Diffusion

Function	For application	For information
CEO		*
Steering comity of Integrated Management System		*
TunTrust Board of Directors		*
Pilot of the process GAC	*	
Pilot of the process GAE		*
PKI Management Service	*	
Risk Analysis and Audit Unit		*

Review

Version	Date	Comment	Page
Version 00	20/02/2017	1st Writing	Whole document
Version 01	31/08/2018	2nd Writing	Whole document
Version 02	14/09/2018	3rd Writing	Sections Timestamp request format and Timestamp response format

Document Approval

	Author	Validated by	Approved by
Entity :	Tuntrust	Steering comity of Integrated Management System	TunTrust Board of Directors
Date :	10 September 2018	13 Septembre 2018	14 September 2018

A. Introduction

TunTrust is a certification authority (CA) that issues digital certificates in accordance with its CP/CPS published in the website http://www.tuntrust.tn/repository. As a CA, TunTrust performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

TunTrust is also a time stamping authority (TSA) and provides proof-of-existence for data at an instant in time as described in the TP/TPS published in the website http://www.tuntrust.tn/repository.

B. TunTrust CAs Hierarchies

TunTrust, acting as CSP is using several Certification Authorities (CAs), as shown in the certificates hierarchy, to issue TunTrust end-users certificates:

- Two level CA hierarchy (figure 1) to issue OV SSL Certificate
- Three level CA hierarchy (figure 2) to issue OV SSL Certificate, Digital Signature Certificate and e-Seal Certificate.
- One level CA hierarchy (figure 3) to issue visible digital seal certificate.

1. Tunisian Root Certificate Authority – TunRootCA2

The first TunTrust CA hiearachy consists of the following CAs (see figure 1):

- One TunRootCA2 self-signed root and kept offline.
- One issuing CA: TunServerCA2 root-signed by ***TunRootCA2*** and operates online to issue OV SSL certificates.

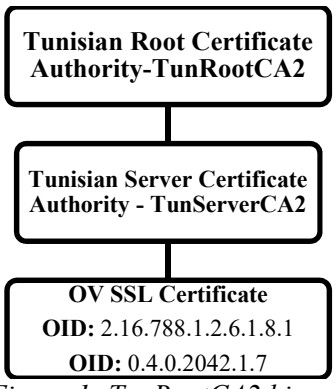

Figure 1- TunRootCA2 hierarchy

2. Tunisia National Root CA

The second TunTrust CA hiearachy consists of the following CAs (see figure 1):

- One Tunisia National Root CA self-signed root and kept offline.

- Two intermediate CAs:
  - Tunisia Gov CA: is a root-signed Tunisia National Root CA and kept offline.
  - Tunisia Corporate CA: is a root-signed Tunisia National Root CA and is revoked on August, 08 2018.
- Four Issuing CAs:
  - TnTrust Gov CA: is a root-signed by Tunisia Gov CA and operates online to issue OV SSL Certificate and LCP certificate
  - TnTrust Qualified Gov CA: : is a root-signed by Tunisia Gov CA and operates online to issue QCP-n-qscd and QCP-l-qscd certificates
  - TnTrust Corporate CA: is a root-signed by Tunisia Corporate CA and is revoked on August, 08 2018.
  - TnTrust Qualified Corporate CA: is a root-signed by Tunisia Corporate CA and is revoked on August, 08 2018.

