



CONFORMITY ASSESSMENT BODY
EIDAS
TRUST SERVICE PROVIDERS
ISO 27001
LA ISO 27001
LI ISO 27001
RM ISO 27005

Audit Attestation for

AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE

*Parc Technologie El Ghazala Route de Raoued Km, 3,5
2083 Ariana - Tunisie*

Reference: No. 1648-69-AL-V1.0

Saint-Malo, 6th November 2018

To whom it may concern,

This is to confirm that LSTI has successfully audited the CAs of the “AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE” without remaining critical findings, if any. This present Audit Attestation Letter is registered under the unique identifier number n°1648-69-AL-V1.0 and consist of 6 pages.
Kindly find here-below the details accordingly.

In case of any question, please contact:

*LSTI Group
10 Avenue Anita Conti
35400 Saint-Malo, France
E-Mail: armelle.trocin@lsti.eu
Phone: +33 608675144*

With best regards,

Armelle Trocin
Head of Certification Body

Identification of the conformity assessment body (CAB):	<p>LSTI¹, 10 Avenue Anita Conti, 35400 Saint-Malo, France registered under n°453867863 Accredited by COFRAC under registration number 5-0546 in accordance with EN ISO/IEC 17065:2013 and in accordance with the eIDAS EU Regulation art. 3 (18) and the ETSI EN 319 403 v2.2.2. Detailed scope at http://cofrac.fr/en/easysearch/index.php</p>
--	--

Identification of the trust service provider (TSP):	<p>AGENCE NATIONALE DE LA CERTIFICATION ELECTRONIQUE Parc Technologie El Ghazala Route de Raoued Km, 3,5 2083 Ariana - Tunisie registered under R.C.S. TN N° 2083</p>
--	--

Identification of the audited Root-CA:	Tunisia National Root CA	
	Distinguished Name	Tunisia National Root CA
	SHA-256 fingerprint	4F:BA:9F:8B:2B:F7:0D:94:7F:F8:47:C1:5F:BA:65:1338:84:01:8A:9B:B2:B2:E2:09:B8:33:C9:3F:57:B6:7C
	Certificate Serial number	683E1155929C8E8E
	Applied policy	None
	Validity	29/11/2016 to 29/05/2037

¹ in the following termed shortly "CAB"

Identification of the audited Sub Root-CA:	Tunisia Gov CA	
	Distinguished Name	Tunisia Gov CA
	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 Serial number	782C1009830A4BEE
	Applied policy	None
	Validity	29/11/2016 - 29/02/2032

Identification of the audited Root-CA:	Tunisian Root Certificate Authority – TunRootCA2	
	Distinguished Name	Tunisian Root Certificate Authority – TunRootCA2
	SHA-256 fingerprint	C7:95:FF:8F:F2:0C:96:66:88:F0:64:A1:E0:91:42:1D 31:10:A3:45:6C:17:EC:24:04:B9:98:73:87:41:F6:22
	Certificate Serial number	2166150505270505BC8AB01DAF0ABEC4
	Applied policy	None
	Validity	05/05/2015 to 05/05/2027

The audit was performed as full annual audit at the TSP's location in *Tunisia*. It took place from *03/09/2018* until *07/09/2018* and covered the period from *13/09/2017* until *07/09/2018*.

The next full assessment has to be carried out before *07/09/2019* as required by browsers.

The audit was performed according to the European Standards "*ETSI EN 319 411-2, V2.1.1 (2016-02)*", "*ETSI EN 319 411-1, V1.1.1 (2016-02)*" and "*ETSI EN 319 401, V2.1.1 (2016-02)*" as well as CA Browser Forum Requirements "*Baseline Requirements, version 1.6.0*" considering the requirements of the "*ETSI EN 319 403, V2.2.2 (2015-08)*" for the Trust Service Provider Conformity Assessment.

The full annual audit was based on the following policy and practice statement documents of the TSP:

CP/CPS	[CPCPS-TunisianNationalPKI-05.pdf]	version 5
	31/08/2018	
CP/CPS	[PolitiqueSERVEURS-PTC-BR-07]	version 7
	31/08/2018	
PDS	[pds-tuntrustgovca.pdf]	version 1
	31/08/2018	
SA	[SubscriberAgreement]	version 3
	31/08/2018	
AD GAC 03	« Naming and Profiles Document »	version 1
	31/08/2018	

The Sub-CAs that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below. The TSP assured that all non-revoked Sub-CA's that are technically capable of issuing server or email certificates and that have been issued by this Root-CA are in the scope of regular audits.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number OID	Applied policy	Service	EKU	Validity
TnTrust Gov CA	CN=TnTrust Gov CA,O=National Digital Certification Agency,L=Tunis,C=TN	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	36716FA436ECC2D2	Policy: 0.4.0.2042.1.7 (OVCP) Policy: 2.16.788.1.2.6.1.9.1.1 Policy: 2.23.140.1.2.2 (Cab Forum BR - Organization Identified)	Web Server authentication	TLS Web Client Authentication, TLS Web Server Authentication	29/12/2026
TnTrust Qualified Gov CA	CN=TnTrust Qualified Gov CA,O=National Digital Certification Agency,L=Tunis,C=TN	45:87:7E:FD:70:09:3B:5B:B3:66:FF:C6:FC:F0:D5:B7:EF:FE:1C:0E:C1:DE:4D:54:E1:06:7D:8B:5F:EB:1F:5C	676363EC156DC7D7	Policy: 0.4.0.194112.1.2 (QCP-n-qscd) Policy: 2.16.788.1.2.6.1.10.1.1 - Policy: 0.4.0.194112.1.3 (QCP-l-qscd) Policy: 2.16.788.1.2.6.1.10.1.2	Electronic Signature eSeal	TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin	29/12/2026
TunServerCA2	CN=Tunisian Server Certificate Authority - TunServerCA2,O=National Digital Certification Agency,C=TN	3A:BA:1F:4F:41:65:69:16:89:42:7A:DC:87:94:8C:CF:6C:7C:4B:D6:B7:CC:50:04:DA:7F:3B:23:D3:8B:B7:26	0F0D7C57C2A92569	Policy: 2.16.788.1.2.6.1.8 Policy: 0.4.0.2042.1.7 (OVCP) Policy: 2.23.140.1.2.2 (Cab Forum BR - Organization Identified)	Web Server authentication	TLS Web Client Authentication, TLS Web Server Authentication	12/07/2020

Table 1: Sub-CA's issued by the Root-CA

Modifications records

Version	Issuing Date	Changes
Version 1	6 November 2018	Initial attestation

End of the audit attestation letter