

## INDEPENDENT ASSURANCE REPORT

To the management of Agence Nationale de Certification Electronique (“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 in Ariana, Tunisia, throughout the period 1 October 2021 to 30 September 2022 (the “Period”) for its CAs as enumerated in [Attachment A](#), TunTrust has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - TunTrust PKI Certificate Policy / Certification Practice Statement, v04.9, 08 April 2022
  - TunTrust PKI Certificate Policy / Certification Practice Statement, v04.8, 20 September 2021

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the 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 SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.6](#)

### 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 – SSL Baseline with Network Security v2.6.

### Our independence and quality control

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 Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and 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 (Revised), *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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of TunTrust's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- (2) selectively testing transactions executed in accordance with disclosed SSL 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.

## Relative effectiveness of controls

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.

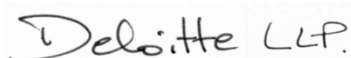
## Practitioner's opinion

In our opinion, throughout the period 1 October 2021 to 30 September 2022, 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 – SSL Baseline with Network Security v2.6

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 – SSL Baseline with Network Security v2.6, 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  
Chartered Professional Accountants  
Toronto, Ontario, Canada  
16 November 2022



ATTACHMENT A

LIST OF IN SCOPE CAs for SSL BASELINE REQUIREMENTS

<b>Root CA</b>
1. TunTrust Root CA
<b>OV SSL Issuing CA</b>
2. TunTrust Services CA

CA IDENTIFYING INFORMATION

CA #	Cert #	Subject	Issuer	Serial Number	Key Type	Hash Type	Not Before	Not After	Extended Key Usage	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	27b4bd1d08289f6d78e2cedceef25dca3a702990	RSA 4096 -bits	RSA SHA-256	Apr 18 09:42:39 2019 GMT	Apr 18 09:42:39 2044 GMT	Digital Signature, Certificate Sign, CRL Sign	069A9B1F537DF1F5A4C8D3863EA17359B4F74421	BABBCA986946352CF9BF382E880652F4E94DBC4FEDD0F1CC21FA9973C96D65AB
1	2	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA	1302d5e2404c92468616675db4bbbb26b3efc13	RSA 4096 -bits	RSA SHA-256	Apr 26 08:57:56 2019 GMT	Apr 26 08:57:56 2044 GMT	Certificate Sign, CRL Sign	069A9B1F537DF1F5A4C8D3863EA17359B4F74421	2E44102AB58CB85419451C8E19D9ACF3662CAFBC61486A53960A30F7D0E2EB41
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	574ebb9529348333d742990c24a4d00c49681e6	RSA 4096 -bits	RSA SHA-256	Apr 18 10:36:54 2019 GMT	Apr 18 10:36:54 2039 GMT	Digital Signature, Certificate Sign, CRL Sign	9F2517CE6F90AB612FC147A9E02F99135DFA2339	598BC438BB33AE8FC2ADBFC701804920E92C1311AFF8FEB49A51D96393987FD8
2	2	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	RSA 4096 -bits	RSA SHA-256	Apr 26 10:23:31 2019 GMT	Apr 26 10:23:31 2039 GMT	Certificate Sign, CRL Sign	9F2517CE6F90AB612FC147A9E02F99135DFA2339	063627355C941A1C93FC515CBAEF2F173D4A646DDEB139CB8C75C102222994F

## TUNTRUST MANAGEMENT'S STATEMENT

Agence Nationale de Certification Electronique ("ANCE" or "TunTrust") operates the Certification Authority (CA) services as enumerated in [Attachment A](#), and provides SSL CA services.

The management of TunTrust is responsible for establishing controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL 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, controls placed into operation can only provide reasonable assurance with respect to TunTrust's Certification Authority operations.

TunTrust management has assessed its TunTrust PKI Certificate Policy / Certification Practice Statement controls over its SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services at Ariana, Tunisia, throughout the period 1 October 2021 to 30 September 2022, TunTrust has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - TunTrust PKI Certificate Policy / Certification Practice Statement, v04.9, 08 April 2022
  - TunTrust PKI Certificate Policy / Certification Practice Statement, v04.8, 20 September 2021

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the 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 SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL 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
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.6](#).

Ramzi Khlif  
Agence Nationale de Certification Electronique  
9 November 2022

**ATTACHMENT A**

**LIST OF IN SCOPE CAs for SSL BASELINE REQUIREMENTS**

<b>Root CA</b>
1. TunTrust Root CA
<b>OV SSL Issuing CA</b>
2. TunTrust Services CA