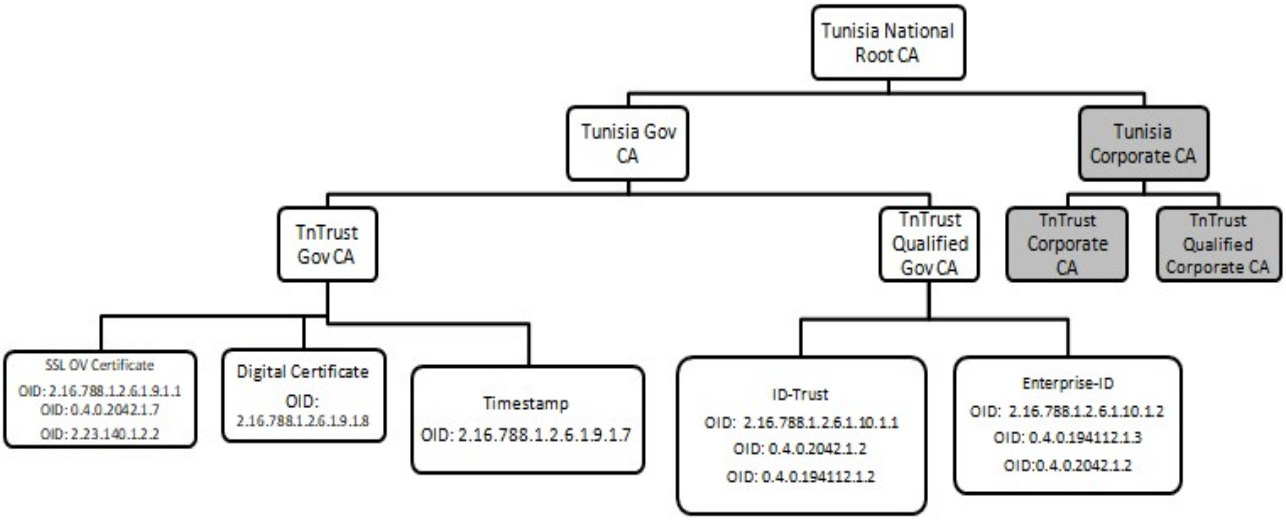

Figure -2 Tunisia National Root CA hierarchy

3. TN01

TunTrust offers a Visible Digital Seal to ensure the authenticity of certain types of documents as well as the integrity and conformity of the copies made compared to their original version.

In this respect, TunTrust issue e-seal certificates that comply with the technical requirements of the 2D-DOC standard v 3.0.0.

The CA is a self-signed root CA that delivers the e-seal certificates directly.

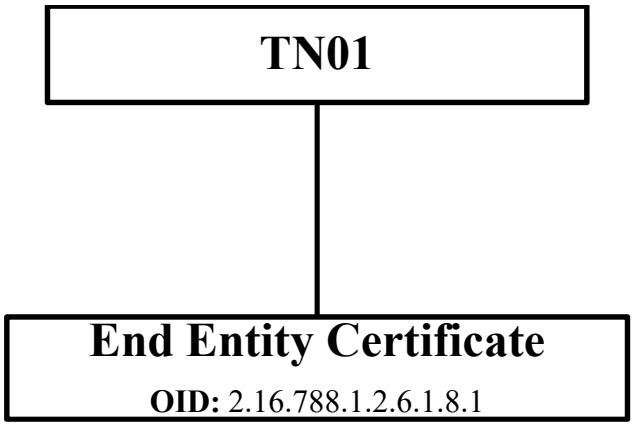

Figure 3- 2DDOC CA hierarchy

C. Certificates Authorities Profiles

4. Tunisian Root Certificate Authority - TunRootCA2

The following table describes the TunRootCA2 certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		2166150505270505BC8AB01DAF0ABEC4
Signature Algorithm			
Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		O = National Digital Certification Agency, CN = Tunisian Root Certificate Authority - TunRootCA2, C=TN
Subject DN	X		O = National Digital Certification Agency, CN = Tunisian Root Certificate Authority - TunRootCA2, C=TN
Validity	X		
Not Before	X		5 May 2015 09:57:01
Not After	X		5 May 2027 09:57:01

SubjectPublicKeyInfo	X		Public Key: Key length: 4096 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
X509v3 Subject Key Identifier	X		CC:73:C5:A3:6A:29:31:97:A7:8D:A0:D8:54 :C1:0A:75:B6:23:3F:A6
X509v3 Basic Constraints	X	True	CA:TRUE
KeyUsage	X	True	
Certificate Sign			Set
CRL Sign			Set

