root Store Policy.	
Standard Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
Standard Audit Statement Date		21 march 2017
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as per Mozilla's Root Store Policy.	
BR Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
BR Audit Statement Date		21 march 2017
EV SSL Audit	NEED: If requesting EV treatment, then also need an EV audit as per Mozilla's Root Store Policy.	
EV SSL Audit Type		EN 319 411 -1 V1.1.1: Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements EN 319 411-2 V2.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificate
EV SSL Audit Statement Date		21 march 2017
BR Commitment to	NEED: If requesting Websites trust bit, need section in the CP/CPS that	Tunisian National Root CA conform to the current version of the CA/Browser Forum
Comply	has the commitment to comply with the BRs as described in section 2.2 of the CA/Browser Forum's Baseline Requirements.	(CABF) requirements including: • Guidelines for the Issuance and Management of Extended Validation (EV) Certificates, • Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and, • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Published at www.cabforum.org. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_SelfAssessment) to the Bugzilla Bug.	I have attached the BR Self Assessment two months ago.
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.	Section 3.2.2 of the CP/CPS 3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules are

	Each decommented and advantage of a suld atotal sulfills and a sulfill a sulfill and a sulfill and a sulfill a sulfill and a sul	adhanad to
	Each documented procedure should state which subsection of BR section	adhered to:
	3.2.2.4 it is complying with.	• The use of the organization field means that the use of the country field is mandatory.
		• The registration process of any registration authority operating under this CP/CPS
		contains provisions to determine the identity of an organization and to authorize the use of
		its name.
		• To validate the name of the organization, the requester provides official documentation
		about the organization.
		• The use of the organization's name is authorized by one or more legal representatives of
		the organization, and handwritten personal signatures is included on the registration form.
		The use of a domain name in a FQDN is authorized by the domain owner or its
		representatives. The domain owner may be determined through the WHOIS information
		provided by the domain registrar. Should an organization be listed as the domain owner,
		authorization is given by one or more legal representatives of the organization with
		handwritten personal signatures on the registration form. Should an individual be listed as
		the owner, this individual personally signs the registration form. The RA will create a copy
		of all required supporting documentation. Alternatively and only if an organization name is
		present in the certificate subject, domain validation according to section 3.1 may be used to
		obtain authorization of the use of the domain name in a FQDN. In this case the handwritten
		signatures of the authorization of the organizational name are the only authorization
		signatures required on the registration form.
		In addition, the TN PKI RA:
		• Determines that the Organization exists by using at least one third party identity proofing
		service or database, or alternatively, organizational documentation issued by or filed with
		the applicable government that confirms the existence of the organization, and
		• Uses information contained in the business records or databases of business information
		(employee or customer directories) of an RA approving certificates to its own affiliated
		individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to
		the organization, the employment with the Organization of the individual submitting the
		Certificate Application and, when appropriate, his/her authority to act on behalf of the
		Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating
		the Applicant's ownership or control of the domain:
		• The FQDN of the server to be used in the certificate;
		• The name and surname of the CHN;
		• The personal identification data of the RCS as well as the legal representative including a
		valid official document of identity, including a photograph of identity;
		Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a
		minimum, an e-mail address as contained in the WHOIS must be used. If this is not the
		case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or
		in the form "admin", "administrator", "webmaster", "Hostmaster ", or" postmaster "@ the
		name of the requested domain;
		• The General Conditions of Use (GTC) signed by the legal representative;
		• An official extract from the trade register of the organization dating no longer than three
		months;
		A certificate of non-bankruptcy for private organizations.
		• The CSR for the public key to be signed.
		A power of attorney for requests of certificates filed by an agent.
EV SSL Verification	NEED: If EV verification is performed, then provide URLs and section/page	Section 3.2.2 of the CP/CPS
Procedures	number information pointing directly to the sections of the CP/CPS	3.2.2 Authentication of organization identity The DN of a certificate issued by one of the
	documents that pertain to EV and describe the procedures for verifying	issuing CAs of TN PKI may contain one instance of the organization field. Should the
	the ownership/control of the domain	requester decide to make the organization field part of the DN, the following rules are
	name, and the verification of identity, existence, and authority of the	adhered to:
	organization to request the EV certificate. The EV verification documentation	• The use of the organization field means that the use of the country field is mandatory.
	organization to request the E v certificate. The E v verification documentation	The use of the organization field means that the use of the country field is mandatory.

