TELIA PUBLIC RESPONSE TO AUDIT 2019

#	Deviation	Relevant WebTrust Criteria	Telia's Response
1	The Key Usage extension in the root CA certificates of *TeliaSonera Root CA v1* and *Sonera Class 2 CA* is not marked critical and *TeliaSonera Root CA v1* certificate's subject information does not include subject:countryName. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.3 to not be met. However, Telia generated a new root CA, *Telia Root CA v2*, on 29 November 2018, which is planned to eventually replace *TeliaSonera Root CA v1* and *Sonera Class 2 CA*. Extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of the new *Telia Root CA v2* certificate conform to the Baseline Requirements.	**Principle 2, Criterion 2.3** The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Root CA certificates generated conform to the Baseline Requirements.	In 2002 and 2007 when these Root CA certificates were created there weren't any clear requirements for noted issues. The first CA Browser Forum BR document appeared in 2011 (effective 2012). Telia has created a compliant new Root CA. Telia will next create an application that the new compliant root CA will eventually replace the old roots. Inclusion applications will be created in Q3/2019 and delivered to all browser vendors.
2	The subscriber certificates issued by *Telia Domain Validation SSL CA v1* contained wrong policy identifier until 25 June 2018. The certificates contained the policy identifier of the Organization Validated certificates (2.23.140.1.2.2) although the certificates were only domain validated. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criteria 2.5 and 2.14 to not be met. All the certificates with the wrong policy identifier have been revoked by Telia before the end of September 2018.	**Principle 2, Criterion 2.5** The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated conform to the Baseline Requirements. **Principle 2, Criterion 2.14** The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including: … • Subject field requirements if Reserved Certificate Policy Identifiers are asserted … …	Telia did an extra Point-In-Time Audit in Oct 2018 to demonstrate that this issue was properly fixed after its discovery. Point-In-Time audit report is available at https://support.trust.telia.com/download/CA/Telia-SSL-Baseline-Requirements-Report-2018-10-31.pdf

#	Deviation	Relevant WebTrust Criteria	Telia's Response
3	Before 9 August 2018 many organization validated subscriber certificates included an email address as an optional subject attribute in the Subject field of the certificate and the CA did not have controls to adequately verify the email address information. As a partly mitigating factor, the email address has not been included in the subject alternative name extension and the certificates have not included key usage purpose id-kp-emailProtection in the Extended Key Usage extension. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.14 to not be met. Since 9 August 2018 email address has not been included in any organization validated subscriber certificates.	**Principle 2, Criterion 2.14** The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including: … • Other Subject Attributes …	Telia did an extra Point-In-Time Audit in Oct 2018 to demonstrate that this issue was properly fixed after its discovery. Point-In-Time audit report is available at https://support.trust.telia.com/download/CA/Telia-SSL-Baseline-Requirements-Report-2018-10-31.pdf
4	13 subscriber certificates with inappropriate locality names were issued to three different organizations by TeliaSonera Server CA v2. According to the CPS, locality name should be a city name, but in these cases locality name consisted of a country name or organization's postal office name. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criteria 2.14 and 4.2 to not be met. All these certificates have been revoked.	**Principle 2, Criterion 2.14** The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including: … • subject:localityName … **Principle 2, Criterion 4.2** The CA maintains controls to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the SSL Baseline Requirements: • Identity (SSL Baseline Requirements Section 3.2.2.1) …	Telia's verification routine regarding L values has been improved during this audit period. Before the improvements some slightly non-compliant values were accepted by Telia to certificate L field. The last problem happened in Feb 2019. The full incident report and detailed explanation can be found here: https://bugzilla.mozilla.org/show_bug.cgi?id=1551372
5	Weekly security configuration reviews were not implemented for three tested security support systems until in October 2018 and therefore configuration	**Principle 4, Criterion 1.8** The CA maintains controls to provide reasonable assurance that configurations of Issuing Systems, Certificate Management Systems,	Telia did an extra Point-In-Time Audit in Oct 2018 to demonstrate that previous review problems were properly fixed after discovery last year. Point-In-Time audit report is available at https://support.trust.telia.com/download/CA/Telia-

#	Deviation	Relevant WebTrust Criteria	Telia's Response
	changes of these systems had not been reviewed on at least a weekly basis during the period from April 2018 to September 2018. In addition, weekly configuration change report of one tested security support system had not functioned correctly and therefore its configurations had not been reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies throughout the period 1 April 2018 to 31 March 2019. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 4, Criterion 1.8 to not be met.	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.	SSL-Baseline-Requirements-Report-2018-10-31.pdf After Point-In-Time audit one automatic reviewing system related to secondary Firewall system failed and was undetected and not operational for several months. Now it has been fixed. All other reviewing systems related the most important CA systems have been functional. The planned change is to monitor with a monthly human review functionality of all reviewing systems. Now only the most important functionalities are verified monthly. Improvements to review system monitoring will be implemented in Q3/2019.