

## 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 business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - [TunTrust PKI Certificate Policy / Certification Practice Statement](#), v02, 29 April 2019 ("CP/CPS")
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - ANCE provides its services in accordance with its Certification Practice Statement
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by ANCE); and
- suitably designed, and placed into operation, 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 v2.1](#).

ANCE does not escrow its CA keys, does not provide subscriber key generation, storage and recovery services,, does not provide integrated circuit card management services, does not provide certificate 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

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 v2.1.

### 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.

### **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 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) evaluating the suitability of the design of the controls; and
- (3) performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of ANCE's controls, individually or in the aggregate.

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 v2.1.

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 v2.1, nor the suitability of any of ANCE's services for any customer's intended purpose.

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



**ATTACHMENT A**

**LIST OF IN SCOPE CAs**

<b>Root CA</b>
1. TunTrust Root CA
<b>OV SSL Issuing CA</b>
2. TunTrust Services CA
<b>Other CA</b>
3. TunTrust Qualified 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	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	063627355C941A1C93FC515CBAEF2F173D4A646DDEB139CB8C75C102222994F
3	1	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Qualified CA	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA	5122200c68e4cce4bc38e5cff0eb2424388aea19	RSA 4096 -bits	RSA SHA-256	Apr 18 12:01:27 2019 GMT	Apr 18 12:01:27 2039 GMT	Digital Signature, Certificate Sign, CRL Sign	286C725FB089109C8E10D630969E8FFCFB9F7436	5D2E8DC2F18664DD9B81BAF8B0FA8D4021D0FCD57B2E2FFF805DAB1C7EE7AFA2
3	2	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Qualified CA	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA	640c4827ee903eafb4d73db2797a91afc985727a	RSA 4096 -bits	RSA SHA-256	Apr 26 09:49:02 2019 GMT	Apr 26 09:49:02 2039 GMT	Certificate Sign, CRL Sign	286C725FB089109C8E10D630969E8FFCFB9F7436	21C266BC3D023249F9F73ECFF03BF15234270D425FE36C8180F623C712DFE28E

## **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 the following CA services:

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

The management of ANCE is responsible for establishing controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 ANCE's Certification Authority operations.

ANCE management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in ANCE management's opinion, in providing its Certification Authority (CA) services at Tunis, Tunisia, as of 30 April 2019, ANCE has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - [TunTrust PKI Certificate Policy / Certification Practice Statement](#), v02, 29 April 2019 ("CP/CPS")
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - ANCE provides its services in accordance with its Certification Practice Statement
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by ANCE); and
- suitably designed, and placed into operation, 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 v2.1](#), 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 and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and 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
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

### **Subscriber Key Lifecycle Management Controls**

- Requirements for Subscriber Key Management

### **Certificate Lifecycle Management Controls**

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

ANCE does not escrow its CA keys, does not provide subscriber key generation, storage and recovery services, does not provide subordinate CA certification, does not provide certificate suspension services, does not provide integrated circuit card management services, does not provide certificate suspension services, and does not provide third-party subordinate CA or cross certificate issuance or management.

**ATTACHMENT A**

**LIST OF IN SCOPE CAs**

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