		The middle of the control of the con
	must meet the requirements of the CA/Browser Forum's EV Guidelines,	• The registration process of any registration authority operating under this CP/CPS contains provisions to determine the identity of an organization and to authorize the use of
	and must also provide information specific to the CA's operations.	its name.
		To validate the name of the organization, the requester provides official documentation
		about the organization.
		The use of the organization's name is authorized by one or more legal representatives of
		the organization, and handwritten personal signatures is included on the registration form.
		• The use of a domain name in a FQDN is authorized by the domain owner or its
		representatives. The domain owner may be determined through the WHOIS information
		provided by the domain registrar. Should an organization be listed as the domain owner,
		authorization is given by one or more legal representatives of the organization with
		handwritten personal signatures on the registration form. Should an individual be listed as
		the owner, this individual personally signs the registration form. The RA will create a copy
		of all required supporting documentation. Alternatively and only if an organization name is
		present in the certificate subject, domain validation according to section 3.1 may be used to
		obtain authorization of the use of the domain name in a FQDN. In this case the handwritten
		signatures of the authorization of the organizational name are the only authorization
		signatures required on the registration form.
		In addition, the TN PKI RA:
		• Determines that the Organization exists by using at least one third party identity proofing
		service or database, or alternatively, organizational documentation issued by or filed with
		the applicable government that confirms the existence of the organization, and
		• Uses information contained in the business records or databases of business information
		(employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to
		the organization, the employment with the Organization of the individual submitting the
		Certificate Application and, when appropriate, his/her authority to act on behalf of the
		Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating
		the Applicant's ownership or control of the domain:
		The EODN of the compants he wood in the contificate.
		 The FQDN of the server to be used in the certificate; The name and surname of the CHN;
		• The personal identification data of the RCS as well as the legal representative including a
		valid official document of identity, including a photograph of identity;
		• Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a
		minimum, an e-mail address as contained in the WHOIS must be used. If this is not the
		case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or
		in the form "admin", "administrator", "webmaster", " Hostmaster ", or" postmaster "@ the
		name of the requested domain;
		 The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three
		• An official extract from the trade register of the organization dating no longer than three months;
		• A certificate of non-bankruptcy for private organizations.
		• The CSR for the public key to be signed.
		A power of attorney for requests of certificates filed by an agent.
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization	Section 3.2.2 of the CP/CPS
	verification procedures for cert issuance.	3.2.2 Authentication of organization identity The DN of a certificate issued by one of the
		issuing CAs of TN PKI may contain one instance of the organization field. Should the
		requester decide to make the organization field part of the DN, the following rules are adhered to:
		• The use of the organization field means that the use of the country field is mandatory.
		• The use of the organization field file and the use of the country field is mandatory. • The registration process of any registration authority operating under this CP/CPS
		contains provisions to determine the identity of an organization and to authorize the use of
L	J	1

		,
		its name. • To validate the name of the organization, the requester provides official documentation
		about the organization.
		• The use of the organization's name is authorized by one or more legal representatives of
		the organization, and handwritten personal signatures is included on the registration form.
		• The use of a domain name in a FQDN is authorized by the domain owner or its
		representatives. The domain owner may be determined through the WHOIS information
		provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with
		handwritten personal signatures on the registration form. Should an individual be listed as
		the owner, this individual personally signs the registration form. The RA will create a copy
		of all required supporting documentation. Alternatively and only if an organization name is
		present in the certificate subject, domain validation according to section 3.1 may be used to
		obtain authorization of the use of the domain name in a FQDN. In this case the handwritten
		signatures of the authorization of the organizational name are the only authorization
		signatures required on the registration form.
		In addition, the TN PKI RA:
		Determines that the Organization exists by using at least one third party identity proofing
		service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and
		Uses information contained in the business records or databases of business information
		(employee or customer directories) of an RA approving certificates to its own affiliated
		individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to
		the organization, the employment with the Organization of the individual submitting the
		Certificate Application and, when appropriate, his/her authority to act on behalf of the
		Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating
		the Applicant's ownership or control of the domain:
		The FQDN of the server to be used in the certificate;
		• The name and surname of the CHN;
		• The personal identification data of the RCS as well as the legal representative including a
		valid official document of identity, including a photograph of identity; • Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a
		minimum, an e-mail address as contained in the WHOIS must be used. If this is not the
		case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or
		in the form "admin", "administrator", "webmaster", " Hostmaster ", or" postmaster "@ the
		name of the requested domain;
		The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three
		• An official extract from the trade register of the organization dating no longer than three months;
		A certificate of non-bankruptcy for private organizations.
		• The CSR for the public key to be signed.
		A power of attorney for requests of certificates filed by an agent.
Email Address	NEED if Email trust bit requested Sections of CP/CPS that sufficiently	Section 3.2.2 of the CP/CPS
Verification Procedures	describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert.	3.2.2 Authentication of organization identity The DN of a certificate issued by one of the issuing CAs of TN PKI may contain one instance of the organization field. Should the
	ownership/control of the chian address to be included in the cert.	requester decide to make the organization field part of the DN, the following rules are
		adhered to:
		• The use of the organization field means that the use of the country field is mandatory.
		• The registration process of any registration authority operating under this CP/CPS
		contains provisions to determine the identity of an organization and to authorize the use of
		its name. • To validate the name of the organization, the requester provides official documentation
		• 10 varidate the name of the organization, the requester provides official documentation

