Independent Accountants' Assurance Report

To the Management of
TeliaSonera AB:

We have been engaged to report on TeliaSonera AB's (TeliaSonera) operation of its TeliaSonera Server CA v1 certification authority services regarding whether during the period from April 1, 2012 through March 31, 2013 TeliaSonera:

- disclosed its Certificate practices and procedures, 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; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

in accordance with the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria. These disclosures and controls are the responsibility of the TeliaSonera's management. Our responsibility is to express an opinion based on our audit.

Our assurance engagement was conducted in accordance with International Standards on Assurance Engagements and, accordingly, included:

(1) obtaining an understanding of TeliaSonera's SSL certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of SSL certificates,

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

The relative effectiveness and significance of specific controls at TeliaSonera 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.

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

In performing our engagement, we noted the following matters that prevented certain SSL Baseline Audit Criteria from being met during the audit period from April 1, 2012 through March 31, 2013:

- Principle 2, Criterion 2.5: TeliaSonera had not implemented controls and procedures to identify certificate requests with known weak private key (such as a Debian weak key). As a result, Principle 2 Criterion 2.5 *The CA maintains controls and procedures to provide reasonable assurance that Certificates are not issued if the requested Public Key does not meet the requirements set forth in Appendix A of the SSL Baseline Requirements or if it has a known weak Private Key (such as a Debian weak key)*, was not met.
- Principle 2, Criterion 3.4: The subscriber agreement used by TeliaSonera during the engagement period did not meet all the requirements of the SSL Baseline Requirements Section 10.3.1. As a result, Principle 2 Criterion 3.4 *The CA maintains controls and procedures to provide reasonable assurance that the CA, prior to the issuance of a Certificate, obtains a subscriber and/or terms of use agreement in accordance with the SSL Baseline Requirements section 10.3.1*, was not met.
- Principle 2, Criterion 5.2: Although TeliaSonera has the capability to accept and acknowledge certificate problem reports on a 24x7 basis through CA's customer service, there were no controls implemented that would provide reasonable assurance that the CA can identify high priority certificate problems and begin investigation of the problems within 24 hours at all times. As a result, Principle 2, Criterion 5.2 *The CA maintains controls to provide reasonable assurance that it: has the capability to accept and acknowledge Certificate Problem Reports on a 24x7 basis; identifies high priority certificate problem reports; begins investigation of certificate problem reports within 24 hours; decides whether revocation or other appropriate action is warranted; and where appropriate, forwards such complaints to law enforcement*, was not met.
- Principle 2, Criterion 7.4: Documentation of verifications and subscriber agreements was not retained for certain certificates issued during the engagement period as required by SSL Baseline Requirements Section 15.3.2. The missing documentation related to certificates issued certain customer organizations that use the CA's self-service software to issue certificates in which the domain and organization names had been pre-validated by the CA in years prior to the start of the engagement period. As a result, Principle 2, Criterion 7.4 *The CA has a policy and maintains controls to provide reasonable assurance that all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, is retained for at least seven years after any Certificate based on that documentation ceases to be valid,* was not met.
- Principle 3, Criterion 2: While TeliaSonera has performed risk assessments, they are not done annually as required by the SSL Baseline Requirements Section 16.2. As a result, Principle 3, Criterion 2 *The CA performs a risk assessment at least annually that: identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes; assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats*, was not met.

- Principle 3, Criterion 3: TeliaSonera has not prepared a Security Plan in accordance with the SSL Baseline Requirements Section 16.3. As a result, Principle 3, Criterion 3 *The CA develops, implements, and maintains a Security Plan consisting of security procedures, measures, and products designed to reasonably manage and control the risks identified during the risk assessment, commensurate with the sensitivity of the certificate data and certificate management processes*, was not met.
- Principle 3, Criterion 4: TeliaSonera's Business Continuity Plan did not include all the topics described in the SSL Baseline Requirements Section 16.4 and the plan had not been reviewed and updated annually. As a result, Principle 3, Criterion 4 *The CA develops, implements, and maintains a Business Continuity Plan that includes at a minimum the topics described in the SSL Baseline Requirements Section 16.4 and that the Business Continuity Plan is tested at least annually, reviewed, and updated*, was not met.

In our opinion, except for the matters described in the previous paragraph, during the period from April 1, 2012 through March 31, 2013, TeliaSonera, 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; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

in accordance with the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria.

This report does not include any representation as to the quality of TeliaSonera's certification services beyond those covered by the WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, or the suitability of any of TeliaSonera's services for any customer's intended purpose.

September 19, 2013

Richard Brown

Partner

Ernst & Young LLP