5. Tunisian Server Certificate Authority - TunServerCA2

The following table describes TunServerCA2 certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		216615050625050514681E592CF41849
Signature Algorithm			
Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		O = National Digital Certification Agency, CN = Tunisian Root Certificate Authority - TunRootCA2, C=TN
Subject DN	X		CN = Tunisian Server Certificate Authority - TunServerCA2, O = National Digital Certification Agency, C = TN
Validity			
Not Before	X		7 May 2015 01:00:00
Not After	X		8 May 2025 00:59:59
SubjectPublicKeyInfo	X		Public Key: Key length: 4096 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
Authority Information Access	X		OCSP - URI:http://ocsp.certification.tn CA Issuers - URI: http://www.certification.tn/pub/TunRootCA2.crt
X509v3 Subject Key Identifier	X		87:AB:F7:69:4B:50:F6:61:57:FF:3F:5B:8E:1D:70:C6:A2:6C:AA:C6
X509v3 Basic Constraints	X	True	CA:TRUE pathlen:0
X509v3 Authority Key Identifier	X		CC:73:C5:A3:6A:29:31:97:A7:8D:A0:D8:54:C1:0A:75:B6:23:3F:A6
X509v3 CRL Distribution Points	X		URI:http://crl.certification.tn/TunRootCA2.crl
Key Usage	X	True	
Certificate Sign			Set
CRL Sign			Set

X509v3 Certificate Policies	X		Policy: 2.16.788.1.2.6.1.8.1 CPS: https://www.certification.tn/cps User Notice: Organization: National Digital Certification Agency Number: 1 Explicit Text: https://www.certification.tn/rpa

6. Tunisia National Root CA

The following table describes the Tunisia National Root CA Certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		68:3E:11:55:92:9C:8E:8E
Signature Algorithm			
Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia National Root CA
Subject DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia National Root CA
Validity	**X**		
Not Before	X		Nov 29 09:02:56 2016 GMT
Not After	X		May 29 09:02:56 2037 GMT
SubjectPublicKeyInfo	X		Public Key: Key length: 4096 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
Authority Information Access	X		OCSP - URI:http://va.certification.tn
X509v3 Subject Key Identifier	X		0E:BE:D1:48:44:12:52:23:2B:47:14:FA:5F:A8:7E:1C:6F:14:08:8E
X509v3Authority Key Identifier	X		0E:BE:D1:48:44:12:52:23:2B:47:14:FA:5F:A8:7E:1C:6F:14:08:8E
X509v3 Private Key Usage Period	X		Not Before: Nov 29 09:02:56 2016 GMT, Not After: May 29 09:02:56 2037 GMT
X509v3 CRL Distribution Points	X		URI:http://crl.certification.tn/tunrootca.crl
X509v3 Basic Constraints	X	True	CA:TRUE
X509v3 Key Usage	**X**	**True**	
Digital Signature			Set
Certificate Sign			Set
CRL Sign			Set

7. Tunisia Gov CA

The following table describes the Tunisia Gov CA certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		78:2C:10:09:83:0A:4B:EE
Signature Algorithm			
Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia National Root CA
Subject DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Gov CA
Validity	**X**		
Not Before	X		Nov 29 09:35:15 2016 GMT
Not After	X		Feb 29 09:35:15 2032 GMT
SubjectPublicKeyInfo	X		Public Key: Key length: 4096 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
Authority Information Access	X		OCSP - URI:http://va.certification.tn
X509v3 Subject Key Identifier	X		AF:81:94:4C:7B:36:7A:6D:F8:9B:12:94:55:9C :42:D3:B7:B8:B9:46
X509v3Authority Key Identifier	X		0E:BE:D1:48:44:12:52:23:2B:47:14:FA:5F:A8 :7E:1C:6F:14:08:8E
X509v3 Private Key Usage Period	X		Not Before: Nov 29 09:35:15 2016 GMT, Not After: Feb 29 09:35:15 2032 GMT
X509v3 Certificate Policies	X		Policy: 2.16.788.1.2.6.1.9
X509v3 CRL Distribution Points	X		URI:http://crl.certification.tn/tunrootca.crl
X509v3 Basic Constraints	X	True	CA:TRUE
Key Usage	**X**	**True**	

