Ernst & Young P/S
Osvald Helmuths Vej 4
P.O. Box 250
2000 Frederiksberg
Denmark

Telephone +45 73 23 30 00
Telefax +45 72 29 30 30
www.ey.com/dk
Reg. no. 30 70 02 28

# Independent Auditor's Assurance Report

To the management of Telia Company AB:

**Scope**

We have been engaged to report on Telia Company AB's (Telia) operation of its SSL Certification Authority (CA) services in Finland and Sweden regarding whether during the period from April 1, 2016 through March 31, 2017, Telia:

- disclosed its Certificate practices and procedures, and its commitment to provide SSL certificates in conformity with the applicable CA/Browser Forum Guidelines in its
  - Telia Root Certificate Policy and Certification Practice Statement v2.2;
  - Telia Server Certificate Policy and Certification Practice Statement v1.7;
  - Telia Gateway Certificate Policy and Certification Practice Statement v1.4; and
  - Telia Production Certification Practice Statement v2.5
- maintained effective controls to provide reasonable assurance that:
  - subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained;
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity; and
- maintained effective controls to provide reasonable assurance that it met the Network and Certificate System Security Requirements set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0 for the following CAs:

| Distinguished name of the CA | Issuer | SHA1 fingerprint of the CA certificate |
|---|---|---|
| CN = Sonera Class2 CA<br>O = Sonera, C = FI | Self-signed | 37 f7 6d e6 07 7c 90 c5 b1 3e 93 1a b7 41 10 b4 f2 e4 9a 27 |
| CN = TeliaSonera Root CA v1<br>O = TeliaSonera | Self-signed | 43 13 bb 96 f1 d5 86 9b c1 4e 6a 92 f6 cf f6 34 69 87 82 37 |
| | Sonera Class2 CA | 9f f6 1d eb b4 ed 26 3b 4d be c7 79 87 ca 49 3c 6c c9 3a a4 |
| CN = TeliaSonera Extended Validation SSL CA v1<br>O = TeliaSonera, C = FI | TeliaSonera Root CA v1 | f1 f5 48 b0 1e b2 66 fa 95 c3 0f 79 c3 c9 1f 58 ea 3d f1 8c |
| CN = TeliaSonera Server CA v2<br>O = TeliaSonera, C = FI | TeliaSonera Root CA v1 | 0e c6 42 d0 0f 8d cf 7b 19 6a c0 a9 f2 c8 57 e3 42 68 79 a4 |
| CN = TeliaSonera Server CA v1<br>O = TeliaSonera | TeliaSonera Root CA v1 | 41 c4 34 fa 80 ed b4 bf 58 a6 98 c2 b1 54 20 d6 f3 4a 33 d0 |

| | | |
|---|---|---|
| CN = TeliaSonera Gateway CA v2<br>O = TeliaSonera, C = FI | TeliaSonera Root CA v1 | 3f 1a 1c cb eb b8 c7 3b e9 94 46 91<br>8e 3f af f3 ae d2 47 a3 |
| CN = TeliaSonera Gateway CA v1<br>O = TeliaSonera | TeliaSonera Root CA v1 | 0d e2 60 f7 96 5c c7 d1 cc be 92 21<br>26 68 52 9f e5 5f 7d cd |

**Telia's responsibility**

Telia's management is responsible for the disclosures and controls as referred to above.

**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.

Ernst & Young Godkendt Revisionspartnerselskab applies International Standard on Quality Control 1[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 responsibility**

Our responsibility is to express an opinion based on our procedures. Our work was conducted in accordance with International Standards on Assurance Engagements 3000 "Assurance Engagements Other Than Audits or Review of Historical Financial Information" in order to obtain reasonable assurance for our opinion, and accordingly, included:

(1) obtaining an understanding of Telia's key and certificate life cycle 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 life cycle management operations, and over development, maintenance and operation of systems integrity;

(2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle 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.

The relative effectiveness and significance of specific controls at Telia 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.

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

**Inherent limitations**

Because of the nature and inherent limitations of controls, Telia'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.

