

TELIA COMPANY AB - PUBLIC RESPONSE

To Independent Auditor's Report WebTrust for CAs Baseline Requirements

#	Observation	Relevant WebTrust Criteria	Telia's Response
1	<p>The Key Usage extension in the root CA certificates of <i>TeliaSonera Root CA v1</i> is not marked critical and <i>TeliaSonera Root CA v1</i> certificate's subject information does not include subject:countryName.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.7, Principle 2, Criterion 2.3 to not be met.</p> <p>However, Telia generated a new root CA, <i>Telia Root CA v2</i>, on 29 November 2018, which is planned to eventually replace <i>TeliaSonera Root CA v1</i> 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.</p>	<p>Principle 2, Criteria 2.3</p> <p>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</p>	<p>The non-conforming Root CA certificate <i>TeliaSonera Root CA v1</i> was created 2007. At the time of creation of the said certificate there were neither CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates (BR) nor WebTrust conformance assurance requirements (WT) for CAs existing. Therefore, the said certificate could not be created conforming to the BR and WT requirements. BR and subsequently WT became effective for the first time from the beginning of 2012.</p> <p>Telia's recent Root CA, <i>Telia Root CA v2</i>, is currently in final stage to be included in all major Root Programs.</p> <p>Telia has begun transition the issuance of certificates from the CA hierarchy created under Telia Root CA v2 in the latter half of 2022.</p> <p>To ensure smooth transition for all Telia CA subscribers, Telia has created a transition plan to gradually move all subscribers from the old root CAs to the new root CA hierarchy and consequently cease the operation of <i>TeliaSonera Root CA v1</i> in the future.</p> <p>Telia's transition plan ensures that effect on subscribers is kept to minimum by transitioning subscriber certificate issuance to new root hierarchy when certificates issued from the old root expire and thus need to be renewed.</p> <p>Telia has transitioned subscribers to Telia Root CA v2 from the beginning of April 2023 for TLS certificate issuance.</p>

Company information