Digital Signature			Set
Certificate Sign			Set
CRL Sign			Set

8. TnTrust Gov CA

The following table describes the TnTrust Gov CA certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		36:71:6F:A4:36:EC:C2:D2
Signature Algorithm			
Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Gov CA
Subject DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Gov CA
Validity	**X**		
Not Before	X		Nov 29 10:47:01 2016 GMT
Not After	X		Dec 29 10:47:01 2026 GMT
SubjectPublicKeyInfo	X		Public Key: Key length: 3072 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
Authority Information Access	X		OCSP - URI:http://va.certification.tn
X509v3 Subject Key Identifier	X		7B:D6:C4:15:45:CF:06:34:95:69:36:86:DA:75:7D:9B:FB:EB:73:D9
X509v3Authority Key Identifier	X		AF:81:94:4C:7B:36:7A:6D:F8:9B:12:94:55:9C:42:D3:B7:B8:B9:46
X509v3 Private Key Usage Period	X		Not Before: Nov 29 10:47:01 2016 GMT, Not After: Dec 29 10:47:01 2026 GMT
X509v3 Certificate Policies	X		Policy: 2.16.788.1.2.6.1.9
X509v3 CRL Distribution Points	X		URI:http://crl.certification.tn/tunisiagovca.crl

X509v3 Basic Constraints	X	True	CA:TRUE Pathlen : 0
Key Usage	X	True	
Digital Signature			Set
Certificate Sign			Set
CRL Sign			Set

9. TnTrust Qualified Gov CA

The following table describes the TnTrust Qualified Gov CA certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		
Signature Algorithm			
Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Gov CA
Subject DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Qualified Gov CA
Validity	**X**		
Not Before	X		Nov 29 10:24:02 2016 GMT
Not After	X		Dec 29 10:24:02 2026 GMT
SubjectPublicKeyInfo	X		Public Key: Key length: 3072 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
Authority Information Access	X		OCSP - URI:http://va.certification.tn
X509v3 Subject Key Identifier	X		73:24:28:25:FA:22:F6:92:A9:15:83:A4:2C:B3:C D:C6:CB:B4:03:56

X509v3Authority Key Identifier	X		AF:81:94:4C:7B:36:7A:6D:F8:9B:12:94:55:9C:42:D3:B7:B8:B9:46
X509v3 Private Key Usage Period	X		Not Before: Nov 29 10:24:02 2016 GMT, Not After: Dec 29 10:24:02 2026 GMT
X509v3 Certificate Policies	X		Policy: 2.16.788.1.2.6.1.10
X509v3 CRL Distribution Points	X		URI:http://crl.certification.tn/tunisiagovca.crl
X509v3 Basic Constraints	X	True	CA:TRUE Pathlen : 0
Key Usage	**X**	**True**	
Digital Signature			Set
Certificate Sign			Set
CRL Sign			Set

10. TN01

The following table describes the TN01 CEV CA certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		6A:B8:26:4E:06:82:56:97
Signature Algorithm			
Algorithm	X		ecdsa-with-SHA256
Signature Value	X		CA Signature
Issuer DN	X		CN=TN01, OU=TN CEV CA, O=National Digital Certification Agency, C=TN
Subject DN	X		CN=TN01, OU=TN CEV CA, O=National Digital Certification Agency, C=TN
Validity	**X**		
Not Before	X		Apr 27 12:52:57 2017 GMT
Not After	X		Apr 27 12:52:57 2027 GMT
ASN1 OID	X		secp384r1

