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 2023 to 30 September 2024 for its CAs as enumerated in Attachment A, TunTrust has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - TunTrust PKI CP/CPS v5.4, released on 2 September 2024
  - TunTrust PKI CP/CPS v5.3, released on 24 May 2024
  - TunTrust PKI CP/CPS v5.2, released on 1st March 2024
  - TunTrust PKI CP/CPS v5.1, released on 12 September 2023
  - TnTrust Sign PKI CP/CPS v1.4, released on 24 May 2024
  - TnTrust Sign PKI CP/CPS v1.3, released on 1st March 2024
  - TnTrust Sign PKI CP/CPS v1.2, released on 12 September 2023
- maintained effective controls to provide reasonable assurance that:
  - TunTrust provides its services in accordance with its Certification Practice Statements;
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by TunTrust); and
- 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 v2.2.2.

TunTrust does not escrow its CA keys, does not provide subscriber key generation, storage, or recovery services, does not provide integrated circuit card management services, does not provide certificate renewal, rekey, or suspension services, and does not provide third-party subordinate CA or cross-certificate issuance or management. Accordingly, our procedures did not extend to controls that would address those criteria.

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 v2.2.2.

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.

Deloitte.

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 key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance, and operation of systems integrity;
2. selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business 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 2023 to 30 September 2024, 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 v2.2.2.

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 v2.2.2, nor the suitability of any of TunTrust's services for any customer's intended purpose.

Use of the WebTrust seal

TunTrust's use of the WebTrust for Certification Authorities 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
13 December 2024

Deloitte.

ATTACHMENT A

LIST OF CAs IN-SCOPE

Root CAs
1. TunTrust Root CA 2. TnTrust Root CA - G1
OV SSL Issuing CA
3. TunTrust Services CA
Other CAs
4. TnTrust CA - QSign1

Deloitte.

CA IDENTIFYING INFORMATION FOR IN-SCOPE 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	sha256WithRSAEncryption	26 April 2019 08:57:56	26 April 2044 08:57:56			069A9B1F537DF1F5A4C8D3863EA17359B4F74421	2E44102AB58CB85419451C8E19D9ACF3662CAFBC614B6A53960A30F7D0E2EB41
2	1	CN=TnTrust Root CA - G1, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN	CN=TnTrust Root CA - G1, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN	3C892671A75CECCD6A9C2080284700A2DD39FF676	rsaEncryption	8192 bits	sha512WithRSAEncryption	21 September 2022 16:27:45	21 September 2047 16:27:45			CBA52528433E52E3554672793D6FFCA95904EB56	54E84A8E9DA7F3BB14F35C7F9C314B6EAB2739EB8086C8000F00C0993C3E694C
3	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	sha256WithRSAEncryption	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
4	1	CN=TnTrust CA - QSign1, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN	CN=TnTrust Root CA - G1, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN	63AD026B2F40B526906C38D0E6D2AD8B3DF29E30	rsaEncryption	4096 bits	sha256WithRSAEncryption	21 September 2022 17:57:31	21 September 2042 17:57:31			48C0C1B5B68B123614366609A8CB255DBA216978	A088363A6B1927E271E184C6F73CF5999F190E6A4A205A4182E017F8121D6331

TUNTRUST MANAGEMENT'S STATEMENT

The Agence Nationale de Certification Électronique ("ANCE" or "TunTrust") operates the Certification Authority (CA) services as enumerated in Attachment A, TunTrust has:

- Subscriber registration
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of TunTrust is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website https://www.tuntrust.tn/repository, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, and 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 CA services. Based on that assessment, in TunTrust management's opinion, in providing its Certification Authority (CA) services at Tunis, Tunisia, throughout the period 1st October 2023 to 30 September 2024, TunTrust has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
    - TunTrust PKI CP/CPS v5.4, released on 2 September 2024
    - TunTrust PKI CP/CPS v5.3, released on 24 May 2024
    - TunTrust PKI CP/CPS v5.2, released on 1st March 2024
    - TunTrust PKI CP/CPS v5.1, released on 12 September 2023
    - TnTrust Sign PKI CP/CPS v1.4, released on 24 May 2024
    - TnTrust Sign PKI CP/CPS v1.3, released on 1st March 2024
    - TnTrust Sign PKI CP/CPS v1.2, released on 12 September 2023
- maintained effective controls to provide reasonable assurance that:
    - TunTrust provides its services in accordance with its Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
    - subscriber information is properly authenticated (for the registration activities performed by TunTrust); and
- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorised individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity;

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

- Security Management
- Asset Classification and Management

- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

TunTrust does not escrow its CA keys, does not provide subscriber key generation, storage, or recovery services, does not provide integrated circuit card management services, does not provide certificate renewal, rekey, or suspension services, and does not provide third-party subordinate CA or cross-certificate issuance or management. Accordingly, our statement does not extend to controls that would address those criteria.

Ramzi Khlif, General Director
TunTrust – Agence Nationale de Certification Électronique
13 December 2024

ATTACHMENT A

LIST OF CAs IN-SCOPE

Root CAs
1. TunTrust Root CA 2. TnTrust Root CA - G1
OV SSL Issuing CA
3. TunTrust Services CA
Other CAs
4. TnTrust CA - QSign1