Approved on
August 7, 2018

Approved by
Telia Finland Oyj
Telia CA Security Board

Creator
Pekka Lahtiharju

Telia CA response to Public WebTrust Audit observations 2018

Description
This document includes Telia CA response to Public Webtrust Audit observations 2018 created by CA auditors.

Company information
Telia Finland Oyj
Teollisuuskatu 15, 00510 HELSINKI, FI
Registered office: Helsinki
Business ID 1475607-9, VAT No. FI14756079

#	Deviation	Relevant WebTrust Criteria	Telia response
1	*Telia Gateway Certificate Policy and Certification Practice Statement v1.5* applicable to server authentication certificates issued by *TeliaSonera Gateway CA v2* does not disclose whether the CA reviews CAA (Certification Authority Authorization) DNS Records, and if so, the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 1, Criterion 6 to not be met.	**Principle 1, Criterion 6** The CA discloses in its Certificate Policy (CP) and/or Certification Practices Statement (CPS) under section 4.2 (if the CA's disclosures follow RFC 3647) or under section 4.1 (if the CA's disclosures follow RFC 2527) whether the CA reviews CAA (Certification Authority Authorisation) DNS Records, and if so, the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names. The CA maintains controls to provide reasonable assurance that it logs all actions taken, if any, consistent with its processing practice.	CAA chapter was missing from this CPS but CAA handling has been done in the similar way compared to Telia's normal SSL certificates. This can be verified from logs. Telia has stopped using this CPS for new certificates in July 2018. The final update stating this close down and fixing the CAA chapter will be official at the end of August 2018 .
2	The CA had not prepared and followed a key generation script for the key generation ceremonies of *Telia Domain Validation SSL CA v1*. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 2, Criterion 1.1 to not be met.	**Principle 2, Criterion 1.1** The CA maintains controls to provide reasonable assurance that Root CA and Subordinate CA Key Pairs are created in accordance with SSL Baseline Requirements Section 6.1.1.1.	Key generation was done according to all requirements in a controlled way even though the document describing the process was inadequate. This can be verified from the video recorded. Telia has now prepared a new template and documentation for this purpose. The missing documentation was created afterwards related to mentioned key ceremony. Telia has recreated the referred CA keys in July using the updated new documentation. The related new CA (v2) will be created in August 2018. All Telia DV certificates will be moved to v2 in September 2018. All V1 certificates and v1 CA will be revoked in September 2018.
3	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 v2.2, Principle 2, Criterion 2.3 to not be met.	**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 a plan to create a new root CA in 2018 that will be compliant with all requirements at the time.
4	The subscriber certificates issued by the *Telia Domain Validation SSL CA v1* contained wrong policy identifier. The certificates contained the policy identifier of the Organization Validated certificates (2.23.140.1.2.2) although the certificates were only domain validated. However, *Telia Domain*	**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 after the Effective Date (1 July	This was immediately fixed when reported to Telia. All new certificates since 26th June 2018 have a correct OID value. Telia has analysed the root cause to the problem be inadequate test processes. Processes are now enhanced. More details can be found

#	Deviation	Relevant WebTrust Criteria	Telia response
	Validation SSL CA v1 issued only 17 certificates throughout the period 8 Mar 2018 to 31 Mar 2018. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 2, Criteria 2.5 and 2.14 to not be met.	2012) 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 …	from public discussion at mozilla.dev.security.policy at bug "Telia CA – incorrect OID value" Telia Incident evaluation process result was that no immediate risk was caused as OID was correct OV OID, all certificates with wrong OID fields were issued to known Telia hosted service customers, even though the issue itself was confirmed serious. As none of these certificates were issued to wrong entities Telia decided to do the replacement/revoking in the organized way so that overall harm would be minimal by replacing these certificates together with the customers. Telia will revoke all incorrect certificates. Most of them have already been revoked. The rest will be revoked in co-operation with the Customers in August and September 2018.
5	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 v2.2, Principle 2, Criterion 2.14 to not be met.	**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 CA has verified all Subject values including E values. However, Telia has used verifying process where values are rejected in case they are technically incorrect or do not seem to be correct support email address in the eyes of the Registration Officer. Telia re-verified that the above mentioned verifying process has not been used with any other subject fields except with E and OU values. Telia customers sometimes want to put email address of another company to indicate email support point related to the server that has the OV certificate. Thus Telia has not required domain ownership for E field domain. This has been clearly documented in Telia CPS. Telia has added this issue to public discussion into bug "Telia CA – problem in E validation" at mozilla.dev.security.policy. Based on that Telia completely stopped adding E values on 7th Aug 2018 to new SSL certificates because E values are not typically added to certificates by other CAs. Telia CPS will be updated accordingly in August 2018.

#	Deviation	Relevant WebTrust Criteria	Telia response
6	Telia had outsourced provision of validation activities in Sweden to a Delegated Third Party during the reporting period. The contract between the CA and the Delegated Third Party did not require the delegated party to: • meet the qualification requirements of the Baseline Requirements Section 5.3.1 • retain documentation in accordance with the Baseline Requirements Section 5.5.2; • abide by the other provisions of the Baseline Requirements that are applicable to the delegated function; and • comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 2, Criterion 6.3 to not be met.	**Principle 2, Criterion 6.3** The CA maintains controls to provide reasonable assurance that before the CA authorizes a Delegated Third Party to perform a delegated function, the CA contractually require the Delegated party to: • meet the qualification requirements of the Baseline Requirements Section 5.3.1, when applicable to the delegated function; • retain documentation in accordance with the Baseline Requirements Section 5.5.2; • abide by the other provisions of the Baseline Requirements that are applicable to the delegated function; and • comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.	The listed issues have been the actual requirements (e.g in training sessions) with the outsourcing party but they are not listed in the contract now. Telia will sign a new contract with this external company in September 2018.
7	The security configurations of all the relevant systems had not been reviewed on at least a weekly basis. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 4, Criterion 1.8 to not be met.	**Principle 4, Criterion 1.8** The CA maintains controls to provide reasonable assurance that 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.	All main systems were included in the weekly reviews but some supporting systems weren't. In July Telia has extended the scope of its weekly reviews. Telia will also automate these checks whenever it is possible. Most automatic controls are now activated but those will be further enhanced later in 2018.
8	Human review of logs had not covered all the relevant application and system logs and that some log reviews had not always been performed at least every 30 days. In addition, testing that the monitoring, logging, alerting, and log-integrity-verification functions were operating properly had not been performed during the reporting period. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 4, Criterion 3.5 to not be met.	**Principle 4, Criterion 3.5** The CA maintains controls to provide reasonable assurance that a human review of application and system logs is performed at least every 30 days and includes: • Validating the integrity of logging processes; and • Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly.	Telia has focused on reviewing SSL certificate logs and some client certificate log checks and process checks have been inadequate. Compensation is that automatic processes have reviewed all logs so that alarms are raised in problematic circumstances. Telia has now added the human reviews to new processes and the first new reviews have been done. Some additional log integrity verification solutions will start later 2018.

#	Deviation	Relevant WebTrust Criteria	Telia response
9	The CA had not documented its vulnerability correction process. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 4, Criterion 4.2 to not be met.	**Principle 4, Criterion 4.2** The CA maintains controls to provide reasonable assurance that a formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities.	Vulnerabilities are always fixed as required but documentation has been scarse because this far Telia CA was using Telia's general vulnerability correction process that has been documented in Telia's internal document "Group Instruction – Cybersecurity v4" in chapter "A.12.6.1 Technical vulnerability management". In July 2018 Telia CA created more extensive vulnerability management documentation specifically for Telia CA.