X509v3 extensions			
X509v3 Subject Key Identifier	X		CE:87:48:48:A9:2F:A8:F5:B6:CB:F7:97:B5:F7:02:91:D2:8A:9C:58
X509v3Authority Key Identifier	X		CE:87:48:48:A9:2F:A8:F5:B6:CB:F7:97:B5:F7:02:91:D2:8A:9C:58
X509v3 Basic Constraints	X	True	CA:TRUE
Key Usage	X	True	
Digital Signature			Set
Certificate Sign			Set
CRL Sign			Set

D. TunServerCA2 End-Entity Certificates Profiles

The following type of Certificates is issued under TunServerCA2 CA:

1. OV SSL Certificates

TunTrust OV SSL Server Certificates are ETSI EN 319 411-1 Certificates not certified as generated on QSCD, with creation of the keys by the Subscriber, with 2048-bit key size and one (1) or two (2years validity from issuing start date.
These TunTrust SSL Certificates are compliant with and include the OID reference of the OVCP certificate policy of the ETSI Technical Standard 319 411-1 (i.e., 0.4.0.2042.1.7).
The usage purpose of these TunTrust SSL Certificates is the combined purpose of digital signature and key encryption. The TunTrust OVCP Server Certificates include the corresponding TunTrust OID for SSL server certificates, i.e., *<2.16.788.1.2.6.1.8 >*.
The following table provides the description of the fields for TunTrust OV SSL Certificates issued under TunServerCA2:

Base Profile	Included	Critical	O/M[1]	CO[2]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	TunServerCA2 Signature
Issuer DN	X			S	C=TN, O=National Digital Certification Agency, CN=Tunisian Server Certificate Authority - TunServerCA2
Subject DN	X	False			
serialNumber	X		M	D	Serial Number as constructed by CRAO
commonName	X		O	D	FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server.
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166).
localityName	X		M	D	Location in which the company's registered office is established.

[1] O/M: O = Optional, M = Mandatory.
[2] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
OrganizationalUnitName	X		O	D	Company department or other information item
emailAddress	X		O	D	Email Address
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 365 days or 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				keyid:87:AB:F7:69:4B:50:F6:61:57:FF:3F:5B:8E:1D:70:C6:A2:6C:AA:C6
authorityInfoAccess	X	False			
Authority Information Access	X				CA Issuers - URI:http://www.tuntrust.tn/pub/TunServerCA2.crt OCSP - URI:http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/TunServerCA2.crl
subjectAltName	X	False			
SubjectAltName-dNSName[3]	X		M		FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server.
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	False
KeyEncipherment	X			S	True
dataEncipherment	X			S	False
certificatePolicies	X	False			

[3] Additional SAN can be added depending on the subscriber requirement

PolicyIdentifier	X				Policy: 2.16.788.1.2.6.1.8 Policy : 0.4.0.2042.1.7 Policy: 2.23.140.1.2.2
Extended Key Usage	X	False			
serverAuth	X			S	True
clientAuth	X			S	True
Certificate Transparency SCTs	X				Timestamp of the log servers.

E. TnTrust Gov CA End-Entity Certificates Profiles

The following types of Certificates are issued under TnTrust Gov CA:

1. OV SSL Certificates

TunTrust OV SSL Server Certificates are ETSI EN 319 411-1 Certificates not certified as generated on QSCD, with creation of the keys by the Subscriber, with 2048-bit key size and one (1) or two (2years validity from issuing start date.
These TunTrust SSL Certificates are compliant with and include the OID reference of the OVCP certificate policy of the ETSI Technical Standard 319 411-1 (i.e., 0.4.0.2042.1.7).
The usage purpose of these TunTrust SSL Certificates is the combined purpose of digital signature and key encryption. The TunTrust OVCP Server Certificates include the corresponding TunTrust OID for SSL server certificates, i.e., <2.16.788.1.2.6.1.9.1.1>.
The following table provides the description of the fields for TunTrust OV SSL Certificates issued under TnTrust Gov CA:

Base Profile	Included	Critical	O/M[4]	CO[5]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	TnTrust Gov CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Gov CA
Subject DN	X	False			
serialNumber	X		M	D	Serial Number as constructed by CRAO
commonName	X		M	D	FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server.
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166).
localityName	X		M	D	Location in which the company's registered office is established.

