Deloitte.

Deloitte LLP
Bay Adelaide Centre, East Tower
8 Adelaide Street West, Suite 200
Toronto, ON M5H 0A9, Canada

Tel: +1 416 601 6150
Fax: +1 416 601 6400
www.deloitte.ca

INDEPENDENT ASSURANCE REPORT

To the management of the Agence Nationale de Certification Électronique ("ANCE" or "TunTrust"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on TunTrust management's statement, that for its Certification Authority (CA) operations at Tunis, Tunisia, throughout the period 1st October 2024 to 30th September 2025 for its CAs as enumerated in Attachment A, TunTrust has:

- disclosed its TLS certificate lifecycle management business practices in its:
  - TunTrust PKI CP/CPS v06.1, released on 08 September 2025
  - TunTrust PKI CP/CPS v06, released on 11 June 2025
  - TunTrust PKI CP/CPS v05.9, released on 24 March 2025
  - TunTrust PKI CP/CPS v05.8, released on 15 March 2025
  - TunTrust PKI CP/CPS v05.7, released on 3 February 2025
  - TunTrust PKI CP/CPS v05.6, released on 16 December 2024
  - TunTrust PKI CP/CPS v05.5, released on 30 October 2024
  - TunTrust PKI CP/CPS v05.4, released on 2 September 2024

  including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on TunTrust website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
  - TLS subscriber information is properly authenticated (for the registration activities performed by TunTrust);

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.9.

The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates require the CA to operate controls to adhere to the Network and Certificate System Security Requirements. The WebTrust Principles and Criteria for Certification Authorities - Network Security address this requirement and are reported on in a separate report.

Certification authority's responsibilities

TunTrust's management is responsible for its statement, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.9.

Our independence and quality management

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behaviour.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's statement based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's statement is fairly stated, and, accordingly, included:

1. obtaining an understanding of TunTrust's TLS certificate lifecycle management business practices, including its relevant controls over the issuance and revocation of TLS certificates;
2. selectively testing transactions executed in accordance with disclosed TLS certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and
4. performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at TunTrust and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period 1st October 2024 to 30th September 2025, TunTrust management's statement, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.9.

This report does not include any representation as to the quality of TunTrust's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.9, nor the suitability of any of TunTrust's services for any customer's intended purpose.

Other Matters

Without modifying our opinion, we noted the following other matters during our procedures. These matters were within the scope of our reasonable assurance engagement. We considered the nature of these matters in our risk assessment and in determining the nature, timing, and extent of our procedures. We performed additional procedures to understand the root cause, as well as the facts and circumstances.

#	Observation	Relevant WebTrust for Certification Authorities or CA/B Forum– TLS Baseline Requirements
1	As disclosed in Tuntrust management statement and publicly reported in Bugzilla 1981680, in course of self-audit, management has identified one subscriber TLS certificate that included an emailAddress attribute in the Distinguished Name (DN), even though this attribute is not permitted in the CP/CPS-approved subscriber certificate profile. The certificate was revoked the same day the issue was detected, and a full audit found no other certificates with the same non-compliance.	• Self audit : section 8.7 in CA/B Forum TLS BRs v2.1.6 • Subscriber Certificate profile: Section 7.1.2.7.4 and Appendix B of CP/CPS version 06 .

#	Observation	Relevant WebTrust for Certification Authorities or CA/B Forum– TLS Baseline Requirements
	Deloitte confirmed no other instances during the audit period.	
	As disclosed by Tuntrust management statement and publicly reported in Bugzilla 1988405, management received external report indicating that the website associated with valid OV SSL test certificate was serving an expired certificate. Investigation was conducted and the DNS records have been corrected on the same day to reflect the updated public IP address. Since then, the domain has been serving the valid test certificate as intended. No other publicly accessible components were affected. This issue was limited exclusively to the valid OV SSL test website certificate. Deloitte retested the valid OV SSL test certificate and noted that the website associated with the valid OV SSL test certificate is serving a valid certificate.	• Section 2.2 in CAB/F TLS BR v 2.1.7 • Section 2.2 in CP/CPS v 06.1

Use of the WebTrust seal

TunTrust's use of the WebTrust for Certification Authorities – TLS Baseline seal constitutes a symbolic representation of the contents of this report, and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Deloitte LLP.

