Memo
Public

Date	**Page**
2020-06-26	1 (1)
Identifier	**Version**
Public Response 2020	1.0

Creator | **Relation**
Telia PKI-team | Telia CA

TELIA PUBLIC RESPONSE TO AUDIT 2020

#	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, Criteria 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 in late 2018. It has already been imported to some OS systems and Telia will next create applications that all OS and browser vendors start using it. However, Telia will need to use old roots for several years so that the new root has time to spread.