[1] ISQC 1, Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements

**Basis for qualified opinion**

In performing our engagement, we identified the following matters that prevented certain SSL Baseline criteria from being met during the examination period from April 1, 2016 through March 31, 2017:

| Criteria | Matters noted |
|---|---|
| **Principle 2 Criterion 2.1 and 2.3**<br>The CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for certificate content and profile as established in section 9 of the SSL Baseline Requirements including the subject information. | Five certificates issued by the TeliaSonera Gateway CA v2 during the reporting period did not contain subject:localityName or subject:stateOrProvinceName attributes. In addition, a few certificates issued by the TeliaSonera Server CA v2 contained inappropriate subject:localityName or subject:stateOrProvinceName attributes such as “L=Default City”, “ST=Unknown” and “ST=.”.<br><br>As a result, Principle 2 Criteria 2.1 and 2.3 were not met for the TeliaSonera Gateway CA v2 and TeliaSonera Server CA v2. |
| **Principle 2, Criterion 7.2**<br>The CA maintains controls to provide reasonable assurance that the following events are recorded:<br>…<br>(2) CA and Subscriber Certificate lifecycle management events, including:<br>…<br>(b) all verification activities stipulated in the Baseline Requirements and the CA’s Certification Practice Statement<br>(c) date, time, phone number used, persons spoken to, and end results of verification telephone calls<br>… | For 7 out of 61 tested verification telephone calls related to certificates issued by the TeliaSonera Server CA v2, the calls had not been adequately documented.<br><br>For 4 out of 74 tested subject identity verifications related to certificates issued by the TeliaSonera Server CA v2, no documentation was found of the activities related to identity verification of the applicant organization.<br><br>As a result, Principle 2, Criterion 7.2 (requirements 2b and 2c) was not met for the TeliaSonera Server CA v2. |
| **Principle 4, Criterion 1**<br>The CA maintains controls to provide reasonable assurance that:<br>…<br>(h) Configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the CA’s security policies;<br>…<br>(l) Recommended security patches are applied to Certificate Systems within six months of the security patch’s availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. | Security configurations of all the relevant systems had not been reviewed on at least a weekly basis.<br><br>In some cases security patches had not been applied to certain Certificate Systems within six months and no reasoning had been documented.<br><br>As a result, Principle 4 Criterion 1 (requirements h and l) was not met. |

| Criteria | Matters noted |
|---|---|
| **Principle 4, Criterion 4**<br>The CA maintains controls to provide reasonable assurance that:<br>…<br>(b) A formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities;<br>…<br>(d) Perform a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant;<br>…<br>(f) Perform one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process:<br>► Remediate the Critical Vulnerability;<br>► If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following:<br>- Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and<br>- Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or<br>► Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following:<br>- The CA disagrees with the NVD rating;<br>- The identification is a false positive;<br>- The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or<br>- Other similar reasons | Vulnerability correction process that would have included identification, review, response, and remediation of vulnerabilities had not been documented for one production site.<br><br>Penetration Tests had not been performed on at least an annual basis. The previous Penetration Test had been performed in December 2015.<br><br>No procedures had been defined and implemented to formally evaluate and document factual basis for determination that discovered critical vulnerabilities did not require remediation within 96 hours.<br><br>As a result, Principle 4 Criterion 4 (requirements b, d and f) was not met. |

**Opinion**

In our opinion, except for the matters described in the previous paragraph, during the period from April 1, 2016 through March 31, 2017, Telia, in all material respects

► disclosed its certificate practices and procedures and its commitment to provide SSL certificates in conformity with the applicable CA/Browser Forum Guidelines

► maintained effective controls to provide reasonable assurance that:

- subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
- the integrity of keys and certificates it manages was established and protected throughout their life cycles;

► maintained effective controls to provide reasonable assurance that:

- logical and physical access to CA systems and data was restricted to authorized individuals;
- the continuity of key and certificate management operations was maintained;
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity; and

- maintained effective controls to provide reasonable assurance that it met the Network and Certificate System Security Requirements set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0.

**Intended users and purpose**

This report does not include any representation as to the quality of Telia's certification services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0, nor the suitability of any of Telia's services for any customer's intended purpose.

Copenhagen June 30, 2017

Ernst & Young P/S
Godkendt Revisionspartnerselskab

Claus Thaudahl Hansen
Partner, State Authorised Public Accountant

Juha Sunila
Senior Manager, CISA, CISSP