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
16 December 2025

ATTACHMENT A

LIST OF OV TLS CAs IN-SCOPE

Root CA
1. TunTrust Root CA
OV TLS Issuing CA
2. TunTrust Services CA

CA IDENTIFYING INFORMATION FOR IN-SCOPE OV TLS CAs

CA #	Cert #	Subject	Issuer	Serial Number	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	Extended Key Usage	EKU [RFC5280]	Subject Key Identifier	SHA256 Fingerprint
1	1	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA	1302D5E2404C92468616675DB4BBBBB26B3EFC13	rsaEncryption	4096 bits	sha256WithRSA Encryption	26 April 2019 08:57:56	26 April 2044 08:57:56			069A9B1F537DF1F5A4C8D3863EA17359B4F74421	2E44102AB58CB85419451C8E19D9ACF3662CAFBC614B6A53960A30F7D0E2EB41
2	1	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Services CA	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA	601A7C2F6093B7A673DA5F8C9C885F37A75897C0	rsaEncryption	4096 bits	sha256WithRSA Encryption	26 April 2019 10:23:31	26 April 2039 10:23:31	TLS Web Client Authentication, TLS Web Server Authentication	id-kp-clientAuth, id-kp-serverAuth	9F2517CE6F90AB612FC147A9E02F99135DFA2339	063627355C941A1C93FC515CBAEF2F173D4A646DDEB139CB8C75C1022222994F

TUNTRUST MANAGEMENT'S STATEMENT

The Agence Nationale de Certification Électronique ("ANCE" or "TunTrust") operates the Certification Authority (CA) services as enumerated in Attachment B, and provides TLS CA services.

The management of TunTrust is responsible for establishing and maintaining effective controls over its TLS CA operations, including its TLS CA business practices disclosure on its website https://www.tuntrust.tn/repository, TLS key lifecycle management controls, and TLS certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to TunTrust's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

TunTrust management has assessed its disclosures of its certificate practices and controls over its TLS CA services. Based on that assessment, in providing its TLS Certification Authority (CA) services at Tunis, Tunisia, throughout the period 1st October 2024 to 30th September 2025, TunTrust has:

- disclosed its TLS certificate lifecycle management business practices in its:
  - TunTrust PKI CP/CPS v06.1, released on 08 September 2025
  - TunTrust PKI CP/CPS v06, released on 11 June 2025
  - TunTrust PKI CP/CPS v05.9, released on 24 March 2025
  - TunTrust PKI CP/CPS v05.8, released on 15 March 2025
  - TunTrust PKI CP/CPS v05.7, released on 3 February 2025
  - TunTrust PKI CP/CPS v05.6, released on 16 December 2024
  - TunTrust PKI CP/CPS v05.5, released on 30 October 2024
  - TunTrust PKI CP/CPS v05.4, released on 2 September 2024

  including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on TunTrust website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
  - TLS subscriber information is properly authenticated (for the registration activities performed by TunTrust)
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations

in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.9.

TunTrust management has reported the following 'bug' on Mozilla's Bugzilla reporting system:

Bug ID	Summary	Opened	Closed
1988405	The valid test webpage temporarily presented an expired certificate. The issue was caused by an outdated DR DNS record that was still pointing to an old DR host with an expired certificate. This occurred after a new host and IP were introduced on 20 June 2025, but only the main site DNS entry was updated. The problem became visible during a planned failover on 10 September 2025, when traffic was redirected to the DR environment. The Issue was resolved on September 11th, 2025, and the bug on Bugzilla was resolved on October 22nd, 2025.	2025-09-13	2025-10-22
1981680	An issue affecting a single subscriber certificate was reported on 07 August 2025 on Bugzilla: The Distinguished Name included the "Email" attribute, which was not permitted under the CP/CPS-approved subscriber certificate profile. The emailAddress attribute had been configured as optional based on the TLS Baseline Requirements version applicable at the time, and validation and internal audit activities relied on the CP/CPS and automated change-management alerts, resulting in the issue not being identified earlier. Remediation actions were implemented, including removal of the emailAddress attribute from the subscriber certificate profile, enhancement of	2025-08-07	2025-09-26

	change-control and validation procedures, integration of the pkimetal linting tool into the issuance process, and inclusion of lessons learned in annual training for trusted roles. The issue was remediated on August 6, 2025, and the related Bugzilla report was closed on September 26, 2025.		

Ramzi Khlif, General Director
TunTrust – Agence Nationale de Certification Électronique
16 December 2025

Ministère des Technologies de la Communication
Agence Nationale de Certification Electronique

ATTACHMENT B

LIST OF OV TLS CAs IN-SCOPE

Root CA
1. TunTrust Root CA
OV TLS Issuing CA
2. TunTrust Services CA