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 Agence Nationale de Certification Electronique ("ANCE" or "TunTrust"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on ANCE management's assertion that for its Certification Authority (CA) operations in Tunis, Tunisia, as of 30 April 2019 for its CAs as enumerated in Attachment A, ANCE has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - TunTrust PKI Certificate Policy / Certification Practice Statement, v02, 29 April 2019 ("CP/CPS"), including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ANCE website, and provided such services in accordance with its disclosed practices

- suitably designed, and placed into operation, 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 ANCE)

- suitably designed, and placed into operation, 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

- suitably designed, and placed into operation, 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 v2.3.

Certification authority's responsibilities

ANCE's management is responsible for its assertion, 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 v2.3.

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, 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.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion 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 assertion is fairly stated, and, accordingly, included**:**

(1) obtaining an understanding of ANCE'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 ANCE'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) evaluating the suitability of the design 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.

Suitability of controls

The suitability of the design of the controls at ANCE 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 suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, ANCE's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, as of 30 April 2019, ANCE management's assertion, 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 v2.3.

This report does not include any representation as to the quality of ANCE's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, nor the suitability of any of ANCE's services for any customer's intended purpose.

Deloitte LLP

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
30 April 2019

Deloitte.

ATTACHMENT A

LIST OF IN SCOPE CAs for SSL BASELINE REQUIREMENTS

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

Deloitte.

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	1302d5e2404c92468616675db4bbbbb26b3efc13	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	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	574ebb95293483333d742990c24a4d00c49681e6	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	063627355C941A1C93FC515CBAEF2F173D4A646DDEB139CB8C75C1022222994F

tuntrust
Agence Nationale de Certification Electronique

ANCE MANAGEMENT'S ASSERTION

Agence Nationale de Certification Electronique ("ANCE" or "TunTrust") operates the Certification Authority (CA) services as enumerated in Attachment A, and provides SSL CA services. ANCE 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 Tunis, Tunisia, as of 30 April 2019, ANCE has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - TunTrust PKI Certificate Policy / Certification Practice Statement, v02, 29 April 2019 ("CP/CPS"), including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the ANCE website, and provided such services in accordance with its disclosed practices

- suitably designed, and placed into operation, 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 ANCE)

- suitably designed, and placed into operation, 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

- suitably designed, and placed into operation, 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 v2.3.

Syrine Tlili
Agence Nationale de Certification Electronique
30 April 2019

Agence Nationale de Certification Electronique

ATTACHMENT A

LIST OF IN SCOPE CAs for SSL BASELINE REQUIREMENTS

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