		about the organization. • The use of the organization's name is authorized by one or more legal representatives of the organization, and handwritten personal signatures is included on the registration form. • The use of a domain name in a FQDN is authorized by the domain owner or its representatives. The domain owner may be determined through the WHOIS information provided by the domain registrar. Should an organization be listed as the domain owner, authorization is given by one or more legal representatives of the organization with handwritten personal signatures on the registration form. Should an individual be listed as the owner, this individual personally signs the registration form. The RA will create a copy of all required supporting documentation. Alternatively and only if an organization name is present in the certificate subject, domain validation according to section 3.1 may be used to obtain authorization of the use of the domain name in a FQDN. In this case the handwritten signatures of the authorization of the organizational name are the only authorization signatures required on the registration form.
		In addition, the TN PKI RA: • Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and • Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.
		NDCA have also internal procedures that are guidelines for the operators to for validating the Applicant's ownership or control of the domain:
Code Signing Subscriber	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	 The FQDN of the server to be used in the certificate; The name and surname of the CHN; The personal identification data of the RCS as well as the legal representative including a valid official document of identity, including a photograph of identity; Information enabling the RA to contact the RCS (telephone number, e-mail, etc.). At a minimum, an e-mail address as contained in the WHOIS must be used. If this is not the case, then the e-mail address must be confirmed from the e-mail address in the WHOIS or in the form "admin", "administrator", "webmaster", " Hostmaster ", or" postmaster "@ the name of the requested domain; The General Conditions of Use (GTC) signed by the legal representative; An official extract from the trade register of the organization dating no longer than three months; A certificate of non-bankruptcy for private organizations. The CSR for the public key to be signed. A power of attorney for requests of certificates filed by an agent. Yes. We need to activate Code Signing trust bit.
Verification Pro		
Multi-factor Authentication	NEED section number of the CP/CPS that states that multifactor authentication is enforced for all accounts capable of directly causing certificate issuance. (reference section 6.5 of the BRs)	Section 5.2.2 of the CP/CPS 5.2.2 Number of persons required per task Two or more persons are required for TN PKI CAs for the following tasks: (a) CA key generation = Three (3) persons (b) CA signing key activation = Three (3) persons (c) CA private key backup = Three (3) persons Where multiparty control for logical access is required, at least one of the participants is an administrator. All participants must serve in a trusted role as defined in Section 5.2.1 (Trusted Roles). Multiparty control for logical access are not achieved using personnel that serve in the

		Auditor Trusted Role. HSM Administrators uses HSM Smartcards for authentication. The HSM itself enforces dual control based on the HSM smartcards for the different functions. The number of needed HSMsmartcards (m) of the total number of produced HSM-smartcards (n) will be: (a) Key generation = 3 of 6 (b) Signing key activation = 3 of 8 (c) Private key backup and restore = 3 of 6 End-user certificate issuance requires the approval of at least two persons. End-user Certificate revocation requires the approval of at least two persons. Registration and Customer Services: Responsible Employees responsible for
N. I.G. S	NEED 4: 1 () 64 GP/GPG 1 I: 4 N 4 1 G	routine certification services such as customer services, document control, processes relating to certificate registration, generation and revocation. These employees are trusted roles. They access the RA system using a smart card and a PIN code.
Network Security	NEED section number(s) of the CP/CPS dealing with Network Security.	Section 6.8 of the CP/CPS: 6.8 Network security controls TN PKI's CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. TN PKI's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root and intermediate CAs Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. It is TN PKI's security policy to block all ports and protocols and open only necessary ports to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. All firewall configurations and changes thereto are documented, authorized, tested and implemented in accordance with change management procedures. TN PKI's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.