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 Company) operation of its SSL Certification Authority (CA) services in Finland and Sweden regarding whether during the period from April 1, 2015 through March 31, 2016 Telia Company:

- 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;
  - 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
  - Effective controls to meet 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:

Root CAs	Issuing CAs capable of issuing SSL certificates
Sonera Class 2 CA TeliaSonera Root CA v1*	TeliaSonera Server CA v1 TeliaSonera Server CA v2
	TeliaSonera Gateway CA v1 TeliaSonera Gateway CA v2

* *Both self-signed and intermediate (signed by Sonera Class 2 CA) versions of TeliaSonera Root CA v1 certificate exist.*

Telia Company's responsibility

Telia Company'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 Company'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 Company 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 Company'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.

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, 2015 through March 31, 2016:

Criteria	Matters noted
Principle 2, Criterion 7.2 The CA maintains controls to provide reasonable assurance that the following events are recorded: … (2) CA and Subscriber Certificate lifecycle management events, including: … (c) date, time, phone number used, persons spoken to, and end results of verification telephone calls …	Telephone calls related to verification of domain authorization document authenticity had not been documented. Out of 35 tested SSL server certificates, domain authorization documents were relied on in two cases. As a result, Principle 2, Criterion 7.2 (requirement 2c) was not met.

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

Criteria	Matters noted
Principle 4, Criterion 1 The CA maintains controls to provide reasonable assurance that: … (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; …	Security configurations of relevant systems had not been reviewed on at least a weekly basis. As a result, Principle 4 Criterion 1 (requirement h) was not met.
Principle 4, Criterion 2 The CA maintains controls to provide reasonable assurance that: … (j) Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations; …	We noted that regular review of systems accounts did not cover all relevant systems and for OCSP system we were not able to determine that the review had been performed at least every 90 days due to lack of documentation. As a result, Principle 4 Criterion 2 (requirement j) was not met.
Principle 4, Criterion 3 The CA maintains controls to provide reasonable assurance that: (a) Security Support System under the control of CA or Delegated Third Party Trusted Roles are implemented to monitor, detect, and report any security-related configuration change to Certificate Systems; …	No Security Support System had been implemented to monitor, detect and report security-related configuration change to OCSP system. As a result, Principle 4 Criterion 3 (requirement a) was not met for OCSP system.

Principle 4, Criterion 4
The CA maintains controls to provide reasonable assurance that:
…
(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:
- Remediate the Critical Vulnerability;
- 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:
  - 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
  - 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
- Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following:
  - The CA disagrees with the NVD rating;
  - The identification is a false positive;
  - The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or
  - Other similar reasons
	No procedures had been defined and implemented to formally evaluate and document factual basis for determination that certain discovered critical vulnerabilities did not require remediation within 96 hours.
	
	As a result, Principle 4 Criterion 4 (requirement f) was not met.

Opinion

In our opinion, except for the matters described in the previous paragraph, during the period from April 1, 2015 through March 31, 2016, Telia Company, 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;
  - 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
  - Effective controls to meet 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 Company'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 Company's services for any customer's intended purpose.

Copenhagen 30 June 2016

Ernst & Young P/S
Godkendt Revisionspartnerselskab

Claus Thaudahl Hansen
Partner, State Authorised Public Accountant

Juha Sunila
Senior Manager, CISA, CISSP