[4] O/M: O = Optional, M = Mandatory.
[5] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
OrganizationalUnitName	X		O	D	Company department or other information item
emailAddress	X		O	D	Email Address
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 365 days or 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				keyid: 7B:D6:C4:15:45:CF:06:34:95:69:36:86:DA:75:7D:9B:FB:EB:73:D9
authorityInfoAccess	X	False			
Authority Information Access	X				CA Issuers - URI:http://www.tuntrust.tn/pub/TnTrustGovCA.crt OCSP - URI:http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustgovca.crl
subjectAltName	X	False			
SubjectAltName-dNSName[6]	X		M		FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server.
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
KeyEncipherment	X			S	True
certificatePolicies	X	False			

[6] Additional SAN can be added depending on the subscriber requirement

PolicyIdentifier	X				Policy: 0.4.0.2042.1.7 Policy: 2.16.788.1.2.6.1.9.1.1 Policy: 2.23.140.1.2.2
Extended Key Usage	X	False			
serverAuth	X			S	True
clientAuth	X			S	True
Certificate Transparency	X				Timestamp of the log servers.

2. Promosport certificate

Promosport Certificates are ETSI EN 319 411-1 Certificates not certified as generated on QSCD, with creation of the keys by the TunTrust RA, with 2048-bit key size and one (1) or two (2years validity from issuing start date.

These Certificates are compliant with the OID reference of the LCP certificate policy of the ETSI Technical Standard 319 411-1 (i.e., 0.4.0.2042.1.3).

The following table provides the description of the fields for Promosport Certificates issued under TnTrust Gov CA:

Base Profile	Included	Critical	O/M[7]	CO[8]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Agency For Digital Certification, CN=TnTrust Gov CA
Subject DN	X	False			
commonName	X		M	D	Concatenation of given name and surname as in ID card separated by a "space" character.
Locality	X		M	D	Locality Name
countryName	X		M	D	Nationality of holder (ISO3166)
emailAddress	X		M	D	Subject's email address
OrganizationName	X		M	D	Name of company/institution.
OrganizationalUnitName	X		O	D	Company department or other information item
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		

[7] O/M: O = Optional, M = Mandatory.
[8] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA

X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TunTrust Qualified CA public key
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.certification.tn/tntrustgovca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
KeyUsage	**X**	**True**			
digitalSignature	X			S	True
nonRepudiation	X			S	True
KeyEncipherment	X			S	True
Extended Key Usage	X	False			
E-mail Protection	X			S	True
Client Authentication	X			S	True

F. TnTrust Qualified Gov CA End-Entity Certificates Profiles

The following types of Certificates are issued under TnTrust Qualified Gov CA :

1. ID-Trust Certificate

ID-Trust is a Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the TunTrust on a qualified cryptographic support (token or Hardware Security module), 2048 bit key size and two (2) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding TunTrust OID, i.e., < OID 2.16.788.1.2.6.1.10.1.1>.

The following table provides the description of the fields for ID-Trust Certificates:

Base Profile	Included	Critical	O/M[9]	CO[10]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Agency For Digital Certification, CN=TnTrust Qualified Gov CA
Subject DN	X	False			
commonName	X		M	D	Concatenation of given name and surname as in ID card separated by a "space" character.
givenName	X		O	D	Given Name as on ID card
surname	X		O	D	Surname as on ID card without indication 'épouse', 'ép' or similar and the subsequent name
countryName	X		M	D	Nationality of holder (ISO3166)
emailAddress	X		M	D	Subject's email address
OrganizationName	X		O	D	For certificate with professional attributes: Name of company/institution.
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			

[9] O/M: O = Optional, M = Mandatory.
[10] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TnTrust Qualified Gov CA public key
authorityInfoAccess	X	False			CA Issuers - URI:http://www.tuntrust.tn/pub/TnTrustQualifiedGovCA.crt OCSP - URI:http://va.tuntruts.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustqualifiedgovca.crl
subjectAltName	X	False			
Rfc822Name	X		O	D	Certificate subscriber's email address
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
Policy Properties					
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	True
keyEncipherment	X			S	False
dataEncipherment	X			S	False
Extended Key Usage	X	False			
E-mail Protection	X			S	True
MS Smart Card Logon	X			S	True
Client Authentication	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.6.1.10.1.1 Policy: 0.4.0.194112.1.2
QualifiedCertificateStat	X	False			
QcCompliance (0.4.0.1862.1.1)	X		M	S	True
QcSSCD (0.4.0.1862.1.4)			M	S	True
QcPDS (0.4.0.1862.1.5)	X		M	S	http://www.certification.tn/pub/pds-tuntrustgovca.pdf
QcType (0.4.0.1862.1.6)	X		M	S	Id-etsi-qct-esign (0.4.0.1862.1.6.1)

2. Enterprise-ID Certificate

Enterprise-ID is a qualified Certificate compliant with ETSI EN 319 411-2 QCP-l-qscd certificate policy with creation of the keys by the TunTrust on a qualified cryptographic support (token or Hardware Security module), 2048 bit key size and two (2) years validity, and with a key usage limited to the support of qualified e-seal. These Certificates include the corresponding TunTrust OID, i.e., < OID 2.16.788.1.2.6.1.10.1.2>.

The following table provides the description of the fields for Enterprise-ID Certificates:

Base Profile	Included	Critical	O/M[11]	CO[12]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TunTrust Qualified Gov CA
Subject DN	X	False			
commonName	X		M	D	Contains the full registred name of the subject (legal person)
countryName	X		M	D	Country in which the company's or institution's registered office is established. (ISO3166)
organisationIdentifier (2.5.4.97)	X		M	D	Contains information using the following structure in the presented order: - 3 character legal person identity type reference; VAT - 2 character ISO 3166 country code; - hyphen-minus "-" and - Tax Identification number
organisationIsentifier			O	D	
OrganizationName	X		M	D	Contains the full registered name of the subject (legal person).
OrganizationalUnitName	X		O	D	Company department or other information item
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days

[11] O/M: O = Optional, M = Mandatory.
[12] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TunTrust Qualified Gov CA public key
authorityInfoAccess	X	False			OCSP - URI:http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustqualifiedgovca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
Policy Properties					
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 2.16.788.1.2.6.1.10.1.2 Policy: 0.4.0.194112.1.3 Policy:0.4.0.2042.1.2
QualifiedCertificateStat	X	False			
QcCompliance (0.4.0.1862.1.1)	X		M	S	True
QcSSCD (0.4.0.1862.1.4)			M	S	True
QcPDS (0.4.0.1862.1.5)	X		M	S	http://www.certification.tn/pub/pds-tuntrustgovca.pdf
QcType (0.4.0.1862.1.6)	X		M	S	Id-etsi-qct-eseal (0.4.0.1862.1.6.2)

G.TN01 End-Entity Certificates Profiles

The following type of Certificates is issued under TN01 CA:

Base Profile	Included	Critical	O/M[13]	CO[14]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	ecdsa-with-SHA384
Signature Value	X	False		D	TN01 Signature
Issuer DN	X			S	CN=TN01, OU=TN CEV CA, O=National Digital Certification Agency, C=TN
Subject DN	X	False			
commonName	X		M	D	04 characters (as assigned bu CRAO)
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166).
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
OrganizationalUnitName	X		O	D	Tax Identifier of the Organization
emailAddress	X		O	D	Email Address
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 365 days or 730 days or 1095 days
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				keyid: CE:87:48:48:A9:2F:A8:F5:B6:CB:F7:97:B5:F7:02:91:D2 :8A:9C:58
authorityInfoAccess	X	False			
Authority Information Access	X				OCSP - URI:http://va.certification.tn

[13] O/M: O = Optional, M = Mandatory.
[14] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

X509v3 CRL Distribution Points	X	False		S	URI: URI:http://crl.certification.tn/cevca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	True
dataEncipherment	X			S	False
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 2.16.788.1.2.6.1.12

H. TimeStamp certificate

The following table provides the description of the fields for Timestamp Certificates issued to TunTrust timestamp unit:

Base Profile	Included	Critical	O/M[15]	CO[16]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	Issuing CA DN
Subject DN	X	False			
commonName	X		M	D	Name of the Timestamp Unit
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166).
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 1095 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				Authority Key Identifier
authorityInfoAccess	X	False			
Authority Information Access	X				OCSP - URI:http://va.certification.tn
X509v3 CRL Distribution Points	X	False		S	URI:URI of the CRL
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True

[15] O/M: O = Optional, M = Mandatory. [15]
[16] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.6.1.9.1.7
Extended Key Usage	X	False			
Time Stamping	X			S	True

I. OCSP Certificate

The following table provides the description of the fields for TunTrust OCSP profile:

Base Profile	Included	Critical	O/M[17]	CO[18]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	Issuing CA DN
Subject DN	X	False			
commonName	X		M	D	Name of the validation Authority
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166).
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
Locality	X		M	D	Locality Name
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				Authority Key Identifier
authorityInfoAccess	X	False			
Authority Information Access	X				OCSP - URI:http://va.certification.tn
X509v3 CRL Distribution Points	X	False		S	URI:URI of the CRL
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
certificatePolicies	X	False			

[17] O/M: O = Optional, M = Mandatory. [17]
[18] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

PolicyIdentifier	X				Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.6.1.9
OCSP No Check	X			S	
Extended Key Usage	X	False			
OCSP Signing	X			S	True

J. CRL profile

In conformance with the IETF PKIX RFC 2459, the TunTrust CAs support CRLs compliant with:

- Version numbers supported for CRLs
- CRL and CRL entry extensions populated and their criticality.

The profile of the CRL is provided in the table below:

Field	Value
Version	V2 in accordance with RFC 5280.
Signature Algorithm	Object identifier of the algorithm used to sign the certificate sha256RSA.
Issuer DN	Subject CA
ThisUpdate	Issue date/time of the CRL. CRLs are effective upon issuance.
NextUpdate	Date by which the next CRL will be issued. Creation date/time + 365 days for Offline CA Creation date/time + 6 days for Online Issuing CA
revokedCertificates	
userCertificate	Certificate serial number
revocationDate	Revocation time
crlExtensions	
CRL Number	A monotonically increasing sequence number in accordance with RFC 5280
Authority Key Identifier	Populated by CA application contains key id (SHA1) of issuer public key
2.5.29.60	True This field is only activated for TnTrust Qualified Gov CA.

K. Timestamp Request Format

The following table lists the fields that are expected by the Time Stamping units:

Field	Value / Comment
Document Hash	Hash of the document on which the TimeStamp must be computed
Hash OID	SHA-256
Nonce	A random number, also referred to as "nonce", allows the developer to better associate a Timestamp Request to its response, since the latter will include the same nonce.
Should TSA Certificate be included?	True/False

L. Timestamp Response Format

The following table lists which fields are populated by the Time Stamping units:

Field	Value / Comment
Generation Time	The Time at which the time-stamp token has been created by the TSA. It is expressed as UTC time (Coordinated Universal Time).
Document Hash	Hash of the document on which the TimeStamp response has been computed.
Hash algorithm	SHA-256
Policy OID	2.16.788.1.2.6.1.11 The OID of the policy that should be applied by the TSU during the generation of the timestamp token. The policy generally describes legal value and accuracy of the resulting timestamp.
Accuracy	1 second
TSA Certificate Information	Current TSU Certificate
QcStatement	True